DELIVERABLE D2.4
Requirements assessment and delivery of website and mobile app of Interactive HandBook (final version)
Project No. 786741
Start date of project: 01-05-2018
Duration: 30 months

Revision: 03
Date: 05/02/2021

Document Information

Document Name: Requirements assessment and delivery of website and mobile app of Interactive Handbook (final version)

WP2 – Title: Requirements, entry questionnaire and interactive handbook

Task 2.3 – Title: T2.3 – SMOOK: Interactive GDPR handbook for micro-enterprises

Deliverable 2.4 - Title: D2.4 – Requirements assessment and delivery of website and mobile app of Interactive HandBook

Revision: 03
Revision Date: 31/01/2021

Authors: Nadia Feci and Brahim Bénichou (KUL - editors), Mathilde Van Brussel, Eva Merloni (ESBA), Thomas Wilczek (FBA), Evangelos Kotsifakos, Maria Aspri (LSTECH), Ángel Cuevas Rumin, Rubén Cuevas, Celia López (UC3M), Roberto González Sánchez, Mathias Niepert (NEC), Rohit Kumar, Alex Pereda (EUT), Ramón Codina (EUT), Rosa Araujo (EUT), Matthias Gallé (NAVER), Narseo Vallina-Rodríguez, Álvaro Feal (IMDEA).

Dissemination Level

<table>
<thead>
<tr>
<th>Project co-funded by the EC within the H2020 Programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>PU</td>
</tr>
<tr>
<td>PP</td>
</tr>
<tr>
<td>RE</td>
</tr>
<tr>
<td>CO</td>
</tr>
</tbody>
</table>
Executive summary

Deliverable 2.4 (D2.4) is the final deliverable under work package 2. As described in the project proposal, D2.4 consists of two distinct parts:

- a report of the assessment of whether the requirements defined at the beginning of the project (in D2.1), are successfully covered by the SMOOTH Platform;
- a report on the delivery of the mobile app and website implementing the SMOOTH interactive GDPR handbook.

In addition to this an example of a so-called ‘human assessment’ is also included. An assessment performed by the SMOTH Platform was re-assessed by a legal expert and the findings of both assessments are compared.

This final version of the deliverable includes findings related to the market validation that has been performed in the last months of the project. This
The document reports the final state of the GDPR Handbook as it has been implemented as a mobile app and a website.

In summary this final version of D2.4 contains:

- a description of how the GDPR Handbook was developed;
- the legal, functional, and technical requirements that have been met;
- the texts, graphics and videos related to the current version of both the mobile and the website application of the SMOOK GDPR Handbook;
- an assessment of whether the requirements defined in D2.1 are successfully covered by the SMOOTH Platform, per relevant work package (WP2, WP3, WP4, WP5, WP6, WP7),
- the “Human assessment”.

### List of abbreviations and acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEPD</td>
<td>Agencia Española de Protección de Datos</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>CNIL</td>
<td>Commission Nationale de l'Informatique et des Libertés</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>DPIA</td>
<td>Data Protection Impact Assessment</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>ESBA</td>
<td>European Small Business Alliance</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>LIA</td>
<td>Legitimate Interests Assessment</td>
</tr>
<tr>
<td>MEnt(s)</td>
<td>Micro-enterprise(s)</td>
</tr>
<tr>
<td>OTT provider</td>
<td>Over-the-top services provider</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
<tr>
<td>WP29</td>
<td>Article 29 Working Party</td>
</tr>
<tr>
<td>SME(s)</td>
<td>Small and medium-sized enterprise(s)</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union</td>
</tr>
</tbody>
</table>
Table of contents

1. Introduction .................................................................................................................. 9
   1.1. Work Package 2 - Requirements, entry questionnaire and interactive handbook ....... 9
   1.2. Deliverable 2.4 .......................................................................................................... 9

2. The GDPR Handbook (for micro-enterprises) ......................................................... 10
   2.1. The requirements of the GDPR Handbook ............................................................... 10
   2.2. Practical implementation .......................................................................................... 12
       2.2.1. Legal requirements for micro-enterprises ......................................................... 12
       2.2.2. Micro-enterprises’ requirements for the Handbook .......................................... 13
       2.2.3. Technical requirements .................................................................................. 14
       2.2.3.1. The GDPR Handbook Mobile App ................................................................. 14
       2.2.3.2 The GDPR Handbook Website ....................................................................... 16
   2.3. Practical implementation ......................................................................................... 16
       2.3.1. In general .......................................................................................................... 17
       2.3.2. Interactivity: flowcharts .................................................................................... 17
           2.3.2.1. Flowchart a: territorial application of the GDPR ....................................... 17
           2.3.2.2. Flowchart b: do I need to appoint a DPO? .................................................. 17
       2.3.3. Multilinguality .................................................................................................. 18
           2.3.3.1. Desktop version .......................................................................................... 18
           2.3.3.2. Mobile app ................................................................................................ 19
       2.3.4 Additional examples .......................................................................................... 19
       2.3.5. Videos ............................................................................................................. 21
       2.3.6. Availability mobile app ..................................................................................... 22
       2.3.7. Testing ............................................................................................................. 22
       2.3.8. Incorporation of the SMOOTH Community on the FundingBox Platform .......... 22
       2.3.9. Translation ....................................................................................................... 23

3. The requirements assessment ...................................................................................... 23
   3.1. WP2: assessment of the legal requirements ............................................................ 23
       3.1.1. Initial requirements ........................................................................................... 23
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.2.</td>
<td>Modified requirements</td>
<td>34</td>
</tr>
<tr>
<td>3.1.3.</td>
<td>Requirements that are/will be covered</td>
<td>34</td>
</tr>
<tr>
<td>3.1.4.</td>
<td>Requirements that will not be covered</td>
<td>44</td>
</tr>
<tr>
<td>3.1.5.</td>
<td>Overall compliance</td>
<td>46</td>
</tr>
<tr>
<td>3.2.</td>
<td>WP3: assessment of the technical requirements SMOOTEXT</td>
<td>46</td>
</tr>
<tr>
<td>3.2.1.</td>
<td>Initial requirements</td>
<td>47</td>
</tr>
<tr>
<td>3.2.2.</td>
<td>Modified requirements</td>
<td>48</td>
</tr>
<tr>
<td>3.2.3.</td>
<td>Requirements that are/will be covered</td>
<td>48</td>
</tr>
<tr>
<td>3.2.4.</td>
<td>Requirements that will not be covered</td>
<td>49</td>
</tr>
<tr>
<td>3.2.5.</td>
<td>Overall compliance</td>
<td>49</td>
</tr>
<tr>
<td>3.3.</td>
<td>WP4: assessment of the technical requirements SMOODATA</td>
<td>49</td>
</tr>
<tr>
<td>3.3.1.</td>
<td>Initial requirements</td>
<td>49</td>
</tr>
<tr>
<td>3.3.2.</td>
<td>Modified requirements</td>
<td>51</td>
</tr>
<tr>
<td>3.3.3.</td>
<td>Requirements that are/will be covered</td>
<td>53</td>
</tr>
<tr>
<td>3.3.4.</td>
<td>Requirements that will not be covered</td>
<td>53</td>
</tr>
<tr>
<td>3.3.5.</td>
<td>Overall compliance</td>
<td>54</td>
</tr>
<tr>
<td>3.4.</td>
<td>WP5: assessment of the technical requirements SMONLINE</td>
<td>54</td>
</tr>
<tr>
<td>3.4.1.</td>
<td>Initial requirements</td>
<td>55</td>
</tr>
<tr>
<td>3.4.2.</td>
<td>Modified requirements</td>
<td>57</td>
</tr>
<tr>
<td>3.4.3.</td>
<td>Requirements that are/will be covered</td>
<td>58</td>
</tr>
<tr>
<td>3.4.4.</td>
<td>Requirements that will not be covered</td>
<td>61</td>
</tr>
<tr>
<td>3.4.5.</td>
<td>Overall compliance</td>
<td>62</td>
</tr>
<tr>
<td>3.5.</td>
<td>WP6: assessment of the technical requirements PLAT</td>
<td>62</td>
</tr>
<tr>
<td>3.5.1.</td>
<td>Initial requirements</td>
<td>62</td>
</tr>
<tr>
<td>3.5.2.</td>
<td>Modified requirements</td>
<td>65</td>
</tr>
<tr>
<td>3.5.3.</td>
<td>Requirements that are covered</td>
<td>65</td>
</tr>
<tr>
<td>3.5.4.</td>
<td>Requirements that will not be covered</td>
<td>68</td>
</tr>
<tr>
<td>3.5.5.</td>
<td>Overall compliance</td>
<td>68</td>
</tr>
<tr>
<td>3.6.</td>
<td>WP7: assessment of the technical requirements PILOT</td>
<td>68</td>
</tr>
<tr>
<td>3.6.1.</td>
<td>Initial requirements</td>
<td>68</td>
</tr>
<tr>
<td>3.6.2.</td>
<td>Modified requirements</td>
<td>70</td>
</tr>
</tbody>
</table>
3.6.3. Requirements that will be covered ................................................................. 70
3.6.4. Requirements that will not be covered .......................................................... 73
3.6.5. Overall compliance ...................................................................................... 73

4. Human assessment of a case assessed by the SMOOTH Platform........................ 73

4.1 Scope .................................................................................................................. 73

4.2 Modus operandi .................................................................................................. 75
  4.2.1. The use of a fictional case ............................................................................ 75
  4.2.2 The automated assessment of the case .......................................................... 75
  4.2.3 The Human Assessment .............................................................................. 76
  4.2.4 The conclusion ............................................................................................. 76

4.4 Conclusion ......................................................................................................... 76

5. Annexes ............................................................................................................... 77

Annex I – Final version of GDPR handbook mobile application, with legal texts and graphic design 78
Annex II - Final text version of SMOOK website application, with some graphics included ..178
Annex III – SMOOK Mobile App – screenshots and demonstration videos ..................298
Annex IV – SMOOK Website App – screenshots ...................................................... 301
Annex V – Human assessment of a case assessed by the SMOOTH Platform ............ 305
1. Introduction

1.1. Work Package 2 - Requirements, entry questionnaire and interactive handbook

This deliverable is the tailpiece of Work Package 2 of the SMOOTH project.

The purpose of Work Package 2 is to:

- provide a detailed analysis of the GDPR, focusing on micro-enterprises;
- extract the relevant requirements (legal, functional, technical, end-users side) for the SMOOTH Platform;
- design the entry questionnaire in order to collect the relevant contextual information from the micro-enterprises using the Platform; and
- create an interactive GDPR Handbook acting as a “go to” guide for data protection questions from micro-enterprises (taking into account their low level of knowledge about data protection).

Specifically, the objectives of this WP2 are to:

- identify and define the main GDPR requirements pertaining to micro-enterprises;
- define legal requirements for ensuring that the SMOOTH Platform is itself compliant with the GDPR;
- define functional requirements for the platform drawn also from micro-enterprises’ necessities, using their feedback;
- define technical requirements to be used as a baseline for the design and deployment of the SMOOTH Platform;
- design the entry questionnaire that micro-enterprises will have to fill in upon registration in the SMOOTH Platform;
- design and implement the Interactive GDPR Handbook for micro-enterprises, presenting in a plain language the rules that have to be complied with in order to be compliant with the GDPR; it will be implemented as a website and a mobile app,
- assess if the requirements that were set out have effectively been met.

1.2. Deliverable 2.4

The current document, Deliverable 2.4, specifically relates to the “Requirements’ assessment and delivery of website and mobile app of Interactive HandBook” and encompasses:

- A report on the assessment of whether the requirements defined at the beginning of the project are successfully covered by the SMOOTH Platform.

- In addition, this deliverable will report on the delivery of the mobile app and website implementing the SMOOTH interactive handbook. This covers Task 2.3 – SMOOK: Interactive GDPR handbook for micro-enterprises”. Task 2.3 compiles all the requirements defined in T2.1 and the design that was made under Task 2.2. These are translated into the Interactive Handbook that uses simple language for people that do not have any previous background in the area of data protection and privacy.
- A comparison between an assessment performed by the Platform and the assessment of the same case by a human legal expert (the ‘human assessment’).

The tasks under Task 2.3 are divided as follows:

- Legal partners (KUL, DVI and AEPD when they were still part of the project) and partners representing micro-enterprises (ESBA, FBA) were in charge of defining the content of the Handbook.
- LSTECH and UC3M were in charge of implementing the website and mobile app associated with the handbook.

The following information and examples are included as annexes in D2.4:

- The content of the GDPR Handbook:
  o the (full) legal texts, tailored to the needs of the micro-enterprises,
  o graphics, tables, and designs used in the GDPR handbook website and mobile applications,
- Examples and screenshots of pages of both the website and the mobile applications.

The document at hand is an update of the initial version of D2.4, submitted in month 24. The updated parts can be found mainly under chapter 2.3 (for the GDPR Handbook), chapter 3 (the requirements assessment) and chapter 4 (human assessment). The other parts have also been updated where required.

2. The GDPR Handbook (for micro-enterprises)

Throughout the project, SMOOTH has created a GDPR Online Interactive Handbook (“The GDPR Handbook (for micro-enterprises”)”). This Handbook aims to serve as a detailed guide for micro-enterprises to help them understand what the GDPR is, how it affects them and how they can become GDPR compliant. The Handbook includes text, infographics and video material as well as sample reference documents. Although focused on helping the Micro-enterprises, all the information is of-course valid for all the companies. In addition, it includes a quiz, flowcharts and links to external resources that may help micro-enterprises in adopting the GDPR. The Handbook is delivered as a website and a mobile application.

2.1. The requirements of the GDPR Handbook

Deliverables 2.1 and 2.2 divided the requirements for the Handbook into:

a) Legal requirements for micro-enterprises (the content of the Handbook)

Legal requirements for micro-enterprises refer to the GDPR and e-Privacy rules that are most relevant for micro-enterprises’ processing activities. They have been extracted from the text of those legal acts by the project’s legal partners and supplemented by opinions and guidance issued by the Article 29 Working Party (WP29), the European data Protection Board (ADPB) and the Data Protection Authorities (DPAs).
From the experience of the initial two DPAs participating to the project, small organisations mainly carry out low-risk data processing. Therefore, for the purposes of SMOOTH, the consortium has focused on such low-risk data processing, paying less attention GDPR provisions linked to high-risk processing, such as the obligation to conduct a Data Protection Impact Assessment (DPIA).

The SMOOTH partners in charge of drafting these texts are KUL, AEPD and DVI. Taken into account the early departure of AEPD from the SMOOTH project, KUL took over the tasks that were to be provided by AEPD under Task 2.3 and Deliverable 2.4. The text also takes into account the information provided below under “MEnts requirements” insofar such information affects the legal requirements for the Handbook.

The outline and structure of these requirements has been defined in D2.1 and D2.2.

b) MEnts’ requirements for the use of the SMOOTH Platform (the design and accessibility of the Handbook)

Micro-enterprises’ requirements for the SMOOTH Platform have been defined through reaching out to and consulting small companies and their representative organisations. Micro-enterprises were consulted\(^1\) to provide the consortium with useful insights on:

- their current data processing practices *(what types of personal data they process, for which purposes, based on which legal basis)*
- their GDPR-readiness *(have they implemented GDPR requirements and documented their compliance)*
- what they consider as important requirements for the SMOOTH Platform in terms of usability, cost and solutions offered.

Based on their input, the consortium strived to develop solutions that meet their needs – ensuring that micro-enterprises’ requirements for the SMOOTH Platform are met is a considerable step for the success of the project.

These requirements and their feasibility have thus been reviewed and discussed by all members of the consortium.

The SMOOTH-partners in charge of adapting the legal texts written by the legal partners to the needs of the micro-enterprises and the graphic designing of the Handbook are ESBA and FBA. This in close collaboration with the legal partners mentioned above to ensure that the final texts and design are still accurate GDPR guidance.

c) Technical requirements for the SMOOTH Platform

The technical partners for Deliverable 2.4, UC3M and LSTECH, developed the SMOK website (LSTECH) and mobile app (UC3M). They did so by using their experience and state of the art technology.

The following part, section 2.2, describes how these requirements have been implemented, while section 2.3 addresses the updates that have happened in the final version of D2.4.

---
\(^1\) See D2.1, Chapter 3.1 for more detailed information on the consultation held with micro-enterprises.
2.2. Practical implementation

2.2.1. Legal requirements for micro-enterprises

The legal requirements to be included in the Handbook were defined by the legal partners KUL, DVI and AEPD under Task 2.1, in collaboration with all SMOOTH-partners and were reported on in Deliverable D2.1.

The content and the structure of the GDPR Handbook were outlined in D2.3, in which the following topics were identified:

- Does the GDPR apply to my company?
- Is my company allowed to process personal data?
- Is my company a data controller or a data processor?
- Data protection principles
- Which rights do my data subjects have?
- Where to start compliance?
- Consequences of GDPR non-compliance
- When to still check national law?
- Should I carry out a DPIA?
- Should I appoint a DPO?
- Data breaches: what now?
- The role of the ePrivacy Regulation
- Specific processing situations
  - Customers’ personal data
  - Suppliers’ personal data
  - Data protection in an employment context
  - Camera surveillance
  - Direct marketing
  - Health data
  - Websites: cookies and other tracking technologies
  - Social media to promote my business
  - A waterproof privacy policy
  - Consent and children’s data
- GDPR compliance toolbox
- Test your GDPR and ePrivacy literacy
- GDPR glossary

All these topics have been covered and the text has been reviewed and amended by the design partners FBA and ESBA to make sure that accessible and intelligible language is used, tailored to the needs of micro-enterprises.

An issue occurred in regard of implementing information on the ePrivacy Regulation: this regulation has still not been approved and it is unsure at this moment when it will be approved and what the content of the regulation will be. Therefore, we have chosen to not add these obligations into the Handbook.
The GDPR compliance toolbox refers to publicly available and freely usable (at least CC BY-NC-SA) templates of:

<table>
<thead>
<tr>
<th>Template</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legitimate Interest Assessment (LIA) Template</td>
<td><a href="#">here</a></td>
</tr>
<tr>
<td>Pre-DPIA Template</td>
<td><a href="#">here</a></td>
</tr>
<tr>
<td>DPIA Template</td>
<td><a href="#">here</a> (in Latvian), <a href="#">here</a> (in English), <a href="#">CNIL Tool</a> (in French and English)</td>
</tr>
<tr>
<td>Example of a good cookie policy</td>
<td><a href="#">here</a></td>
</tr>
<tr>
<td>Record of processing activities</td>
<td><a href="#">ICO examples</a> (in English)</td>
</tr>
<tr>
<td>Privacy policy</td>
<td><a href="#">template from IAPP</a> (in English)</td>
</tr>
</tbody>
</table>

The full texts are annexed to this Deliverable:

- Annex I: Final text version of the GDPR handbook mobile application, graphic design included
- Annex II: Final text version of GDPR handbook website, with graphic design included

### 2.2.2. Micro-enterprises’ requirements for the Handbook

The design and implementation of the Handbook required the involvement of a multidisciplinary team combining legal expertise and deep knowledge of the GDPR (DVI, KUL) with technical expertise (UC3M and LSTECH) under a clear perspective of the micro-enterprises’ necessities (ESBA, FBA).

ESBA and FBA’s role was to ensure that the language and overall content was made as comprehensible as possible for entrepreneurs to efficiently assimilate and successfully use the Handbook, in accordance with the usability requirements defined in D.2.2 (T2.3).

A final tree structure and complete content for the desktop and the mobile version of the handbook have been agreed and shared. Decisions were also taken with regards to layout and design.

The infographics had been designed but were not all implemented yet (M24).

The videos were the latest inputs to be conceived. Due to a shift in the task’s responsibilities between ESBA and FBA, they were in the making in M24 and were going to be made available to the technical partners for a final integration as soon as possible.

The then (and still) current COVID-19 crisis inevitability had consequences on the videos’ deliverable. The constrain of a full ‘homeworking’ environment had obliged FBA and ESBA to review
the original strategy behind the videos and switch from a “live-video” to full “animation”. Requiring therefore more work and time.

The full texts, including directions for the design and parts of the graphics were annexed to this Deliverable:

- Annex I: Final text version of SMOOK mobile application, graphic design partly included
- Annex II - Final text version of SMOOK website application, with graphic design partly included

2.2.3. Technical requirements

2.2.3.1. The GDPR Handbook Mobile App

a. Implementation overview

UC3M is the partner in charge of the development of the mobile app version of the Handbook. For this task, UC3M has followed the guidelines provided by those partners in charge of the design of the app and creating the content: ESBA, FBA and KUL, in accordance with D.2.2 and T2.3.

During the development the partners involved have been in a continuous interaction process to be sure the information required was properly transmitted and understood.

The initial commitment was developing the app for Android, but UC3M has worked towards having the mobile app also available for iOS. This objective has significantly increased the complexity of the development, which has meant a significant increase of the resources and time initially planned for this task.

UC3M has used three different frameworks to develop the GDPR Handbook app: Apache Cordova, AngularJS and Ionic 4, each of them covering a specific requirement of the app. UC3M has looked for open-source frameworks in order to reduce as much as possible the cost of the development. Following, we briefly describe the functionality provided for each of these frameworks during the development:

- **Apache Cordova**: It is an open-source framework for mobile app development. It allows using standard web technologies such as HTML5, CSS3 and Javascript. These technologies allow multiplatform development that avoids the requirement of using native development languages from each mobile platform. The apps run isolated in each platform and use standard APIs to access the sensors, data, and network status in each platform. In particular in the context of SMOOK, it is of great value since it allows creating apps for iOS and Android using HTML.

- **AngularJS**: It is an open-source JavaScript framework provided and maintained by Google. It is used to create and keep web applications within a single page. The main goal is increasing the number of applications based on browser that include Mode-View-Controller. This facilitates both the development and testing efforts. In the context of SMOOK, this framework has been very useful (beyond its core functionality) because it
allows create and reuse components, and in addition, it allows managing the routes among the different app pages. Since SMOOK app has many different pages the complexity of managing the links among them is high, and AngularJS has allowed us to accomplish that task.

- **Ionic 4:** It is referred to as a complete and open-source SDK (Software Development Kit) for the development of hybrid mobile apps. Ionic provides tools and services to develop hybrid mobile apps using web technologies such as CSS, HTML and Sass (Syntactically awesome style sheets). The apps can be compiled with the referred web technologies. They can be latter distributed across different mobile app stores to be installed in different OSes using Apache Cordova. In the context of SMOOK Ionic 4 has been the tool used to compile the code of the app.

b. Content embedded within the app

The GDPR Handbook app includes natively all the textual content and infographics created by ESBA, FBOX and KUL. That means all this content is embedded within the app. However, for the case of the videos the Mobile app includes a link to their external source, since it is not a good practice embedding videos in an app because they significantly increase the size of the app and its performance. Furthermore, some official stores limit the size of the app that can be uploaded. This could mean that after the development effort we could face the situation in which our app is not accepted in official stores; Even if the app is within the permitted limit, users that sometime have limited storage capacity in their mobile devices may prefer not to install the app due to its size. Therefore, the decision is that the mobile app will link to videos from external sources (e.g., SMOOTH website, Youtube, etc) and once the user clicks on the link will be automatically redirected to those sources. Expert partners within the SMOOTH consortium consider users are used to be redirected to external sources for visualizing video so it will not affect the Quality of Experience in the case of SMOOTH app.

c. App development status

This deliverable includes the final version of the app. It includes all the textual and infographics content, and the links to the videos. In addition, the app has been tested and revised within the consortium to find potential bugs, content errors, etc. In the case new bugs are found or improvements can be made, the partners will try to correct them and upload a new version in the future.

At Annex III, we had added:

- A few screenshots of what the GDPR handbook mobile app looks like
- Links to eight videos (to be viewed online) which demonstrate the functioning and the design of the app.

d. App stores upload plan
The GDPR handbook app is available in the google play store and in the apple store under the following links


2.2.3.2 The GDPR Handbook Website

a. Implementation overview

The GDPR Handbook website has been based on the guidelines provided by ESBA, FBA and KUL, the partners who created and designed the content in accordance with what was defined in D.2.2 and T2.3. The material has been communicated thought the project’s repository and various interactions and conference calls have been carried out to ensure a quality outcome.

For the implementation of the website LSTECH has used the WIX framework which offers a modern UX and easy to maintain web-pages. Whenever needed custom HTML and Javascript code has been developed to provide a better functionality.

The website is hosted under LSTech’s WIX account and it is available under the gdprhandbook.eu domain that the partners have agreed and LSTECH has purchased.

b. Content embedded within the app

The final version of the GDPR Handbook website includes all the textual content and infographics created by ESBA, FBA and KUL. The website also embeds the related videos created for that purpose and are hosted in the project’s Youtube channel (https://www.youtube.com/channel/UCKPNX7SNWjYgwTDIMYH4gw).

c. Website development status

The GDPR handbook website is finalized and it is available in the following address

https://www.gdprhandbook.eu/

It includes all the textual and infographics content and also all the related videos.

Some sample screenshots can be found below, in Annex IV.

2.3. Practical implementation

From the submission of the initial version of D2.4 onwards, the partners involved in the making of the GDPR Handbook have been continuously working to improve and finalise the GDPR Handbook. The changes that were made are mainly based on:

- things that were already scheduled to be done;
- the comments of the reviewers after the second review meeting;
- changes based on feedback and issues identified during the testing of the app (by the partners).

2.3.1. In general

The consortium has agreed to use the name the GDPR Handbook (for micro-enterprises) instead of SMOOK, because it is more representative and because the word “SMOOK” does not have an attractive meaning.

Every partner involved in the creation of the GDPR Handbook was able to provide feedback on the first version(s) of the website and mobile app. This feedback was collected and concerned typo’s, punctuation, layout, overlaps, small structural changes, etc. This feedback was taken into account and addressed by the partners to deliver the final version.

Below, we describe specific changes that were implemented. Some of them were already planned, while others follow from the recommendations made after our second review meeting.

2.3.2. Interactivity: flowcharts

In addition to the GDPR quiz and internal and external links within the Handbook, we have improved interactivity of the GDPR Handbook, such as by adding interactive flowcharts.

2.3.2.1. Flowchart a: territorial application of the GDPR

2.3.2.2. Flowchart b: do I need to appoint a DPO?
2.3.3. Multilinguality

2.3.3.1. Desktop version

Although the initial plan was to provide the handbook only in English, the consortium decided to also provide it in Latvian. Furthermore, it is planned to have it translated in Greek in the near future.

To support other languages, we have added a related page where we guide users to GDPR related sources in other languages and also offer a google translate option.

An icon showing different flags has been added at the end of the menu bar at the top of the landing page:

This icon symbolizes the place to go for the owners of small companies who do not speak English (very well). Clicking on this icon redirects them to a new page where there are two things to be found:

- A link to the website of the European Data Protection Board where GDPR-related content in any EU language can be found.
- The possibility to obtain a Google translate version of the entire Handbook.²

2.3.3.2. Mobile app

The same icon (see first image 3.1) showing different flags has also been added to the mobile app in order to link visitors to the website of the European Data Protection Board where they can find GDPR-related content in any EU language.

![Screen shot of the mobile app with Google Translate icon](image)

There will not be a possibility to obtain a Google translate version of the Handbook via the mobile app because automatic translation is not possible in the app.

2.3.4 Additional examples

All the examples in the handbook were given a uniform layout to easily spot them. To see what the examples look like, see the screenshot below:

² It seems that google does not support the embedding of the translator service, see: [https://translate.google.com/intl/en/about/website/](https://translate.google.com/intl/en/about/website/). Instead, we added a link to the “home” of the Google translator page. The result looks like the following: [https://translate.google.com/translate?hl=en&sl=en&tl=it&u=https%3A%2F%2Fstechltd1.wixsite.com%2Fgdp](https://translate.google.com/translate?hl=en&sl=en&tl=it&u=https%3A%2F%2Fstechltd1.wixsite.com%2Fgdp).
We have also added some extra examples to the GDPR Handbook to make the theoretical content more tangible.

**New examples added**

<table>
<thead>
<tr>
<th>Where?</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR Principles &amp; Rights</td>
</tr>
<tr>
<td>Persons’ rights</td>
</tr>
<tr>
<td>How to respond?</td>
</tr>
</tbody>
</table>

A company stores certain personal data in coded form, intelligible for those who do not have the key. Upon receiving an access request from an individual concerned, the company provides that individual with the coded information, without any further explanation. This practice is not GDPR compliant! Information needs to be provided in a manner that is understandable by an average person.

A real estate agency processes personal data of its clients (name, date and place of birth, address) to conduct a client analysis in light of money laundering. Under the GDPR, real estate agencies can justify this personal data processing based on the legal obligation to which they are subject in the money laundering law.

A company mistakenly sends marketing communication to an individual who happens to be part of the company’s customer database. Upon receiving this marketing communication, the individual reaches out to the company, requesting more information on how his data had been obtained, what type of personal data the company holds on him and the legal basis relied upon by the defendant to process his data. The company ignores this request and continues to send marketing communications. This is not in line with the GDPR. If the company does not respond to the request within a period of 1 month, it can be fined by the competent national data protection authority.
A company manages a customer database storing personal data for the purpose of commercial communication. All individuals in this database have provided their consent to the use of their data for commercial purposes. Now, the company plans to make further use of the data stored to keep statistics on customers’ buying behaviour, without asking for their consent. In principle, as this is a different purpose than marketing, the company would need to rely on another legal basis for this processing. However, the GDPR explicitly considers the keeping of statistics as a compatible purpose. The company will have to put in place appropriate safeguards to protect the individuals’ rights and freedoms (i.e., technical and organisational measures such as pseudonymisation).

<table>
<thead>
<tr>
<th>GDPR Principles &amp; Rights</th>
<th>2. Purpose limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR principles</td>
<td></td>
</tr>
</tbody>
</table>

2.3.5. Videos

To keep the readers interested and entertained, we have replaced some textual parts of the Handbook by videos. Four animated videos have been added to the Handbook. The topics covered are:

- What are personal data? (watch here)
- Controller or processor? (watch here)
- Legitimate interest(s) (watch here)
- Social media pages (watch here)

A screenshot is added below to give an impression of the look and feel of the videos:
Additionally, a fifth video is added to the section ‘Compliance – where to start?’. This video is a recording of a webinar that was given by KUL in light of the SMOOTH-Project. This webinar – entitled “5 GDPR Commandments for Small Businesses” – aims to assist small companies in their struggle with the GDPR.

The video of the webinar is embedded on the website, but for the mobile app, a link is provided to the YouTube video of this webinar.

2.3.6. Availability mobile app

As mentioned above, UC3M has posted the Handbook app to both the Google and Apple store and several updates have been published in the meantime. Links are provided to the download pages for the apps in the Apple and Google Store on the SMOOTH website and on the GDPR handbook website.

2.3.7. Testing

The testing is part of WP7. We have gathered a small group of micro-enterprises engaged in different activities who wanted to act as testers of the GDPR Handbook. The testing has taken place by means of an app version and a web version survey, led by FundingBox, with overall positive results (please find more detailed survey results in deliverables D7.4 and D9.4).

2.3.8. Incorporation of the SMOOTH Community on the FundingBox Platform

To boost interactivity of the GDPR Handbook the public version of the Smooth Community on the FundingBox platform has been embedded in the handbook as an additional source of information and if needed a discussion forum where the SMEs can ask each other for help and exchange tips and tricks. It has the form of an incorporated newsfeed, where people can see any posts that are...
made in the main space (comparable to a Twitter feed that can be found on many websites). The public version of the Smooth Community on the FundingBox platform, is the version that is currently visible to any user of the internet via the following url: [url]. In order to actively participate in the conversation by posting, the user has to click through to the FundingBox platform and sign up for it (a very simple process in order to create a username, just like in any other forum). This element will ensure interactivity within the handbook after the end of the SMOOTH project and with it support sustainability.

2.3.9. Translation

Later on, we can still reach out to the EDPS/EDPB to disseminate the Handbook across the data protection authorities (DPAs) and discuss translation of the GDPR Handbook into different languages.

3. The requirements assessment

This section entails a reporting of the assessment of whether the requirements defined at the beginning of the project – in D2.1 – are successfully covered by the SMOOTH Platform. This assessment is done per work package, as you can see below.

It also contains the outcome of the ‘human assessment’, in which a case analyzed by the SMOOTH platform has also been assessed by a human GDPR expert.

3.1. WP2: assessment of the legal requirements

- Organizations: KUL and DVI
- WP: 2
- Name of the person(s) completing this document: Nadia Feci (KUL) and Brahim Bénichou (KUL)

3.1.1. Initial requirements

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O³</th>
<th>Subject</th>
<th>Legislation</th>
<th>Description</th>
<th>Type of implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-Dev-1</td>
<td>M</td>
<td>Material scope</td>
<td>GDPR, Art. 2</td>
<td>Internal assessment of the types of data to be processed during the Platform’s development, to determine the processing or not of personal data.</td>
<td>Pre-processing internal analysis</td>
</tr>
</tbody>
</table>

³ O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).
<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O¹</th>
<th>Subject</th>
<th>Legislation</th>
<th>Description</th>
<th>Type of implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-Dev-2</td>
<td>M</td>
<td></td>
<td></td>
<td>Internal assessment of the types of data to be processed during the Platform’s development, to determine the processing or not of sensitive personal data.</td>
<td>Pre-processing internal analysis</td>
</tr>
<tr>
<td>SP-Dev-3</td>
<td>M</td>
<td></td>
<td></td>
<td>Allocation of different roles and responsibilities of partners for data processing (controller, processor, joint controllers).</td>
<td>Pre-processing internal analysis</td>
</tr>
<tr>
<td>SP-Dev-4</td>
<td>M</td>
<td>Lawfulness</td>
<td>GDPR, Arts. 5(1)(a), 6 and 7</td>
<td>There is an appropriate legal basis for processing operations during the Platform’s development.</td>
<td>Pre-processing internal analysis</td>
</tr>
<tr>
<td>SP-Dev-5</td>
<td>M</td>
<td></td>
<td></td>
<td>Where data is processed on the basis of consent, processing can only start following a clear affirmative act of the individual concerned.</td>
<td>Informed consent process</td>
</tr>
<tr>
<td>SP-Dev-6</td>
<td>M</td>
<td></td>
<td></td>
<td>Where data is processed on the basis of consent, consent is informed and meets the GDPR requirements for valid consent.</td>
<td>Informed consent process</td>
</tr>
<tr>
<td>Requirement name</td>
<td>O</td>
<td>Subject</td>
<td>Legislation</td>
<td>Description</td>
<td>Type of implementation</td>
</tr>
<tr>
<td>------------------</td>
<td>---</td>
<td>---------</td>
<td>-------------</td>
<td>-------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>SP-Dev-7</td>
<td>M</td>
<td></td>
<td></td>
<td>Where data is processed on the basis of consent, there is a process allowing individuals to withdraw their consent.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-8</td>
<td>M</td>
<td></td>
<td></td>
<td>Where data is processed on the basis of consent, there is a process allowing the erasure of personal data of individuals who withdraw their consent to the processing.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-9</td>
<td>M</td>
<td></td>
<td></td>
<td>Where data is processed on the basis of legitimate interests, processing can only start following a LIA demonstrating that the rights of data subjects are not overridden.</td>
<td>Pre-processing internal analysis</td>
</tr>
<tr>
<td>SP-Dev-10</td>
<td>M</td>
<td></td>
<td></td>
<td>Where data is processed on the basis of legitimate interests, there is a process allowing individuals to object to the processing.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-11</td>
<td>M</td>
<td>Purpose limitation</td>
<td>GDPR, Art. 5(1)(b)</td>
<td>(Sufficiently specified, explicit and legitimate) purposes have been identified before the start of</td>
<td>Pre-processing internal analysis</td>
</tr>
<tr>
<td>Requirement name</td>
<td>O</td>
<td>Subject</td>
<td>Legislation</td>
<td>Description</td>
<td>Type of implementation</td>
</tr>
<tr>
<td>------------------</td>
<td>---</td>
<td>------------------------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>SP-Dev-12</td>
<td>M</td>
<td></td>
<td></td>
<td>Data may be further processed by SMOOTH only for purposes compatible with the original collection purpose and within the reasonable expectations of data subjects. A purpose compatibility assessment needs to be carried out before any further processing takes place.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-13</td>
<td>M</td>
<td>Data minimisation</td>
<td>GDPR, Art. 5(1)(c)</td>
<td>Personal data processed during the Platform’s development are limited to what is necessary to accomplish the (specified) purposes of processing.</td>
<td>Pre-processing internal analysis</td>
</tr>
<tr>
<td>SP-Dev-14</td>
<td>M</td>
<td>Accuracy</td>
<td>GDPR, Art. 5(1)(d)</td>
<td>There are processes to record the source of personal data and to provide data subjects the right to rectify their data.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-15</td>
<td>M</td>
<td>Storage limitation</td>
<td>GDPR, Art. 5(1)(e)</td>
<td>The consortium defines an appropriate retention period for personal data. Personal data are</td>
<td>Pre-processing internal analysis; Internal organisational process</td>
</tr>
<tr>
<td>Requirement name</td>
<td>O1</td>
<td>Subject</td>
<td>Legislation</td>
<td>Description</td>
<td>Type of implementation</td>
</tr>
<tr>
<td>------------------</td>
<td>----</td>
<td>---------</td>
<td>-------------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>SP-Dev-16</td>
<td>M</td>
<td></td>
<td></td>
<td>not stored for longer than is necessary to achieve the processing purposes defined by the consortium.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-17</td>
<td>M</td>
<td>Security</td>
<td>GDPR, Arts. 5(1)(f), 32 and 34</td>
<td>A prior assessment of the risks associated to the processing is made to establish the risk levels and define precautionary actions.</td>
<td>Pre-processing internal analysis</td>
</tr>
<tr>
<td>SP-Dev-18</td>
<td>M</td>
<td></td>
<td></td>
<td>Physical and digital security measures are implemented.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-19</td>
<td>R</td>
<td></td>
<td></td>
<td>Data obfuscation techniques to mitigate the threat posed by accidental disclosure of data are implemented – the consortium will consider the techniques of cross-tabulation, data swapping and salting, depending on the needs of the database</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>Requirement name</td>
<td>O</td>
<td>Subject</td>
<td>Legislation</td>
<td>Description</td>
<td>Type of implementation</td>
</tr>
<tr>
<td>------------------</td>
<td>---</td>
<td>---------</td>
<td>-------------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>SP-Dev-20</td>
<td>M</td>
<td>Legislation</td>
<td></td>
<td>Exchange of personal data among partners is handled by a separate sharing service that is secure and in which data are encrypted to ensure maximum security during transmission.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-21</td>
<td>R</td>
<td></td>
<td></td>
<td>Databases containing sensitive personal data are encrypted.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-22</td>
<td>R</td>
<td></td>
<td></td>
<td>Personal data used during the Platform’s development are destroyed after analysis: data marked for destruction are securely erased using the latest industry standard technique, such as the recommendations of NIST 800-80 R1.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-23</td>
<td>M</td>
<td></td>
<td></td>
<td>Personal data breaches are notified to the Spanish Data Protection Agency where required under Art. 34 GDPR.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-24</td>
<td>M</td>
<td>Accountability</td>
<td>GDPR, Arts. 5(1), 28 and 30</td>
<td>EURECAT as data controller has the responsibility to ensure and</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>Requirement name</td>
<td>O³</td>
<td>Subject</td>
<td>Legislation</td>
<td>Description</td>
<td>Type of implementation</td>
</tr>
<tr>
<td>------------------</td>
<td>----</td>
<td>---------</td>
<td>-------------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>demonstrate compliance with the GDPR.</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>Where data processing is carried out by other partners (processors) or third parties (processors or sub-processors) there are processing contracts in place.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-25</td>
<td>M</td>
<td></td>
<td></td>
<td>EURECAT as data controller and other partners involved in the processing of personal data as data processors keep records of processing activities as required by Art. 30(1) and (2).</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-26</td>
<td>M</td>
<td>Data subjects’ rights: information</td>
<td>GDPR, Arts. 13-14</td>
<td>Privacy policies are established to ensure that personal data are processed in a manner transparent to the data subjects. Privacy policies include all the information required under Arts. 13 and 14, are drafted in a clear and concise manner and are easily accessible.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>Requirement name</td>
<td>O</td>
<td>Subject</td>
<td>Legislation</td>
<td>Description</td>
<td>Type of implementation</td>
</tr>
<tr>
<td>------------------</td>
<td>---</td>
<td>---------</td>
<td>-------------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>SP-Dev-27</td>
<td>M</td>
<td>Data subjects’ rights: access</td>
<td>GDPR, Art. 15</td>
<td>There are processes enabling individuals to obtain access to their personal data and to obtain a free copy. Access to personal data must not negatively affect the rights and freedoms of other individuals — therefore, there should be processes to filter out information concerning other persons.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-28</td>
<td>M</td>
<td>Data subjects’ rights: rectification</td>
<td>GDPR, Art. 16</td>
<td>There are processes enabling individuals to rectify (directly) or request the rectification of inaccurate personal data.</td>
<td>Internal organisational process</td>
</tr>
</tbody>
</table>
| SP-Dev-29        | M | Data subjects’ rights: erasure | GDPR, Art. 17 | There are processes enabling individuals to request erasure of their personal data if:  
  - Individuals withdraw their consent to the processing  
  - Individuals object to the processing and there are no | Internal organisational process |
<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O</th>
<th>Subject</th>
<th>Legislation</th>
<th>Description</th>
<th>Type of implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-Dev-30</td>
<td>M</td>
<td>Data subjects’ rights: restriction of processing</td>
<td>GDPR, Art. 18</td>
<td>There are processes enabling individuals to request restriction of processing where one of the grounds mentioned in Art. 18 GDPR applies.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-31</td>
<td>M</td>
<td>Data subjects’ rights: data portability</td>
<td>GDPR, Art. 20</td>
<td>Where processing is: i) based on consent and ii) carried out by automated means, there are processes enabling individuals to receive their personal data in a commonly used electronic form.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>Requirement name</td>
<td>O¹</td>
<td>Subject</td>
<td>Legislation</td>
<td>Description</td>
<td>Type of implementation</td>
</tr>
<tr>
<td>------------------</td>
<td>----</td>
<td>---------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>SP-Dev-32</td>
<td>M</td>
<td>Data subjects’ rights: Object</td>
<td>GDPR, Art. 21</td>
<td>There are processes enabling individuals to object to the processing carried out by SMOOTH on the basis of ‘legitimate interests’. SMOOTH no longer processes this data unless there are compelling grounds for the processing which override the interests and rights of the particular data subject.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-Dev-33</td>
<td>M</td>
<td></td>
<td></td>
<td>There are processes enabling individuals to object to processing for direct marketing purposes. After receiving an objection, personal data are not processed for direct marketing purposes.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-EXP-1</td>
<td>M</td>
<td>Relationship in data processing</td>
<td>NA</td>
<td>Determine the project partner that will take over the Platform’s exploitation.</td>
<td>Pre-processing internal analysis</td>
</tr>
<tr>
<td>SP-EXP-2</td>
<td>M</td>
<td></td>
<td></td>
<td>Project partner has the role of processor, processing personal data on behalf of MEnts’</td>
<td>Pre-processing internal analysis</td>
</tr>
</tbody>
</table>
### Requirement Assessment (final version)

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O</th>
<th>Subject</th>
<th>Legislation</th>
<th>Description</th>
<th>Type of implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-EXP-3</td>
<td>M</td>
<td>Data processing clauses</td>
<td>GDPR, Art. 28(3)</td>
<td>There is a data processing agreement between the partner responsible for exploitation (processor) and the MEnts wishing to use the SMOOTH Platform (controllers). Data processing clauses have to be accepted by the MEnts as part of the terms of use of the Platform. They include all the information required under Art. 28(3).</td>
<td>Contractual terms</td>
</tr>
<tr>
<td>SP-EXP-4</td>
<td>M</td>
<td>Records of processing activities</td>
<td>GDPR, Art. 30(2)</td>
<td>Partner responsible for exploitation, as data processor, keeps records of processing activities as required by Art. 30(2).</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-EXP-5</td>
<td>M</td>
<td>Security</td>
<td>GDPR, Arts. 32 and 34</td>
<td>Partner responsible for exploitation, as data processor, implements appropriate security measures.</td>
<td>Internal organisational process</td>
</tr>
<tr>
<td>SP-EXP-6</td>
<td>M</td>
<td></td>
<td></td>
<td>Partner responsible for exploitation, as data processor,</td>
<td>Internal organisational process</td>
</tr>
</tbody>
</table>
### 3.1.2. Modified requirements

No requirements have been modified.

### 3.1.3. Requirements that are/will be covered

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O</th>
<th>Description</th>
<th>Coverage Level / Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Development phase</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP-Dev-1</td>
<td>M</td>
<td>Internal assessment of the types of data to be processed during the Platform’s development, to determine the processing or not of personal data.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The categories of personal data used by NEC are the following: taxId, socialSecurity, email, postalAddress, name, phoneNumber</td>
</tr>
<tr>
<td>SP-Dev-2</td>
<td>M</td>
<td>Internal assessment of the types of data to be processed during the Platform’s development, to determine the processing or not of sensitive personal data.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NEC didn’t use actual sensitive data to develop the Platform (train the algorithms), only synthetic data. The special</td>
</tr>
<tr>
<td>SP-Dev-3</td>
<td>M</td>
<td>Allocation of different roles and responsibilities of partners for data processing (controller, processor, joint controllers).</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>---</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FULLY COVERED</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Several discussions on this matter have been held between the legal partners of the project (AEPD, KUL and DVI). It was agreed that for the task of developing the algorithm in WP4, NEC and EUT are separate controllers, each one developing their own algorithms. At the initial step of the data life cycle, when the data is disclosed from micro-enterprises to them, EUT provided a data exchange platform for NEC and themselves. For this initial step, EUT acted as processor for NEC and only for this phase, a controller (NEC) – processor (EUT) agreement was drafted. For all other processing that is done during the development phase EUT is the controller.</td>
<td></td>
</tr>
</tbody>
</table>
(From the start of the market validation during the final months of the project, EUT will be seen as the processor and the micro-enterprises using the platform will be the controllers.)

Other consortium members did not get access to the processed personal data. Consequently, there are no other processors or controllers of this data.

<table>
<thead>
<tr>
<th>SP-Dev-4</th>
<th>M</th>
<th>There is an appropriate legal basis for processing operations during the Platform’s development.</th>
<th>FULLY COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>The legal partners (AEPD, KUL and DVI) discussed this and agreed to rely on Recital 50 jo. Article 89 GDPR (further processing for research purposes). AEPD, being the project’s DPO and responsible data protection authority confirmed the validity hereof.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SP-Dev-5</th>
<th>M</th>
<th>Where data is processed on the basis of consent, processing can only start following a clear affirmative act of the individual concerned.</th>
<th>FULLY COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>We have put in place a participation agreement to be signed by the micro-enterprises who join as testers. Do note that the only personal data that is processed relying on the legal basis of consent is personal data from the micro-enterprises acting as testers. This is very little personal data that is moreover strictly related to a professional context. The data that are asked from these participants are e-mail, username, company, country, and language.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SP-Dev-6</th>
<th>M</th>
<th>Where data is processed on the basis of consent, consent is informed and meets the GDPR requirements for valid consent.</th>
<th>FULLY COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Participation agreement.</td>
<td></td>
</tr>
<tr>
<td>SP-Dev-7</td>
<td>M</td>
<td>Where data is processed on the basis of consent, there is a process allowing individuals to withdraw their consent.</td>
<td>FULLY COVERED Participation agreement.</td>
</tr>
<tr>
<td>-----------</td>
<td>---</td>
<td>----------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SP-Dev-8</td>
<td>M</td>
<td>Where data is processed on the basis of consent, there is a process allowing the erasure of personal data of individuals who withdraw their consent to the processing.</td>
<td>FULLY COVERED We have not yet had such a request but there is a process and the withdrawal is possible.</td>
</tr>
<tr>
<td>SP-Dev-11</td>
<td>M</td>
<td>(Sufficiently specified, explicit and legitimate) purposes have been identified before the start of processing operations</td>
<td>FULLY COVERED The purpose underlying the processing activities in the development phase is scientific research. It was decided by the consortium members (including the legal partners KU Leuven, DVI and AEPD, who at the time acted as DPO), that such processing could lawfully take place under Recital 50 GDPR, together with art. 89 GDPR. The applicable conditions therefore were agreed upon.</td>
</tr>
</tbody>
</table>
| SP-Dev-13 | M | Personal data processed during the Platform’s development are limited to what is necessary to accomplish the (specified) purposes of processing. | FULLY COVERED The consortium only collects personal data which are necessary and proportionate to achieve the specific purpose of the research.

SMOOTH is respecting the data minimisation principle in multiple ways:

- In order to be able to identify the nature of the different data sets that micro-enterprises are storing, it is necessary – to the largest extent possible – to have access to the most thorough variety of different data sources. Samples of these different data sources are deployed to train the classification models and to validate them at a later stage. Partners have committed to |
| SP-Dev-14 | M | There are processes to record the source of personal data and to provide data subjects the right to rectify their data. | FULLY COVERED
This is possible, however, we did not yet receive such a request. |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-Dev-15</td>
<td>M</td>
<td>The consortium defines an appropriate retention period for personal data. Personal data are not stored for longer than is</td>
<td>FULLY COVERED</td>
</tr>
</tbody>
</table>
necessary to achieve the processing purposes defined by the consortium.

Such a retention period has been defined in the participation agreement: “…to not store the Data longer than required under this Agreement and to, in any case, delete the Data within 6 months after the completion of the Project;”

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-Dev-16</td>
<td>M</td>
<td>All personal data are anonymised or securely deleted after completion of the project (end of the SMOOTH Platform development phase)</td>
</tr>
<tr>
<td>SP-Dev-17</td>
<td>R</td>
<td>A prior assessment of the risks associated to the processing is made to establish the risk levels and define precautionary actions.</td>
</tr>
</tbody>
</table>

**WILL BE COVERED** (See previous requirement)

**FULLY COVERED**

Within the framework of carrying out a prior assessment of risk and identification of precautionary actions proportional to the potential risk/harm in the project, SMOOTH has requested and obtained the necessary clearance from Comitè Ètic d’Investigació amb medicaments⁴ in light of the validation and assessment procedure envisaged under Task 7.2. (See Annex II D9.2)

In the first year of the project, we have conducted a preliminary assessment to decide on the necessity for SMOOTH’s processing activities to be made subject to a data protection impact assessment (DPIA) under the GDPR. (See Annex I of D9.2 for the actual assessment) It is good practice to conduct such a preliminary assessment to ascertain, map and minimize potential risks to

---

⁴ The CEIm is an independent interdisciplinary body made up by health professionals and other non-medical staff and it safeguards the protection of the rights, safety and well-being of the participants of clinical trials. Its approval of trial protocols constitutes a public guarantee of the aforementioned. It also assures the staff are adequately qualified, the installations adequate and the documents informing the patient subjects of the nature of the study are well redacted so that the patient consent is valid. For more information: [https://www.iis.lafe.es/en/iis-la-fe/governing-bodies/ethics-committees/medicaments-research-ethics-committee-ceim/](https://www.iis.lafe.es/en/iis-la-fe/governing-bodies/ethics-committees/medicaments-research-ethics-committee-ceim/)
the envisaged data processing activities. The outcome of this assessment was that, at the time, no DPIA was needed. The pre-DPIA was reviewed for the second year of the project: still no DPIA was needed.

In the third year, a DPIA was performed which concluded that the market pilot could take place without additional security measures besides those that were already in place.

<table>
<thead>
<tr>
<th>SP-Dev-18</th>
<th>M</th>
<th>Physical and digital security measures are implemented.</th>
<th>FULLY COVERED</th>
</tr>
</thead>
</table>
|           |   | The legal partners have engaged in conversations with NEC and EUT – the two consortium members that will have access to personal data in the development phase of project – to ensure that security measures they envisage are in line with the GDPR. EUT and NEC are both companies with extensive experience in processing personal data on a large scale and do comply with state-of-the-art security requirements, both technically and organisationally. The collected data will be kept in secure servers, only accessible to them and their processors.

For a more detailed description of the security measures committed to by EUT and NEC, please see D9.2 p. 28-29.

It’s also worth mentioning that both NEC and EUT have their own DPO’s who also safeguard the GDPR compliant and secure processing by them of personal data. |
| SP-Dev-20 | M | Exchange of personal data among partners is handled by a separate sharing service that is secure and in which data are encrypted to ensure maximum security during transmission. | FULLY COVERED  
EUT has provided a secure file exchange platform to allow the transfer of the personal data from the micro-enterprises to NEC whenever this was needed for training, testing, and debugging purposes. The exchange platform serves as a means to collect the personal data from the micro-enterprises, and to transmit that data to NEC. The data is securely erased from the exchange platform once it is stored on the controller servers. |
| --- | --- | --- | --- |
| SP-Dev-24 | M | EURECAT as data controller has the responsibility to ensure and demonstrate compliance with the GDPR. | FULLY COVERED  
EUT is able to demonstrate GDPR compliance. |
| | M | Where data processing is carried out by other partners (processors) or third parties (processors or sub-processors) there are processing contracts in place. | FULLY COVERED  
We have put in place a data processing agreement between EUT and NEC, regulating the data sharing and processing practices in the development phase of the Platform. |
| SP-Dev-25 | M | EURECAT as data controller and other partners involved in the processing of personal data as data processors keep records of processing activities as required by Art. 30(1) and (2). | FULLY COVERED  
Only NEC and EUT have processed personal data used for the development of the Platform, both as data controllers. They both have registered these processing activities in their records of data processing activities, as verified with their respective DPO’s. |
| SP-Dev-26 | M | Privacy policies are established to ensure that personal data are processed in a manner transparent to the data subjects. Privacy policies include all the information required under Arts. 13 and 14, are drafted | FULLY COVERED  
The processing of personal data for the development of the Platform is regulated by the participation agreement and the |
<table>
<thead>
<tr>
<th>SP-Dev-27 M</th>
<th>There are processes enabling individuals to obtain access to their personal data and to obtain a free copy. Access to personal data must not negatively affect the rights and freedoms of other individuals – therefore, there should be processes to filter out information concerning other persons.</th>
<th>FULLY COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>At the start of the project, the legal partners addressed this requirement with NEC and EUT. It was confirmed that, upon receiving such a request, they would be able to grant it. This is included in the participation agreement. However, we have not yet received such a request.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SP-Dev-28 M</th>
<th>There are processes enabling individuals to rectify (directly) or request the rectification of inaccurate personal data.</th>
<th>FULLY COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>At the start of the project, the legal partners addressed this requirement with NEC and EUT. It was confirmed that, upon receiving such a request, they would be able to grant it. This is included in the participation agreement. However, we have not yet received such a request.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SP-Dev-29 M</th>
<th>There are processes enabling individuals to request erasure of their personal data if: - Individuals withdraw their consent to the processing - Individuals object to the processing and there are no overriding legitimate grounds for processing - Data is no longer necessary for the purposes for which they were collected and processed.</th>
<th>FULLY COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>At the start of the project, the legal partners addressed this requirement with NEC and EUT. It was confirmed that, upon receiving such a request, they would be able to grant it. This is included in the participation agreement.</td>
<td></td>
</tr>
</tbody>
</table>
There are processes to securely delete personal data from both live and back-up systems. However, we have not yet received such a request.

| SP-Dev-30 | M | There are processes enabling individuals to request restriction of processing where one of the grounds mentioned in Art. 18 GDPR applies. FULLY COVERED
|           |   | At the start of the project, the legal partners addressed this requirement with NEC and EUT. It was confirmed that, upon receiving such a request, they would be able to grant it. This is included in the participation agreement. However, we have not yet received such a request. |

### Exploitation phase (from market validation onwards)

| SP-EXP-1  | M | Determine the project partner that will take over the Platform’s exploitation. FULLY COVERED
|           |   | It has been agreed upon that the partner taking over the Platform’s exploitation will be LSTECH. |

| SP-EXP-2  | M | Project partner has the role of processor, processing personal data on behalf of MEnts’ using SMOOTH as SaaS. FULLY COVERED
|           |   | This was covered as from the market pilot phase, where EURECAT and LSTECH became data processors. |

| SP-EXP-3  | M | There is a data processing agreement between the partner responsible for exploitation (processor) and the MEnts wishing to use the SMOOTH Platform (controllers). Data processing clauses have to be accepted by the MEnts as part of the terms of use of the Platform. They include all the information required under Art. 28(3). WILL BE COVERED
|           |   | From the market validation on, we are processors. A data processing agreement will be entered into between LSTECH, EURECAT and the participating MEnts. |

| SP-EXP-4  | M | Partner responsible for exploitation, as data processor, keeps records of processing activities as required by Art. 30(2). FULLY COVERED
|           |   | This requirement is covered by EURECAT and LSTECH. |
### 3.1.4. Requirements that will not be covered

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O</th>
<th>Description</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Development phase</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP-Dev-9 M</td>
<td>Where data is processed on the basis of legitimate interests, processing can only start following a LIA demonstrating that the rights of data subjects are not overridden.</td>
<td>N/A Since we did not process personal data based on the legal basis of legitimate interest, this requirement did not have to be covered.</td>
<td></td>
</tr>
<tr>
<td>SP-Dev-10 M</td>
<td>Where data is processed on the basis of legitimate interests, there is a process allowing individuals to object to the processing.</td>
<td>N/A Since we did not process personal data based on the legal basis of legitimate interest, this requirement did not have to be covered.</td>
<td></td>
</tr>
<tr>
<td>SP-Dev-12 M</td>
<td>Data may be further processed by SMOOTH only for purposes compatible with the original collection purpose and within the reasonable expectations of data subjects. A purpose compatibility</td>
<td>N/A Since we did not ‘further process’ the personal data for any other purpose than research, this requirement did not have to be covered.</td>
<td></td>
</tr>
</tbody>
</table>
### SMOOTH Deliverable 2.4

**Handbook and Requirements Assessment (final version)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Type</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP-Dev-19</td>
<td>R</td>
<td>Data obfuscation techniques to mitigate the threat posed by accidental disclosure of data are implemented – the consortium will consider the techniques of cross-tabulation, data swapping and salting, depending on the needs of the database.</td>
<td>As we are receiving personal data directly from micro-enterprises, it is not feasible to expect from micro-enterprises that they have the capacity to anonymize the data before they hand it to SMOOTH. Furthermore, to achieve the purpose set by the SMOOTH Project, anonymization of personal data is not possible. Anonymisation would take away all utility of the processing activities as it is necessary to retain a link between the research subjects and their personal data: one of the tasks of WP4 is to work on re-identification of individuals based on the data sorted by micro-enterprises. Also note that it concerns a sole recommendation here, and not an obligation.</td>
</tr>
<tr>
<td>SP-Dev-21</td>
<td>R</td>
<td>Databases containing sensitive personal data are encrypted.</td>
<td>N/A</td>
</tr>
<tr>
<td>SP-Dev-20</td>
<td>M</td>
<td>Personal data breaches are notified to the Spanish Data Protection Agency where required under Art. 34 GDPR.</td>
<td>We have not (yet) encountered a data breach, hence no personal data breaches had to be notified to the Spanish DPA. However, the consortium is well aware that if such a breach was to take place in the future, the competent DPA needs to be notified of this immediately.</td>
</tr>
<tr>
<td>SP-Dev-31</td>
<td>M</td>
<td>Where processing is: i) based on consent and ii) carried out by automated means, there are processes enabling individuals to receive their personal data in a commonly used electronic form.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

This requirement relates to the right to data portability, which is not applicable within the context of our project as very few data are collected on the basis of consent. Nevertheless, the partners processing the personal data during the development
3.1.5. Overall compliance

In order to assess micro-enterprises’ compliance with the GDPR and to generate the compliance report and relevant recommendations, the SMOOTH innovations inevitably have to process personal data. This triggers the applicability of the EU framework on data protection and privacy (GDPR and e-Privacy Directive) to the SMOOTH-Platform itself. In light of this, legal requirements for the SMOOTH Platform were identified. These requirements were to be kept in mind and implemented throughout the project. Overall, the requirements have been implemented very well and without many problems. To be able to do this, there were many discussions between the legal and technical partners. Since we are not yet at the end of the project, there are still a number of requirements which are to be implemented in the future. A number of legal requirements were not implemented by the consortium, this is mainly due to the fact that these requirements are not applicable to our data processing activities (so it is not necessary to implement these). Therefore, we can conclude that the legal requirements were successfully addressed.

3.2. WP3: assessment of the technical requirements SMOOTEXT

- Organization: Naver Labs Europe
- WP: 3
- Name of the person(s) completing this document: Matthias Gallé and Jos Rozen
### 3.2.1. Initial requirements

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O(^5)</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP3-1</td>
<td>M</td>
<td>SMOOTH users can upload their privacy policy, cookie policy and terms of use to be analysed, or alternatively an URL Privacy policy URL will not be classified automatically from the high-level domain and should either be provided or uploaded</td>
<td></td>
</tr>
<tr>
<td>R-WP3-2</td>
<td>M</td>
<td>The module will be able to extract most of the GDPR elements in the uploaded text with high precision and recall</td>
<td>See text before for exact numbers</td>
</tr>
<tr>
<td>R-WP3-3</td>
<td>M</td>
<td>The module will be able to handle documents in English and Spanish, as well as Latvian (although less accurate)</td>
<td></td>
</tr>
<tr>
<td>R-WP3-4</td>
<td>M</td>
<td>The module will provide a readability analysis, highlighting ambiguous or overly complicated phrases</td>
<td></td>
</tr>
<tr>
<td>R-WP3-5</td>
<td>R</td>
<td>The interface will provide a feedback tool that allows SMOOTH user to correct the predictions, improving the module and making it more robust to data-distribution shift</td>
<td></td>
</tr>
<tr>
<td>R-WP3-6</td>
<td>M</td>
<td>The module shall be able to process documents fast enough to allow the user to get feedback while on the web-site, in general less than 5 seconds</td>
<td></td>
</tr>
<tr>
<td>R-WP3-7</td>
<td>M</td>
<td>The module shall be able to process documents in text and html format</td>
<td></td>
</tr>
<tr>
<td>R-WP3-8</td>
<td>R</td>
<td>Each prediction shall be associated with a confidence measure, which – depending on the user study – can or not be displayed in the interface</td>
<td></td>
</tr>
</tbody>
</table>

\(^5\) O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).
3.2.2. Modified requirements

**R-WP3-1 & R-WP3-7**: instead of processing HTML document, SMOOTEXT implemented text extractor for PDF and DOCX. It was considered by the consortium that those two are the most common document types used by micro-enterprise.

**R-WP3-3**: in addition to those languages, SMOOTEXT also covers all the languages that are supported by the google translate service, since this is the one used before analyzing the text.

In the project proposal it was indicated that SMOOTEXT would also be able to analyse and assess the terms of use and consent forms of MEnts. SMOOTEXT is technically able to analyse these documents to extract companies but this is not related to the context of the report. The SMOOTH platform can also parse these kinds of documents but since they usually do not include information related to data categories or companies present in the websites, we are not asking the users to upload them and add more questions and increase the time of the questionnaire without adding value on that.

3.2.3. Requirements that are/will be covered

**R-WP3-4**: covered completely, the readability analysis is done at the paragraph level, giving them all a score, and lists the most complicated ones (with the highest score) for a given document.

**R-WP3-6**: the limit of 5 second for extraction from textual elements is fulfilled. Analysis of policies in some other format take more time, due to the additional overhead of extracting the content. Most importantly, the whole platform is now based on asynchronous calls, so each API call comes with a callback URL to provide the result of the analysis by a module to the platform.

**R-WP3-8**: a probability measure is associated with each prediction, permitting its display as-is, or binning in – for example – [confident, low-confidence, no-confidence].

**R-WP3-2** The final set of GDPR elements that are extracted are:

- Right to access personal data
- Right to port personal data
- Right to rectify personal data
- Storage of personal data
- Type of personal data collected
- Target activity of personal data collected

The limitations of what Smootext can do are the following:

- by design, it performs its analyses and extractions only on texts in English but does also translate texts in other languages into English before proceeding with the analysis on the translated text in English. This also helps with the adaptation to a new language and has been shown to give very good results, so this is not a limitation per se;
- it handles docx (Microsoft Word) documents but uses an open-source library to open them, which might struggle on some documents, especially with complicated tables;
- it handles (Adobe) pdf files but uses an open-source libraries to open them, which does struggle on some documents, as this format is quite tricky.

### 3.2.4. Requirements that will not be covered

**R-WP3-5.** The feedback process was not added. It would have required a major re-design of the platform to feedback that information back to the SMOOTEXT module, as well as requiring re-training in order to make use of that additional information. This is not possible with the service infrastructure (in particular, it would require GPU). Also, it would add a non-negligible cognitive overhead to the end-user, in a context where he/she is already exposed to a large quantity of information he/she is not an expert in.

In order to tackle the problem of capturing domain shift, we have instead developed a generic method that is able to predict the performance drop of a new dataset.

### 3.2.5. Overall compliance

The modifications of the requirement where done to ensure compatibility with other work-packages, including the technical modules and the entry questionnaire. While some aspects where dropped (eg: export of data outside EU), many others where added such as handling of PDF and DOCX and one additional language (Italian).

### 3.3. WP4: assessment of the technical requirements SMOODATA

- **Organization:** NEC, EUT
- **WP:** 4
- **Name of the person(s) completing this document:** Roberto González Sánchez, Mathias Niepert, Rohit Kumar

#### 3.3.1. Initial requirements

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP4-1</td>
<td>M</td>
<td>SMOOTH users shall upload their company small databases to the SMOOTH Platform.</td>
<td>The Platform should provide an easy way to upload and analyse data bases below 5mb.</td>
</tr>
</tbody>
</table>

* O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).
### R-WP4-2
**M**  
SMOOTH users can give access to some databases (MySQL) without uploading the whole database.  
The system should be easy to understand for the users.

### R-WP4-3
**M**  
The system should be easy enough to be used for people without computer science knowledge.  
The process should be intuitive and easy. It should provide a wizard-like interface to help the users.

### R-WP4-4
**M**  
The system should provide an easy-to-understand report describing the personal data found by the ML engine.

### R-WP4-5
**M**  
Users from MEnts will be able to identify which attributes of their datasets are able to identify individuals.  
This identification will be based on the algorithms developed in the task T4.2.

### R-WP4-6
**M**  
SMOODATA will be able to remove the attributes identified as personal identifiers, together with potential quasi-identifiers.  
The removal of attributes will be based on generalization and suppression approaches that will consider the different characteristics of the attributes and the business goals identified by the customers.

### R-WP4-7
**R**  
Users from MEnts and allowed third-parties will be able to access to aggregations of the data without any loss in the privacy of individuals.  
The idea is to deliver something similar to Google’s RAPPOR tool, based on differential privacy techniques that allows the analysis of the data while preserving the privacy, but considering the multi modal nature of the data held by MEnts. Moreover, the reduced volume of these datasets might complicate the application of standard techniques without compromising the reliability of the aggregations thus obtained.
### 3.3.2. Modified requirements

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O⁷</th>
<th>Modification</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP4-2</td>
<td>M</td>
<td>SMOOTH users can obtain data from different storing systems such as Mysql databases, and commercial products like Moodle or Prestashop.</td>
<td>Users contacted were not able to provide access to their systems, so, tutorials are provided using the standard methods provided by the system.</td>
</tr>
<tr>
<td>R-WP4-5</td>
<td>M</td>
<td>Users are provided with an indication of the risk of re-identification.</td>
<td>The platform initially proposed was complex for the standard user. Moreover, it required the data to be stored after the compliance report was generated. The new method provides simple information.</td>
</tr>
<tr>
<td>Personal data identified</td>
<td>M</td>
<td>Originally, SMOOTH was designed to detect the data formats identified by the legal partners in D2.1. Those data formats are listed below: Political Opinion Trade Union Membership Religious Beliefs Philosophical Beliefs Racial or Ethnic Origin Health Sexual Life Criminal Offences Administrative Offences TIN-Tax ID number Social Security Number</td>
<td>We decided to limit the platform to the analysis of text. Thus, all the formats that are not text (voice, image, etc.) are excluded from the analysis. This change was made to simplify the platform interface and the interaction with the users that will only upload their database without the need of looking for those kinds of data. Then, a set of categories (including sexual life or health data) are technologically supported (the platform includes the ML algorithms to identify them) but are not included in the final piloting of the platform because they were considered as special categories of personal data (specially protected by GDPR).</td>
</tr>
</tbody>
</table>

⁷ O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).
<table>
<thead>
<tr>
<th>Personal Unique Register</th>
<th>and the ML algorithms require the usage of real data for the training of the solution. A discussion among the DPAs involved in the project concludes that the risk of using such kind of data for training was higher than the possible benefit. However, we note that the algorithms are ready for training if, in the future, the company exploiting the platform decides to include them.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and surname</td>
<td></td>
</tr>
<tr>
<td>Health card</td>
<td></td>
</tr>
<tr>
<td>Postal Address</td>
<td></td>
</tr>
<tr>
<td>Phone number</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
<tr>
<td>Image/Voice</td>
<td></td>
</tr>
<tr>
<td>Electronic Signature</td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td></td>
</tr>
<tr>
<td>Other biometric data</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Data types not supported:</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
<tr>
<td>Image/Voice</td>
<td></td>
</tr>
<tr>
<td>Electronic Signature</td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td></td>
</tr>
<tr>
<td>Other biometric data</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Data types supported by the technology but not included in the testing:</td>
<td></td>
</tr>
<tr>
<td>Trade Union Membership</td>
<td></td>
</tr>
<tr>
<td>Health</td>
<td></td>
</tr>
<tr>
<td>Sexual Life</td>
<td></td>
</tr>
<tr>
<td>Criminal Offences</td>
<td></td>
</tr>
<tr>
<td>Administrative Offences</td>
<td></td>
</tr>
<tr>
<td>Newly added data types:</td>
<td></td>
</tr>
<tr>
<td>E-mail</td>
<td></td>
</tr>
</tbody>
</table>

However, during the development of the project those formats were limited and modified, as following:

Finally, the e-mail address was added to the data identified since the pilots demonstrate that it was one of the most common personal data types owned by MENTs.
### 3.3.3. Requirements that are/will be covered

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O⁹</th>
<th>Description</th>
<th>Coverage Level/ Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP4-1</td>
<td>M</td>
<td>SMOOTH users shall upload their company small databases to the SMOOTH Platform.</td>
<td>Connectors are provided to allow users to upload their databases. Moreover, we provide them with different tutorials that allow them to easily obtain the data from the most common back-end systems.</td>
</tr>
<tr>
<td>R-WP4-3</td>
<td>M</td>
<td>The system should be easy enough to be used for people without computer science knowledge.</td>
<td>The process is limited to the filling of a form and the “drag and drop” of a file into a website.</td>
</tr>
<tr>
<td>R-WP4-4</td>
<td>M</td>
<td>The system should provide an easy-to-understand report describing the personal data found by the ML engine.</td>
<td>The report generated by WP6 is easy to understand. Moreover, WP4 provides examples of the data types identified to facilitate its understanding.</td>
</tr>
</tbody>
</table>

### 3.3.4. Requirements that will not be covered

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O⁹</th>
<th>Description</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP4-6 Removal of personal identifiers</td>
<td>M</td>
<td>SMOODATA will be able to remove the attributes identified as personal identifiers, together with potential quasi-identifiers.</td>
<td>This requirement has been removed, since the MENTs participating in the pilots do not require it and it added complexity to the platform and understanding of the results (The whole GUI of re-identification risks has not been integrated into the</td>
</tr>
</tbody>
</table>

⁹ O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).
3.3.5. Overall compliance

WP4 has significantly updated the original requirements during the execution of the project, after the interaction with the final users has evidenced the limitation of the SMOOTH platform users. The main changes have been related to the simplification of the processes. First, the data uploading process was simplified to avoid the direct connection to users' systems. Instead, the users can follow easy to use tutorials to obtain their data.

Moreover, the envisioned service to assist users with the anonymization of datasets and the understanding of re-identification risks was completely removed from the SMOOTH platform (following both, the recommendations of the first review, and the experience obtained in the interaction with the beta testers). Instead, the SMOOTH compliance report provides a simple indication of the risks associated with the re-identification.

Finally, the core functionality of WP4, the identification of the personal data into the MENTs datasets has been completely fulfilled as planned for 4 different languages (the original planning only included 3).

3.4. WP5: assessment of the technical requirements SMONLINE

- Organizations: UC3M, LSTECH and IMDEA
- WP: 5
- Name of the person(s) completing this document: Rubén Cuevas (UC3M), Celia López (UC3M), Narseo Vallina-Rodríguez (IMDEA), Álvaro Feal (IMDEA), Evangelos Kotsifakos (LSTECH).
### 3.4.1. Initial requirements

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O⁰</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP5-1</td>
<td>M</td>
<td>SMOOTH users shall provide the URL (or URLs) of the website in the entry questionnaire to be analysed by SMONLINE.</td>
<td>Website URLs will not be inferred or predicted, thus need to be provided by SMOOTH users when filling in the entry questionnaire. In the case of SMONLINE-MobileApp, app developers must provide access to the source code or a pointer to an app store.</td>
</tr>
<tr>
<td>R-WP5-2</td>
<td>M</td>
<td>SMOOTH platform shall include an OS that allows executing instances of popular desktop browsers (e.g., google chrome, Mozilla Firefox, etc.) to perform the analysis of websites.</td>
<td>SMONLINE submodules to analyse websites rely on the capacity of running web browser instances.</td>
</tr>
<tr>
<td>R-WP5-3</td>
<td>M</td>
<td>SMOOTH platform shall allow running instances of Google Chrome.</td>
<td>We commit to perform all analyses using Google Chrome as reference which according to very recent statistics covers 2/3 of the desktop browser market.¹¹</td>
</tr>
<tr>
<td>R-WP5-4</td>
<td>R</td>
<td>The module to analyse MEnts’ websites may be implemented in other popular web browser following this priority list: Mozilla Firefox, Safari, Edge, Internet Explorer.</td>
<td>In principle this is something unnecessary because the browser used should not affect the cookies and third-party connections analysed.</td>
</tr>
<tr>
<td>R-WP5-5</td>
<td>M</td>
<td>SMONLINE-Website shall provide the list of third parties domains for which the browser opens connections when accessing the MENT website.</td>
<td>This functionality will allow identifying third parties that may be obtaining personal data from users accessing the MENT website. This requirement also applies to SMONLINE-MobileApp, which should be able to identify networking activity to third-party services emanating from a given app.</td>
</tr>
<tr>
<td>R-WP5-6</td>
<td>M</td>
<td>SMONLINE-Website shall provide the list of cookies stored in the browser of the user when accessing the MENT website.</td>
<td>This functionality will allow listing the cookies stored in the browser of the user when she accesses the MENT website.</td>
</tr>
</tbody>
</table>

⁰ O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Type</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP5-7</td>
<td>R</td>
<td>SMONLINE-Website should classify the third-party domains for which the browser opens a connection (e.g., tracker, content distribution network, etc.) and the cookies stored in the browser of the user (e.g., first-party Vs. third-party cookie, session cookie Vs. temporal cookie Vs. persistent cookie, etc.).</td>
<td>Classifying the third-party domains and cookies will be useful to provide more detailed information in the GDPR compliance report in case some of them raise a warning after running the compliance analysis. Third party classification also applies to SMONLINE-MobileApp, which should be also capable of identifying the types of personal and sensitive data being collected by them from mobile users.</td>
</tr>
<tr>
<td>R-WP5-8</td>
<td>M</td>
<td>SMONLINE-Website shall provide the output list of cookies and third-party companies in standard format easy to process (e.g., JSON).</td>
<td>It is important to find a global agreement in the input data format used in WP6 to integrate and process together he information from SMOOTEXT, SMOODATA and SMONLINE to assess GDPR compliance and generate the compliance report. This requirement also applies to SMONLINE-MobileApp.</td>
</tr>
<tr>
<td>R-WP5-9</td>
<td>R</td>
<td>SMONLINE-Advertising module should be able to define specific personas (artificial user profiles) to check (audit) the MEnt’s website.</td>
<td>SMONLINE-Advertising is able to detect targeted advertisement based on specific personas-user profiles, that visit websites of specific subjects and categories. SMONLINE-Advertising can be guided by the users by providing personas to be checked, or it can assume personas that are relevant to MEnt website, or even random ones.</td>
</tr>
<tr>
<td>R-WP5-10</td>
<td>M</td>
<td>SMONLINE-Advertising shall provide a metric about the possibility of a (MENT) website to present advertisements that violate GDPR.</td>
<td>The report that SMONLINE-Advertising will provide a high-level information about the possibility that the website is displaying targeted advertisement.</td>
</tr>
<tr>
<td>R-WP5-11</td>
<td>M</td>
<td>SMONLINE-Advertising shall provide all the evidence found that relates the advertisements displayed on MENT website and the targeting of the user. Visiting websites that train the persona and screenshots of the visited websites showing the advertisements will be available.</td>
<td>SMONLINE-Advertising will offer a detailed report of the experiments that ran and drove to the conclusion that there is targeted advertisement or not. This report is not part of the basic compliance report, but it will be available upon user request.</td>
</tr>
<tr>
<td>R-WP5-12</td>
<td>M</td>
<td>SMONLINE-MobileApp shall be able to identify personal data</td>
<td>Many applications and third-party services currently encode personal data before</td>
</tr>
</tbody>
</table>
leakages (e.g., IMEI, geo-location) over network flows for applications not resorting to obfuscation and non-standard encryption mechanisms such as TLS.

uploading it to the server and may use techniques such as TLS certificate pinning to prevent independent auditing. In those cases, the report will indicate that a particular application may use such mechanisms and flag that they could have not been fully analysed.

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O</th>
<th>Modification</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP5-13</td>
<td>R</td>
<td>SMONLINE-MobileApp shall be able to study both iOS and Android applications.</td>
<td>The closed nature of iOS does not allow performing the same set of tests as for Android applications. Our efforts to support iOS during the development of SMOOTH were in vain due to platform limitations.</td>
</tr>
<tr>
<td>R-WP5-14</td>
<td>M</td>
<td>SMONLINE-MobileApp shall be able to scale the auditing analysis to at least 100 applications per hour.</td>
<td>This will be achieved through the use of Android’s executioner monkey to automatize application’s analysis using synthetic user input.</td>
</tr>
<tr>
<td>R-WP5-15</td>
<td>R</td>
<td>SMONLINE-MobileApp shall be able to comprehensively study applications requiring user accounts and logins.</td>
<td>One of the main limitations in analysing applications at scale is their complex user-interfaces and the need to create user accounts. This process can be difficult to scale (e.g., a banking app may require a user with a bank account). Currently, there are no methods for the automatic testing of apps that require user accounts.</td>
</tr>
</tbody>
</table>

### 3.4.2. Modified requirements

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O</th>
<th>Modification</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP5-4</td>
<td>R</td>
<td>We did not run full experiments using multiple browsers. We just did a preliminary analysis.</td>
<td>We did some preliminary tests that suggested the differences between browsers (mainly Google Chrome and Mozilla) were negligible. The reason is that MENTs websites run a single implementation for any type of browser. Therefore, the final version of the module is simply running in Google Chrome.</td>
</tr>
<tr>
<td>R-WP5-16</td>
<td>M</td>
<td>SMONLINE-Website and SMONLINE-MobileApp shall</td>
<td>This is actually a new requirement that arose during the development phase,</td>
</tr>
</tbody>
</table>

12 O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).
provide an output list with the company name behind third-party cookies and trackers. particularly when testing the platform after the integration of WP3 and WP5 outputs. We found that in many cases the name of the third-party tracker derived from a cookie or a network domain was different from the actual company name appearing in cookie or privacy policies. This could lead to potential false positives when we report third-party organizations in the compliance report, when in reality they were reporting either the product, the company name or even a subsidiary corporation. We developed a specific task in SMONLINE-Website and SMONLINE-Mobile app to consider all the possible names associated with a third-party company and provide this important functionality.

3.4.3. Requirements that are/will be covered

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O(^{13})</th>
<th>Description</th>
<th>Coverage Level / Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP5-1</td>
<td>M</td>
<td>SMOOTH users shall provide the URL (or URLs) of the website in the entry questionnaire to be analysed by SMONLINE.</td>
<td>FULLY COVERED. The Entry Questionnaire of the SMOOTH platform includes a section where MENTs can add the URL to be analyzed by WP5. It has been tested and it works.</td>
</tr>
<tr>
<td>R-WP5-2</td>
<td>M</td>
<td>SMOOTH platform shall include an OS that allows executing instances of popular desktop browsers (e.g., google chrome, Mozilla Firefox, etc.) to perform the analysis of websites.</td>
<td>FULLY COVERED. SMOOTH platform has been designed in a way in which each module runs in a separate docker. That docker allowed us to select the OS to run SMONLINE-Website, where we could instantiate any type of browser.</td>
</tr>
<tr>
<td>R-WP5-3</td>
<td>M</td>
<td>SMOOTH platform shall allow running instances of Google Chrome.</td>
<td>FULLY COVERED. SMONLINE-Website it is running Google Chrome in its normal operation.</td>
</tr>
</tbody>
</table>

\(^{13}\) O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).
<table>
<thead>
<tr>
<th>Requirement ID</th>
<th>Role</th>
<th>Description</th>
<th>Compliance Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP5-5</td>
<td>M</td>
<td>SMONLINE-Website shall provide the list of third parties domains for which the browser opens connections when accessing the MENT website.</td>
<td>FULLY COVERED. The output JSON file generated by SMONLINE-Website includes the list of third-party domains for which the browser opens connection when accessing the MENT website.</td>
</tr>
<tr>
<td>R-WP5-6</td>
<td>M</td>
<td>SMONLINE-Website shall provide the list of cookies stored in the browser of the user when accessing the MENT website.</td>
<td>FULLY COVERED. The output JSON file generated by SMONLINE-Website includes the list of cookies stored in the browser of the user when accessing the MENT website.</td>
</tr>
<tr>
<td>R-WP5-7</td>
<td>R</td>
<td>SMONLINE-Website should classify the third-party domains for which the browser opens a connection (e.g., tracker, content distribution network, etc.) and the cookies stored in the browser of the user (e.g., first-party Vs. third-party cookie, session cookie Vs. temporal cookie Vs. persistent cookie, etc.).</td>
<td>FULLY COVERED. The output JSON file generated by SMONLINE-Website includes a category for each third-party domain/cookie found (TRACKER, AD, BOTH or OTHER). In addition, it classifies the cookies in the browser as first party or third-party cookie, and whether it is a session cookie or permanent cookie. We also classify the third-party domains (either via cookies or connections) as static or dynamic. SMONLINE-Website is implemented in a way that runs 5 times at different times per URL. Those third party cookies/domains that are present in each execution are labelled as static, while those ones that only appear in one of few of the execution is labelled as dynamic.</td>
</tr>
<tr>
<td>R-WP5-8</td>
<td>M</td>
<td>SMONLINE-Website shall provide the output list of cookies and third-party companies in standard format easy to process (e.g., JSON).</td>
<td>FULLY COVERED. The output JSON file generated by SMONLINE-Website was agreed across WP3, WP5 and WP6. We have iterated several times until we reached its final format.</td>
</tr>
<tr>
<td>R-WP5-9</td>
<td>R</td>
<td>SMONLINE-Advertising module should be able to define specific personas (artificial user profiles) to check (audit) the MEnt’s website.</td>
<td>FULLY COVERED. In the SMONLINE-Advertising module we define personas in order to audit the MEnt’s website. These personas can be changed/configured in the future through configuration files/database.</td>
</tr>
<tr>
<td>R-WP5-10</td>
<td>M</td>
<td>SMONLINE-Advertising shall provide a metric about the possibility of a (MENT) website to present advertisements that violates GDPR.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td>R-WP5-11</td>
<td>M</td>
<td>SMONLINE-Advertising shall provide all the evidence found that relates the advertisements displayed on MENT website and the targeting of the user. Visiting websites that train the persona and screenshots of the visited websites showing the advertisements will be available.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td>R-WP5-12</td>
<td>M</td>
<td>SMONLINE-MobileApp shall be able to identify personal data leakages (e.g., IMEI, geo-location) over network flows for applications not resorting to obfuscation and non-standard encryption mechanisms such as TLS.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td>R-WP5-14</td>
<td>M</td>
<td>SMONLINE-MobileApp shall be able to scale the auditing analysis to at least 100 applications per hour.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td>R-WP5-15</td>
<td>R</td>
<td>SMONLINE-MobileApp shall be able to comprehensively study applications requiring user accounts and logins.</td>
<td>FULLY COVERED</td>
</tr>
</tbody>
</table>
Furthermore, the questionnaire has specific fields in which MENTs can provide test accounts so that we can further test these applications if they deem it appropriate.

**R-WPS-16**  
**M**  
SMONLINE-Website and SMONLINE-MobileApp shall provide an output list with the company name behind third-party cookies and trackers.  
FULLY COVERED  
MobileApp provide such lists of companies behind third-party cookies and trackers through separate service points (API).  
The main service of the SMOOTH platform, the workflow service (WP6) has incorporated in its pipeline these service points and the output is available for comparison. So, SMONLINE-Website and SMONLINE-MobileApp modules are invoked twice. The first time to get the analysis information and the second time to receive the list of actual companies behind third party trackers.

### 3.4.4. Requirements that will not be covered

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O[^14]</th>
<th>Description</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WPS-4</td>
<td>R</td>
<td>The module to analyse MEnts’ websites may be implemented in other popular web browser following this priority list: Mozilla Firefox, Safari, Edge, Internet Explorer.</td>
<td>We did some preliminary tests that suggested the differences between browsers (mainly Google Chrome and Mozilla) were negligible. The reason is that MENTs websites run a single implementation for any type of browser. Therefore, the final version of the module is simply running in Google Chrome. This does not imply any performance downgrade neither in the delivery of SMONLINE-Website nor in the delivery of the SMOOTH platform.</td>
</tr>
<tr>
<td>R-WPS-13</td>
<td>R</td>
<td>SMONLINE-MobileApp shall be able to study both iOS and Android applications.</td>
<td>The infrastructure that is needed to run Smonline-MobileApp is highly complex and completely dependent of Android core functionalities. Therefore, implementing a similar solution for iOS was deemed too</td>
</tr>
</tbody>
</table>

[^14]: O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).
complex and time-consuming for this project. Nevertheless, we have seen that MENTs do not often have Android applications in place, and taking into account that the cost to publish iOS applications is even higher than for Android we believe that SMOOTH’s capability to provide a service to MENTs will barely be reduced by this limitation.

3.4.5. Overall compliance

SMONLINE module (WP5) has been designed from the very beginning like three separate modules: SMONLINE-Website, SMONLINE-Advertising and SMONLINE-Mobile app. For each of them we described clear requirements in the first phase of the project that has been used to drive the development in order to cover them as close as possible. As a result of the assessment, we can confirm that WP5 has successfully covered 14/16 requirements including all the mandatory ones. The 2 requirements that are not covered, as explained, do not have a negative impact in the module development, nor in the SMOOTH platform.

3.5. WP6: assessment of the technical requirements PLAT

- Organizations: EUT, LSTECH
- WP: 6
- Name of the person(s) completing this document: Evangelos Kotsifakos (LSTECH), Jordi Allue (EUT).

3.5.1. Initial requirements

a. Functional requirements

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O(^\text{15})</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-WP6-1</td>
<td>R</td>
<td>The user could register on the platform prior to the completion of a GDPR assessment.</td>
<td></td>
</tr>
<tr>
<td>R-WP6-2</td>
<td>M</td>
<td>The user will be able to access the platform and start a GDPR assessment that combines questionnaire and the use of different modules if he/she has previously registered.</td>
<td></td>
</tr>
</tbody>
</table>

\(^{15}\) O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).
| R-WP6-3 | M | The user will receive a GDPR customized report after the assessment phase. | The report could be sent either by email or downloaded in a pdf format. |
| R-WP6-4 | M | Previously to the assessment, the user will be present with all the relevant informed consents (privacy policy and cookie policy) specifying their rights regarding the privacy of their data as well as the purpose why it is being collected. | The consent will clearly specify in which way the project processes their data, as well as how to enforce their rights. |
| R-WP6-5 | M | The dynamic questionnaire will display or hide relevant questions based on the user’s previous answers. | This will apply to possible calls to other modules. Ex: If user A specifies it has no webpage and no App, SMONLINE module might not be called. |
| R-WP6-6 | R | User could be able to save a draft of the current assessment form to be completed later. | Dependency on R-WP5-1: The user will need to be registered and logged in. |
| R-WP6-7 | M | The user will need to opt in to share any personal information. | |
| R-WP6-8 | R | The user will be able to access the platform and start a GDPR assessment that combines questionnaire and the use of different modules anonymously. | The user could be complete an assessment without being previously registered. |
| R-WP6-9 | R | The platform will have an administrator view to manage the platform. | The admin role will be able to see statistics from previous assessments and manage different back-end settings |
| R-WP6-10 | M | A registered user will be able to log in and download a previously fulfilled compliance report. | Up to 90 days after the completion. |
| R-WP6-11 | M | The system will allow the erasure of any information pertaining to a specific user if said user requests so at any moment. | |
| R-WP6-12 | M | The platform provides methods for users to enforce their data rights. | A questionnaire, form or an email box that allows to request withdrawal of their data from the platform. |
### b. Non-Functional requirements

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFR-WP6-1</td>
<td>R</td>
<td>The system should be able to handle up to 100,000 companies.</td>
<td>Not simultaneously.</td>
</tr>
<tr>
<td>NFR-WP6-2</td>
<td>R</td>
<td>The customized report on GDPR compliance should be generated in less than 12 hours.</td>
<td>For the scope of the project, the compliance report will be ready in less than 12 hours from the moment a user fulfils the questionnaire.</td>
</tr>
<tr>
<td>NFR-WP6-3</td>
<td>R</td>
<td>The Platform should be able to handle 50 recurrent users at the same time.</td>
<td>Based on expected concurrency.</td>
</tr>
<tr>
<td>NFR-WP6-4</td>
<td>R</td>
<td>The Platform could store a GDPR assessment for as long as the user requests to.</td>
<td></td>
</tr>
<tr>
<td>NFR-WP6-5</td>
<td>M</td>
<td>Any information stored that could potentially be deemed as personal will be encrypted and protected through several layers of security.</td>
<td>In general, the system will guarantee standardised methods of cybersecurity (Encryption, firewalls...).</td>
</tr>
<tr>
<td>NFR-WP6-6</td>
<td>M</td>
<td>The Platform will be fully interoperable with the rest of the modules developed in WP3-4 and 5. The modules will operate within the Platform or communicate with it by means of standardised protocols.</td>
<td></td>
</tr>
<tr>
<td>NFR-WP6-7</td>
<td>M</td>
<td>Any information exchanged between modules will be done in a secure channel and only if totally necessary for the proper functioning of the system.</td>
<td>The system will prevent the use of unsecure data exchange.</td>
</tr>
</tbody>
</table>

---

16  O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).
3.5.2. Modified requirements

The requirements have been implemented as they have been defined.

3.5.3. Requirements that are covered

<table>
<thead>
<tr>
<th>Requirement name</th>
<th>O(^{17})</th>
<th>Description</th>
<th>Coverage Level / Notes</th>
</tr>
</thead>
</table>
| R-WP6-1          | R          | The user could register on the platform prior to the completion of a GDPR assessment. | FULLY COVERED  
After visiting the home page of the SMOOTH platform, the user has to register before they can proceed to enter data and have a compliance report. |
| R-WP6-2          | M          | The user will be able to access the platform and start a GDPR assessment that combines questionnaire and the use of different modules if he/she has previously registered. | FULLY COVERED.  
The user can access the SMOOTH platform using their credentials and they can start the process of the assessment at any time, using the entry questionnaire, that in its turn uses the backend modules to process the data. |
| R-WP6-3          | M          | The user will receive a GDPR customized report after the assessment phase. | FULLY COVERED.  
After the assessment is over the user receives an email that notifies them that the report is ready and can be accessed through the platform, while it is also attached as a pdf document. |
| R-WP6-4          | M          | Previously to the assessment, the user will be present with all the relevant informed consents (privacy policy and cookie policy) specifying their rights regarding the privacy of their data as well as the purpose why it is being collected. | FULLY COVERED.  
The user, after registration to the platform, has to read and agree to the informed consent before proceeding on using the platform. |
| R-WP6-5          | M          | The dynamic questionnaire will display or hide relevant questions based on user previous answers. | FULLY COVERED  
The questionnaire has been designed in a way that displays questions that are relevant to the answers that the user is |

\(^{17}\) O = obligation; M = mandatory; R = optional but recommended. Requirements are indicated as mandatory (M) or recommended (R).
<table>
<thead>
<tr>
<th>R-WP6-6</th>
<th>R</th>
<th>User could be able to save a draft of the current assessment form to be completed later.</th>
<th>FULLY COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>The user can start answering the questionnaire and their answers are saved in the system. The user can stop answering the questions and if he visits the platform in the future, they can resume from the point they have stopped.</td>
<td></td>
</tr>
<tr>
<td>R-WP6-7</td>
<td>M</td>
<td>The user will need to opt in to share any personal information.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The user is not obliged to provide any information at any point. Apart from the initial consent that they have to accept to use the platform, they are asked to provide other data/ files only if they want to.</td>
<td></td>
</tr>
<tr>
<td>R-WP6-8</td>
<td>R</td>
<td>The user will be able to access the platform and start a GDPR assessment that combines questionnaire and the use of different modules anonymously.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The user has the option to start at any time a GDPR assessment that combines the questionnaire and the related modules without providing any personal-identified information apart from an email address that they have to provide in order to receive notification and the assessment and also to ensure the security of the platform.</td>
<td></td>
</tr>
<tr>
<td>R-WP6-9</td>
<td>R</td>
<td>The platform will have an administrator view to manage the platform.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The platform provides an admin panel with a lot of information about the users and the reports that they have run, the modules needed for the report and some statistical information among others.</td>
<td></td>
</tr>
<tr>
<td>R-WP6-10</td>
<td>M</td>
<td>A registered user will be able to log in and download a previously fulfilled compliance report.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The user can login with their credentials and accessing the related page, they can download their compliance report.</td>
<td></td>
</tr>
<tr>
<td>R-WP6-11</td>
<td>M</td>
<td>The system will allow the erasure of any information pertaining to</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The data files that the user uploads to the system are deleted right after their</td>
<td></td>
</tr>
<tr>
<td>Requirement ID</td>
<td>Type</td>
<td>Requirement</td>
<td>Coverage</td>
</tr>
<tr>
<td>---------------</td>
<td>------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>R-WP6-12</td>
<td>M</td>
<td>The platform provides methods for users to enforce their data rights.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td>NFR-WP6-1</td>
<td>R</td>
<td>The system should be able to handle up to 100,000 companies.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td>NFR-WP6-2</td>
<td>R</td>
<td>The customized report on GDPR compliance should be generated in less than 12 hours.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td>NFR-WP6-3</td>
<td>R</td>
<td>The Platform should be able to handle 50 recurrent users at the same time.</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td>NFR-WP6-4</td>
<td>R</td>
<td>The Platform could store a GDPR assessment for as long as the user requests to.</td>
<td>FULLY COVERED</td>
</tr>
</tbody>
</table>
runs another one, or they request it deletion.

<table>
<thead>
<tr>
<th>NFR-WP6-5</th>
<th>M</th>
<th>Any information stored that could potentially be deemed as personal will be encrypted and protected through several layers of security.</th>
<th>FULLY COVERED. The platform has been designed in a way that will not store any personal information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFR-WP6-6</td>
<td>M</td>
<td>The Platform will be fully interoperable with the rest of the modules developed in WP3-4 and 5. The modules will operate within the Platform or communicate with it by means of standardised protocols.</td>
<td>FULLY COVERED. The platform and the modules are integrated and interconnected under the platform environment and they communicate through well-documented APIs.</td>
</tr>
<tr>
<td>NFR-WP6-7</td>
<td>M</td>
<td>Any information exchanged between modules will be done in a secure channel and only if totally necessary for the proper functioning of the system.</td>
<td>FULLY COVERED. The communication between the platform modules is done through secure communication using security tokens.</td>
</tr>
</tbody>
</table>

3.5.4. Requirements that will not be covered

All WP6 requirements have been fulfilled as defined.

3.5.5. Overall compliance

The consortium has carefully defined the platform requirements and followed them during the implementation phase. All the requirements have been fulfilled without modifications.

3.6. WP7: assessment of the technical requirements PILOT

- Organization: FBOX, ESBA, and EURECAT
- WP: 7
- Name of the person(s) completing this document: Thomas Wilczek, Alex Pereda, Eva Merloni

3.6.1. Initial requirements

<table>
<thead>
<tr>
<th>MEnt Requirement name</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
According to the MEnts consulted, the main assessment options to verify GDPR compliance are: low-cost online solution and to follow a course regarding GDPR.

76% of MEnts stated that their companies would choose to use a low-cost online solution to assist them be compliant with the GDPR.

Moreover, 64% of the MEnts consulted, indicated that they could consider as a solution to follow a course to obtain the required expertise to deal with the GDPR, within their company.

Only 17% of the MEnts consulted considered subcontracting a law firm or consultancy to verify the company’s processing activities in light of the GDPR.

Most MEnts considered that the time consumed for the preparation of reports was an important factor.

More than 50% indicated that they would dedicate a maximum of 30 minutes to complete the SMOOTH Platform process.

MEnts were consulted regarding the time they will be willing to wait for the Platform to generate a compliance report.

Almost 50% of the companies answering the survey indicated that 1 week for generating the ad-hoc report will be reasonable.

The other MEnts indicated 1 day and 1 hour as reasonable to generate a compliance report.

We have seen that cost is also an important factor for MEnts.

More than 62% of the MEnts are not willing to pay more than €50 (per use) for the online solution, while the remaining MEnts oscillate between €100 and €200.

Due to their lack of expertise in GDPR, MEnts need examples of GDPR documents and templates.

100% of MEnts consulted indicated that they would like GDPR templates for informed consent.

81% of MEnts consulted indicated that they would like GDPR templates for privacy notice and privacy notice for the website.
75% of MEnts consulted indicated that they would like GDPR templates for a cookie policy.

69% of MEnts consulted indicated that they would like to have templates for Data Processor Agreements and records of Processing activities and templates regarding data breach notification form to the Data Protection Authority and to the individuals concerned.

The GDPR Handbook takes care of this requirement.

MEnts clearly need reliable materials and tools to guide them through the GDPR compliance process.

According to the consultation, one crucial requirement is the use of plain language in order to let MEnts understand the GDPR process.

The Entry Questionnaire to the Platform should use plain language and not require prior understanding of data protection law.

Interfaces should be easy to use and provide a comfortable user experience.

This requirement is crucial for MEnts that do not have time to compile paperwork. The SMOOTH Platform should be simple and easy to use and avoid unnecessary processes.

### 3.6.2. Modified requirements

No requirements have been modified.

### 3.6.3. Requirements that will be covered

<table>
<thead>
<tr>
<th>MEnt Requirement name</th>
<th>Description</th>
<th>Coverage Level/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MENT-SP1</td>
<td>GDPR Assistance</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SMOOTH fully responds to the users’ requirement of a low-cost online solution to assist them to be compliant with the GDPR.</td>
</tr>
<tr>
<td>MENT-SP2</td>
<td>Time spent on the SMOOTH Platform</td>
<td>FULLY COVERED</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In pilot 1 average completion times were 37 minutes, which is 7 minutes over the time limit requirement set by users. However, it should be noted that in pilot 1 we were working on a preliminary version of the questionnaire. In pilot 2, completion times were amply below the KPI of 30 minutes, even for participants in modality 3 for which the evaluation procedure was slower.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MENT-SP3</th>
<th>Report Generation Time</th>
<th>FULLY COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Report generation times are well below the highest limit indicated by users of a day and an hour</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MENT-SP4</th>
<th>Affordable</th>
<th>FULLY COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Affordable</td>
<td>After carrying out a benchmarking analysis, a yearly subscription price of €99 was established. However, after having taken into consideration results from the market pilot, and the high number of answers expressing that it was somewhat expensive, this price has been revised to €90 for the yearly subscription. In order to maximize the access, after validating the frequency of use, which is for almost 52% of users, one time per year, a pay-per-use model has been also created at a cost of €29. This way, customers not willing to pay the yearly subscription will also have access to the SMOOTH platform services at an affordable price.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MENT-SP5</th>
<th>Compliance GDPR - templates - content</th>
<th>FULLY COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A SMOOTH Handbook has been developed that will provide users with templates and guidance through the GDPR compliance process.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MENT-SP6</th>
<th>Plain Language</th>
<th>FULLY COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Results of both pilots showed that users had a good understanding of the language used in the Entry Questionnaire and compliance report. In cases where users indicated any term they did not understand, an explanation box has been added. Over 94% of answers in the market pilot answered that they are very satisfied, satisfied, or neutral with the statement regarding that SMOOTH tools are easy to use and to understand.</td>
<td></td>
</tr>
</tbody>
</table>
MENTS-SP7 | Usability | FULLY COVERED
--- | --- | ---
Metrics for usability and attractiveness of the interfaces obtained in pilot 1 indicated a good user satisfaction with these aspects, especially regarding clearness of the design and ease of use. However, some issues were noted regarding orientation and navigability in the entry questionnaire, thus, the Entry Questionnaire was analysed by an UX design expert and his recommendations for improving the navigability of the interface were implemented for Pilot 2, where these issues with the orientation and navigability raised in pilot 1 are not observed anymore. Finally, based on the feedback obtained in pilot 2, the compliance report was improved in terms of layout attractiveness.

The questionnaire onboarding and the questionnaire UX were further assessed and improved during the first weeks of the market pilot.

The market validation pilot (T7.4) was implemented in the final 3 months of the project (M31-M33) with an overall KPI target of 500 participants. Due to the impact of the Covid19 pandemic on the overall project, which was extended 3 months, the market pilot was postponed to M31-M33. In reaction to the low participation numbers, the market pilot was extended till the very last day of the project.

A total of 161 MEnts participated in the market validation assessment.

Despite a number of mitigation actions throughout the market pilot, implementing additional learnings by among other things, including the extension of the pilot, further UX improvements and extensive promotion activities (described in detail in deliverables D8.5 and D7.4) it was not possible to increase the final market pilot participations. The following very useful main learnings according to our research based on both qualitative and quantitative feedback have already helped the project to further improve elements of the platform, an activity that will carry on after the end of the project.

- **The Covid19 impact**: It has amplified and intensified certain aspects of how small companies deal with the GDPR theme and SMOOTH’s service offering. On the one hand, MEnts were more focussed on survival since they have been impacted especially also due to their vulnerability in terms of financial recourses. On the other that the shift of professional and day-to-day life into the digital sphere have caused “over-information” and “overexposure” resulting in digital fatigue and making it extremely hard to get the market pilot promo message across, despite the powerful campaign numbers in terms of reach and impressions. Although it has not been possible to recruit 500 MEnts, there have been first commercial contacts with intermediaries, multipliers and prescribers with the aim of paving the path towards a successful commercial exploitation.

- **The GDPR theme and its complexity**: despite efforts to make this theme more accessible including change of branding, accessible relatable content including interviews with
representatives of the target group, informative webinars, UX optimisation and implementation of accessible language, GDPR still seems a complex theme which requires certain attention and time investment.

- **Lack of trust:** a number of MEnts were not willing to provide their or their customers’ data to an automated service. Mitigation actions in the form of clear statements regarding the data security of the project and descriptions of the actual process both in written content pieces and during webinars were not able to change this perception. The MEnts in question prefer their already existing human to human set ups (lawyer, admin, etc)

- **Already existing set-ups:** other MEnts indicated that they already have their set-up with a physical service, which they prefer.

- **New timeline (due to Covid19 Impact):** 2\textsuperscript{nd} pilot extension overlapped with the market pilot launch, which significantly impacted the first month of its running time due to the 2\textsuperscript{nd} pilot rewards being more substantial and a certain message collusion of the two. The festive period in the second month of the market pilot (early December festivities, Christmas, New Year additionally impacted the promo campaign negatively.

3.6.4. Requirements that will not be covered

All requirements are covered, as described above (i.e., relating to the market pilot).

3.6.5. Overall compliance

This requirements analysis is based on the results of Pilots 1, 2 and the market assessment pilot. Based on these results we can consider the requirements are fully achieved.

4. Human assessment of a case assessed by the SMOOTH Platform

4.1 Scope

In Recommendation 8 of the first review report, the SMOOTH consortium partners were recommended to\textsuperscript{18}:

‘The partners should consider confronting their automated generation of a compliance report to the compliance work that would undertaken by a legal expert. To this end, the recommendations and notification of a compliance report for some MEnts could be compared to the advise/indications to be provided by a legal expert. In this way, SMOOTH will be able to evaluate not only the automation and speed of its solution, but also the quality of its outputs.’

The SMOOTH consortium proposed the following in its action plan:

*Action: It is foreseen that the report generated automatically by the platform apart from the results coming from the analysis made by the different modules, will compile the*

\textsuperscript{18} Review report of 3 July 2019, p. 7.
explanations of why the warnings are generated, how to address the raised issues and to add relevant links to external resources.

From the legal documents’ analysis and extraction, we plan to provide confidence scores, which can be used to filter out low confident predictions.

The disclaimer for the limits of the SMOOTH platform has been defined by our legal partners and will be added to the compliance reports generated by the platform.

This recommendation was also repeated in the second review report:19

‘Recommendation 8 (Pilots/Exploitation): In order to demonstrate the added-value of SMOOTH, as well as clarify the limitations of the service, it is advised that a comparison of the SMOOTH capabilities and assessment results against those of an experienced legal expert is performed. Emphasis should be paid on the automation vs. quality trade off, as human experts are expected to give high quality recommendations, yet the SMOOTH system can provide them automatically.

Moreover, it should be explored whether the SMOOTH system can provide insights on privacy issues that could be missed by a human (e.g., detection of hidden patterns of privacy data abuse).’

The SMOOTH consortium proposed the following proposed in its action plan:

Action: A disclaimer about the limitations of the compliance report is already implemented and we will make sure to highlight what aspects of the GDPR may not have been assessed because of the limitation of the report or because the lack of information provided by the user.

The comparison of the SMOOTH platform report and the potential report provided by a legal expert will be added into the next deliverable D6.3.

This assessment will be further referred to as the ‘Human Assessment’.

Performing such an assessment would only be possible if the Platform would be up and working, so it was decided to add this assessment to a deliverable that would be submitted near the end of the project, in D6.3 (due by the end of October 2020).

However, as the Platform was not yet fully operational at that moment,20 it was decided to add the Human Assessment to D.2.4, which would be only due at the end of the project.

The modus operandi and the conclusions of the Human Assessment are below. The actual Human Assessment and the assessment provided by the Smooth Platform are added to this Deliverable in Annex V.

---

20 See Deliverables 7.3 and 7.4 for more information.
4.2 Modus operandi

4.2.1. The use of a fictional case

It was decided by the consortium to perform the Human Assessment on a fictional case. This choice was made for the following reasons:

- The data files uploaded by the participants using the SMOOTH Platform (the ‘Participants’) are immediately deleted by the Platform for data protection reasons. If the Human Assessment was to be performed on an actual case, the legal expert would not have access to the data file.
- Working with a fictional case allows to construct a sufficiently complex case to be tested, allowing to add for example special categories of data that would not occur often in practice, such as data related to racial origin or religious beliefs.
- As explained D7.4, less MEnts have used the Platform than anticipated. This results in less useful cases being available for the Human Assessment.

4.2.2 The automated assessment of the case

The initial automated assessment of the Smooth Platform, the testcase, was created by EURECAT and relates to the following situation

A Belgian lawfirm ‘Lawfrin’. Lawfrin is a Belgian lawfirm, mainly active on the Belgian market. It is a business law firm, focussing on tax, white collar crime, wealth planning, corporate and general private law issues, delivering services to both enterprises and individuals.

The entry questionnaire is completed on behalf of Lawfrin. Lawfrin has a privacy and a cookie policy and uploads both to the Platform during the assessment. It also provides a website to be scanned and an APK-file for its mobile app to be scanned.

Lawfrin uploads one data file, related to its clients, to be scanned by the Platform. The data file contains the following types of personal data:

- Internal identification number
- Name
- E-mail
- Phone number
- Bank account number
- Address
- Monthly income
- Date of birth
- Username
- Password
- Racial origin
- Religious belief
The completed questionnaire and the data file are added as Annex V to this deliverable.\textsuperscript{21}

To make the case as realistic as possible, the actual website, privacy policy and cookie policy of an actual Belgian law firm where used. To avoid that they could be recognized, and that their assessment would become public, these documents are not added and any information in the entry questionnaire that may lead to the recognition of the law firm concerned, is removed.

The compliance report generated by the Smooth Platform is joined to this deliverable as Annex V.3.

4.2.3 The Human Assessment

The automated assessment and all the information it used was transferred to the legal expert appointed by the consortium, to perform the Human Assessment.

This Human Assessment will be performed by KU Leuven, as legal partner.

The Human Assessment, in which each part is immediately compared with the compliance report generated by the Platform, is joined to this deliverable as Annex V.4. To be able to compare both, the Human Assessment has followed the same structure as the compliance report.

4.2.4 The conclusion

Each part of the Human Assessment has been compared with each part of the compliance report generated by the Platform in Annex V.4. The general conclusion can be found below.

4.4 Conclusion

In general, we can establish that the Platform and the Human Assessment come to roughly the same conclusions and recommendations.

It is clear that the combination between the compliance report and the GDPR Handbook is very valuable, as it allows the compliance report to briefly explain the essence of a number of notions and to refer to the GDPR Handbook for further. It is also able to process large volumes of data and APK-files related to mobile apps, which are much more difficult for humans to do.

On the other hand, the technical limitations of the Platform\textsuperscript{22}, and the general nature and broad applicability of the Platform, cause that it is not always as accurate in identifying details that are applicable on a specific type of MEnt. This is however covered by warnings and disclaimers shown to the participating MEnt. Also, the compliance report doesn’t always mention what information appears to be missing, but we should be able to easily fix this for some types of information in the Platform and the compliance report.

As a general conclusion, we estimate that the Platform provides a good solution to assess the GDPR compliance of MEnts, taking into account a few limitations and its general nature. This is especially the case, as the Platform is able to render its report in a matter of minutes at no marginal cost at all, after the MEnt has completed the survey in less than 30 minutes. Whereas individual advisors would need several days, including meetings, to arrive at more or less the same conclusions, at a

\textsuperscript{21} Annex V.1: the entry questionnaire of Lawfrin and Annex V.2: the data file related to the clients of Lawfrin.

\textsuperscript{22} Such as the types of data that can be recognized, see above in this deliverable, ‘3.3.2. Modified requirements’.
much higher cost and time investment for the MEnts, probably causing them to not undertake the effort at all.

5. Annexes

**Annex I** – Final text version of SMOOK mobile application, graphic design partly included

**Annex II** – Final text version of SMOOK website application, with graphic design partly included

**Annex III** – SMOOK Mobile App – screenshots and demonstration videos

**Annex IV** – SMOOK Website App – screenshots

**Annex V** – Human assessment of a case assessed by the SMOOTH Platform
Annex I – Final version of GDPR handbook mobile application, with legal texts and graphic design

Annex I.1 A few screenshots to demonstrate the look and feel of the application
1. MENU 1 - HOME PAGE or ABOUT - Landing Page

1.1. FACTS & NUMBERS

Annex I.2 The application (full text)
1.2. WHAT IS SMOOK?

SMOOK is an online interactive handbook for micro-enterprises, providing detailed guidance to help them understand:

- How the General Data Protection Regulation (GDPR) affects their enterprises.
- What actions they must undertake in order to become GDPR-compliant.
- How to navigate through the GDPR regulation.

1.3. WHO IS SMOOK FOR?

SMOOK is especially designed for micro-enterprises. Although the content is tailor-made for them, any enterprise can extract GDPR information from this handbook.

Link - SMEs & the GDPR

1.4. My Data Protection Authority

For any questions or advices on your processing activities, you need to turn to the competent data protection authority. This is also the case if you want to request an audit or to file a complaint.

If a data protection impact assessment indicates that your enterprise is engaging in high risk processing, you are obliged to consult the data protection authority prior to the processing of any data.
You will find the name and contact details of all the Data Protection Authorities in the EU and EEA.
2. MENU 1 – The GDPR Regulation in a nutshell

2.1. A brief History


However, since 1995, the internet has grown immensely and the way data is being used, collected and stored has fundamentally changed.

Data is everywhere

READ MORE

Therefore, a revision of the Data Protection Directive was long overdue. This time, the EU opted for a regulation instead of a directive. This means that the GDPR – as one unified data protection regulation – directly applies in all EU member states, harmonising national data protection laws across the EU.

Although GDPR-compliance is still widely perceived as an administrative burden by many companies, there is also a reverse side to the coin: it creates new business opportunities and value in the future digital economy.

- Take back control – as its primary objective, the GDPR strives to give back the control of personal data to all citizens in the EU. Therefore, improving their overall sense of trust and security.
- GDPR in the Digital Age - by simplifying the monitoring environment for international businesses, through the standardisation of the regulation within the EU, the GDPR facilitates the international data flows.
- A fair competition - by creating the same set of rules between companies established in the EU, and those based outside the EU, the GDPR puts an end to distortion of competition.

The most important novelties introduced by the GDPR:

- Extended territorial scope;
- New basic principles;
- New obligations – for processors too;
- New rights for data subjects;
- Rules on children’s consent;
- High fines – up to 20 million or 4% of the total worldwide turnover.

2.2. It’s scope

2.2.1. What?

For the GDPR to be applicable, personal data needs to be:

- Entirely or partly, processed by automated means.
Part of a filing system, or intended to be part of a filing system, when processing does not happen by automated means.

2.2.1.1. Personal data

2.2.1.1.1. What constitutes “personal data”?

2.2.1.1.2. When is a person “identifiable”?

The context in which the data is being collected is also very important.

One single piece of data (E.G. hair colour, occupation, car...) might not be enough to identify a natural person as such. Now should the data be combined with other data; this might change the situation. Enterprises that collect multiple types of data on people should take this into account.

Anonymizing and pseudonymizing data are encouraged by the GDPR. The difference between these techniques is that pseudonymous data merely reduces likability but still allows for some form of re-identification (E.G. encryption or when the identifiers are replaced by individual codes), while anonymous data cannot be re-identified (linked to persons) at all.

Any data or information - which have had their identifiers removed (anonymization) or replaced (pseudonymization) - will still be considered being a “personal data” for the purposes of the GDPR.

N.B. Information which is truly and fully anonymous even before being processed is not covered by the GDPR.

2.2.1.1.3. What is not “personal data”?

Information about a deceased person, cookies tracking the number of visits to a website without identifying the visitors (statistics), data about companies or public authorities or any other data from which it is not possible to directly or indirectly link it to a person are not to be considered as personal data.

However, a nuance should be added regarding information about individuals acting as sole traders, employees, partners and enterprise directors when the information relates to them as individuals and where they are individually identifiable. In that case, it does concern “personal data”. This means that a work email address containing the business partner’s name (E.G. adam.johnson@enterprise.com) is personal data, while a generic email address (E.G. contact@enterprise.com) is not.
2.2.1.1.3. Special categories of data

The GDPR make a distinction between ‘regular’ personal data and special categories of data. The latter require extra protection because of their sensitive nature. Therefore, processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation are, in principle, prohibited.

However, a limited number of exceptions to this rule is provided by the legislator.

Link – Is my enterprise allowed to process personal data?

2.2.1.2. Processing

“Processing” is defined very broadly under the GDPR:

- Any operation or set of operations;
- Which is performed on personal data or on sets of personal data;
- Whether or not by automated means.

Recording – Collecting – Organising – Structuring – Adapting or altering – Storing – Retrieving – Consulting – Disclosing by transmission – Using – Disseminating or otherwise making available – Aligning or combining – Erasing or destructing – Restricting

💡 When you pseudonymize or anonymize personal data, you are also processing in the sense of the GDPR.

2.2.1.2.1. What does not constitute “processing” under the GDPR?

The GDPR does not apply to certain activities such as processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities (e.g. when collecting names and telephone numbers of attendees of a party at your house).

In the absence of processing activities or personal data, the GDPR will not apply.

2.2.2. Where?

For the GDPR to apply your enterprise, it should fall under the territorial scope of the Regulation. Article 3 defines this territorial scope based on two main criteria:

- The “establishment criterion” - Your enterprise is established in the Union. The GDPR applies if your enterprise – operating either as controller or as processor – is established in the Union, regardless of whether the processing takes place in the Union or not. An enterprise is established in the Union if it has a stable presence there, which exercises real and effective activities considering the nature of the economic activity carried out by the enterprise.

- The “targeting criterion” - Your enterprise is established outside the Union but is processing data of individuals in the Union.
The GDPR also applies when your enterprise – operating either as controller or as processor – is not established in the Union but does process personal data of individuals who are in the Union, where the processing activities are related to:

- The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- The monitoring of their behaviour, as far as their behaviour takes place within the Union.

Thus, under certain conditions the GDPR has extraterritorial applicability.

2.2.2.1. Need an example?

A start-up established in the USA, without any business presence or establishment in the EU, provides a city-mapping application for tourists. The city-mapping application processes personal data concerning the location of customers in the city they are visiting, in order to offer targeted advertisement for places to visit, such as restaurant, bars, shops and hotels.

The application is available for tourists while they visit New York, San Francisco, Toronto, London, Paris or even Rome. The US start-up, via its city mapping application, is offering services to individuals in the Union (London, Paris or Rome). The processing of the EU-located data subjects’ personal data in connection with the offering of the service falls within the scope of the GDPR. (Source: EDPB Guidelines 3/2018 on the territorial scope of the GDPR)

2.2.2.2. What if your enterprise is established in the EU but you work with a processor to which the GDPR does not apply?

If you as a controller, subject to the GDPR, choose to use a processor located outside of the Union and not subject to the GDPR, it will be necessary for you to ensure that the processor processes the data in accordance with the GDPR, just as if the processor is subject to the GDPR, but with some extra requirements. Compliance with the GDPR requires that processing by a processor shall be governed by a contract or other legal act. You will thus need to ensure that a contract – a data processing agreement – is put in place with the processor addressing all the requirements set out in Article 28(3) GDPR.

Link - Data processing agreements

2.2.2.3. What if the processor falls under the GDPR, but your enterprise does not?

Your enterprise – as a non-EU controller – will not become subject to the controller obligations under the GDPR. A “non-EU controller” will not become subject to the GDPR simply because it chooses to use a processor in the Union. The processor however will need to comply with the GDPR if he meets the criteria for GDPR applicability.

2.2.3. Who?

The GDPR protects natural persons regarding processing of personal data and rules relating to the free movement of personal data protection of natural persons. For SMEs it often concerns personal data of clients, suppliers and employees.
The GDPR applies to controllers and processors – which can be natural persons, legal persons, government bodies, etc. irrespective of their size, sector, number of employees or turnover.

[Link – SMEs & the GDPR]

[Link – Is my company a data controller or a data processor]
3. SMEs and the GDPR

The application of the GDPR depends on the nature of your enterprise or organisation activities, not on its size.

The GDPR introduces a risk-based approach into data protection law. This means that activities posing high risks to individuals’ rights and freedoms, regardless whether they are carried out by an SME or by a large corporation, trigger the application of more stringent rules.

Nevertheless, the GDPR encourages the Union institutions and bodies, Member States and their supervisory authorities, to take account on the specific needs’ micro, small and medium-sized enterprises may have regarding the application of this Regulation.

Additionally, the Regulation also recognises the specific situation of micro and small companies (to a limited extend) by allowing, under certain conditions, that some of the obligations of the GDPR do not apply to certain SMEs.

READ MORE

- The obligation to appoint a DPO does not apply to SMEs when processing is not their main business and the processing does not pose specific threats to individuals’ rights and freedoms. Indicators for such threats are for example (1) processing sensitive data or criminal records (2) monitoring individuals or (3) large scale processing.

Link - Should my enterprise appoint a DPO?

- Companies with fewer than 250 employees do not have to keep records of their processing activities unless they regularly process personal data, pose a threat to individuals’ rights and freedoms, or process sensitive data or criminal records.

Link - Recording and managing content
3.2. Is my enterprise allowed to process personal data?

3.2.1. In a nutshell

For any processing activity of personal data, it is required to identify one or more valid ground(s) under the GDPR – known as a ‘lawful basis’ – to justify the collection, use and other forms of processing of personal data.

In today’s business world, companies may conduct several processing operations for different purposes. This entails that SMEs may rely on different legal bases for their different processing activities. It is however not possible to rely on more than one lawful basis for the same processing activity.

**Article 6 of the GDPR provides an exhaustive list of the possible lawful bases:**

- Contract
- Legal obligation
- Legitimate interest
- Consent
- (Vital interest)
- (Task carried out in the public interest or in the exercise of official authority)

Since the first 4 grounds for lawful processing are the most common in the context of SME’s businesses, we will only further elaborate on these grounds.

3.2.1.1. Contract

When you need to process personal data to comply with your contractual obligations, you can rely on the lawful basis “contract”.

Some contractual obligations cannot be performed without collecting and processing certain personal data. This is often the case for SMEs, which process personal data of their customers, employees or suppliers in order to be able to carry out a contract with the them.

Contract can also be used as a lawful basis by enterprises carrying out pre-contractual requests from potential clients (e.g., when a potential client asks a home repair company to provide a quote to paint his house). Only situations where requests originate from the potential clients and were not the initiative of the controller or any third party, are covered.

“Contractual necessity” should be interpreted strictly. This means that you must be able to demonstrate that processing personal data is objectively necessary for a purpose that is integral to the performance of the contract or for addressing the pre-contractual request (e.g. name of the contracting partner, contact data of a customer or client, delivery address etc.). On the contrary, processing which is useful, yet not objectively necessary, for performing the contractual service or for taking relevant pre-contractual steps will not be covered, even if it is necessary for your other business purposes.

**READ MORE**
To decide whether you can rely on “contractual necessity” to justify your enterprise’s processing activities, it is essential that you determine the precise substance and fundamental objective of the contract. Then, you need to be able to demonstrate how the main object of the contract cannot be performed without the specific processing of the personal data in question. Detailed background checks of potential customers or clients – such as health checks by an insurance company or credit reference checks by a bank – are not to be considered as necessary steps made at the request of the potential customer or client.

This does not mean that such processing activities are per definition illegal, the lawful bases of “consent”, “legitimate interest” or “legal obligation” could be applicable.

Example:

A customer goes to a small enterprise selling electronics and there he learns that the laptop he was planning to buy is currently out of stock. The customer orders the laptop and asks for it to be delivered to his home address when available. To be able to deliver the laptop – and thus perform the contract – it is necessary for the enterprise to process the customer’s name and address. If after the delivery of the laptop the enterprise wants to process the customer’s data to send promotional e-mails, this processing cannot be considered objectively necessary for the contract’s performance. In practice this means that the enterprise must resort to a different lawful basis that could be appropriate for processing for marketing purposes (e.g. consent or legitimate interest).

💡 The fact that certain personal data processing is included in a contract does not automatically mean that the processing is necessary for its performance!

### 3.2.1.2 Legal obligation

The GDPR has also foreseen the possibility to justify your personal data processing activities in case you find yourself in a situation where processing is necessary for compliance with a legal obligation of the controller.

To be able to rely on this lawful basis, the obligation to process personal data must be imposed by EU law or the applicable national law of an EU Member State (including secondary legislation or a binding decision of a public authority) and must be mandatory.

READ MORE

A contract, a voluntary unilateral engagement or a public-private partnership are examples that can never qualify as a legal obligation in this sense, when processing personal data beyond what is required by law.

It is important that the legal obligation on which you want to base your processing does not leave room for discretion as to the manner of compliance. This rules out provisions in instruments such as general policy guidelines. The legal obligation must be sufficiently clear regarding the processing of personal data it requires, referring explicitly to the nature and object of the processing. If this is not the case, you will have to look for another lawful basis for your processing.

Examples of valid legal obligations could be:
• A legal obligation of banks to consult an official list of registered debtors;
• An obligation on employers to report salary data of their employees to social security or tax authorities by using the employee’s social security number;
• An obligation on financial institutions to report suspicious transactions to the competent authorities under anti-money-laundering rules.

3.2.1.3. Legitimate interest

Sometimes personal data processing is necessary to pursue legitimate interests of the enterprise (or a third party). Those legitimate interests can serve as a lawful basis for processing, provided that the interests and (fundamental) rights of the individual concerned are not overriding such interests.

A legitimate interest is a clearly articulated benefit to your enterprise, to third parties or to society, that results from processing personal data in a lawful way. It must concern a real and present interest that is expected in the very near future, ruling out interests that are too vague or speculative. An interest can be considered as legitimate if it is in accordance with the applicable EU and national law.

READ MORE

The objective of the “legitimate interest” ground is to give controllers the necessary flexibility for situations where there is no undue impact on data subjects. In other words, it should not be a wildcard.

There exists no exhaustive list of what a legitimate interest can be but the GDPR and the “Art. 29 Working Party” (now: European Data Protection Board) give some examples:

• Processing to prevent fraud
• Ensuring the health and safety of staff
• Employee monitoring for safety or management purposes
• Physical, IT and network security
• (Direct) marketing and other forms of advertising
• Unsolicited non-commercial messages, including for political campaigns or charitable fundraising
• Exercise of the right to freedom of expression or information, including in the media and the arts
• Scientific research
• Historical, scientific or statistical purposes

Thus, a broad range of interests could potentially qualify as a “legitimate interest”. However, merely having a legitimate interest does not automatically mean that you are lawfully processing personal data. There should be a case-by-case assessment for every single personal data processing activity that is to be justified on the ground of “legitimate interest”.

When you decide to justify your personal data processing by relying on the legitimate interest ground, make sure to perform the 3-step assessment – or, the legitimate interest assessment (“LIA”).
3.2.1.3.1. How to conduct a LIA?

[video animation]

Based on the accountability and transparency principles, it is necessary to document and keep records of the legitimate interest assessment. This allows you to prove you conducted a LIA and to justify your decision to rely on “legitimate interests” for your processing activities.

For the ICO’s LIA template, please visit the SMOOK website.

Link – Principles relation to the processing of personal data

3.2.1.4. Consent

You could be allowed to process personal data when the persons concerned have given you their consent to do this.

“Consent” in the sense of the GDPR presents individuals with real choice and control. It should put individuals in charge, build trust and engagement, as well as positively benefit your enterprise’s reputation.

For the consent to be valid it should be freely given, specific, informed, and unambiguous.
A common misconception is that "consent" is the main basis for data processing. Although it plays an important role, it is certainly not excluded that, depending on the context, other lawful bases are more appropriate. Because of the strict, cumulative requirements for valid consent under the GDPR, it is better to be cautious about the use of "consent" and to merely fall back on this when no other lawful basis is better suited.

To be able to rely on “consent” as a lawful basis under the GDPR, it should be:

3.2.1.4.1. Freely given

This implies that a genuine choice to agree or not should exist for the person whose consent is requested. It rules out situations in which an imbalance of power or a dependency exists between you and the individual concerned, as this often leads to fear of negative consequences of the refusal of consent.

In case you are processing in the capacity of a public authority or an employer, you will need to be extra cautious when relying on consent!

Freely given consent also excludes the possibility of “bundling consent”. Consent cannot be made a condition for the provision of a contract or service since “consent” and “contract” are two distinct lawful grounds for processing personal data. Therefore, bundling consent with the acceptance of terms or conditions does not constitute valid consent under the GDPR.

Example: An SME selling bicycles processes address details of its customers in order to fulfil its contractual obligation to deliver the bicycles that were ordered to the correct locations. However, if this SME only delivers the bicycles under the condition that customers agree to processing their e-mail addresses for the purpose of sending promotional mail, it is not obtaining GDPR-compliant consent.

There should be “granularity” in obtaining consent: individuals should be free to choose for which individual processing activities and purposes to grant consent and for which not.

You should separate the different purposes of your processing activities and obtain consent for each of these activities while providing individuals with the choice to only agree to one of the processing activities!

Example: The owner of a local real estate agency asks for its clients consent to process their telephone numbers when they make an appointment to check out a certain property. The purpose thereof is to be able to contact the potential clients in case they are late. Moreover, the owner wants to sell these telephone numbers to renovation companies who will use the information for marketing purposes. Consent for both processing activities is asked, however, without the choice to solely agree to one of these processing activities. Consequently, this consent is invalid.

For consent to be freely given it should not result in any detriment. You should ensure that no negative consequences – such as costs or a downgrade of the service – follow from a refusal or withdrawal of consent.
Example: A company selling goods online wants to start targeting its advertisements to certain (groups) of people. Therefore, it asks the visitors of its website to consent to the tracking of their online behaviour. If visitors do not grant their consent, the company is not allowed to ‘punish’ them by providing them with a less favourable experience, for example banning them from opting for the fast delivery option.

3.2.1.4.2. Specific

GDPR-compliant consent should also be used for a specific purpose. From that it follows that consent may not be given as a general authorization to process the personal data for any purpose.

💡 A request for consent must be specific, separated from information relating to other matters, important and may not be hidden behind lengthy terms and conditions.

3.2.1.4.3. Informed

When relying on consent to justify the processing of personal data, you should always make sure that you provide individuals with the necessary information, allowing them to make a meaningful choice. This is also in line with the transparency principle, one of the main principles upon which the GDPR is built.

**Link – Principles relation to the processing of personal data > Transparency principle**

What kind of information should you provide?

- The identity of the controller (your enterprise) and the purposes of the processing for which the personal data are intended
- The type of data that will be collected and used;
- The existence of the right to withdraw consent;
- If the data is to be transferred to, or processed by, other controllers who wish to rely on the original consent, these controllers should all be named. (it is not necessary to name processors)
- The information that is part of your privacy policy.

How should you provide this information?

Requests for consent need to be intelligible, easily accessible, using clear and plain language. To decide this, it is essential that you consider your audience. Many of the required information will be provided through your privacy policy, to which you provide a link in your consent request.

3.2.1.4.4. Unambiguous

A final requirement for valid consent is that it should be unambiguous. This means that consent should be obtained by statement or a clear affirmative action to avoid confusion.

<table>
<thead>
<tr>
<th>Do’s</th>
<th>Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require the ticking of an unticked box to obtain consent</td>
<td>Do not interpret silence or inactivity as consent</td>
</tr>
</tbody>
</table>
Provide individuals with the possibility to actively choose technical settings to allow the use of cookies or other conduct that clearly indicates that the individual accepts the proposed processing

Do not use pre-ticked boxes

Time for action - draft an informed consent form.

An informed consent form is a document setting out specific information about the personal data processing you undertake and for which you want to obtain the individual’s consent. All the information set out above should be included and all the requirements for obtaining valid consent should be considered in the drafting of this document.

Besides the 4 requirements for valid consent, it is of the utmost importance that your company can grant and accommodate individuals’ right to withdraw consent.

READ MORE

• Allow individuals to exercise the right to withdraw consent at any time.
• Information on the right to withdraw consent and on how to exercise it should be provided upon request for consent.
• Withdrawing consent should be made as easy as giving consent and should not require undue effort. Changing to another electronic interface (website, app or email) just for withdrawing consent is not allowed.
  
  E.G. Consent obtained through ticking a box on a website, should not have to be withdrawn by contacting a call center

It should not necessarily take place through the same action

• Withdrawing consent should not lead to any detriment for the individual concerned.
  
  E.G. no fee, no lowering of service levels

In principle, data processed on the basis of consent needs to be deleted when consent is withdrawn or is no longer valid, unless another lawful basis can be relied upon to justify the continued processing of the personal data!

Subsequent to the accountability principle, companies must keep records to prove consent was validly obtained. The records should allow them to easily identify (and prove to the supervisory authority where needed):

• Who: Which individuals gave consent?
• When was consent obtained?
• How was consent obtained?
• What: To what exactly did the individuals agree?

3.2.2 Special categories of personal data
Special category data is personal data that is deemed more sensitive, and hence, in need of more protection. Processing such data could create more significant risks to a person’s fundamental rights and freedoms (e.g. unlawful discrimination).

The GDPR lists 10 special categories of personal data:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for id purposes);
- Health
- Sex life
- Sexual orientation.

In principle, the processing of special categories of personal data is prohibited (Art. 9(1)GDPR). This general prohibition is lifted only if – additional to a lawful basis for your processing – one of the specific conditions exhaustively listed in the GDPR (Art. 9(2)) is satisfied. Any other processing of special categories of personal data is unlawful.

Therefore, before starting to process sensitive data you must determine whether any of the GDPR justification grounds apply and you should document it.

Not all legal bases are relevant for SMEs, you will most commonly be able to rely on the following grounds:

- Explicit consent of the individual whereby the individual will indicate that he or she understands and agrees that special categories of personal data will be processed (unless prohibited under national law!).

This form of consent is even stricter than the usual high standard of consent under the GDPR, which requires all consent to represent a specific, informed and unambiguous indication of the individual’s wishes. Explicit consent requires the strongest form of agreement by additionally requiring the person concerned to give an express statement of consent (E.G. by way of a written statement) while referring to the element of the processing that requires explicit consent.

In practice, this means that consent inferred from a person’s actions is not a form of explicit consent. This does not exclude pre-written consent statements, as long as you ensure that individuals can clearly indicate they agree with the statement (E.G. by ticking a box or signing the statement).
Explicit consent can also be obtained orally, but in that case a record of the script should be kept!

- Processing in the field of employment, social security and social protection law if authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- Processing necessary for the establishment, exercise or defence of legal claims.
- **Processing for individual health care purposes**
  - Processing necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. SMEs should assess whether specific EU or national legislation is adopted authorizing them to process the data.
  - Processing pursuant to a contract with a health professional, carried out by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies. E.g. doctors or psychologists

**Time for action -**

- It is very important to still check the national law of the country in which you are processing special categories of data, as the GDPR leaves room for Member States to introduce additional conditions and safeguards.
- Due to the sensitive nature of these types of personal data, it is important to place special emphasis on data security! Appropriate technical and organisational measures should be put in place, such as access restrictions, encryption, etc.

3.2.3 **Specific rules for consent & children**

**Link – Consent and children’s data**
3.3. Is my enterprise a data controller or data processor?

3.3.1. In a nutshell

Every time you process personal data, you will do so either as a data controller or as a data processor. It is very important to know in which of these roles you are operating for each and every data processing activity you undertake. This is because the legal obligations you will bear, differ according to this qualification.

This section aims to clarify when your company will qualify as a data controller, or rather a processor.

3.3.2. When am I a data controller or a data processor?

[video animation]

3.3.2.1. Controller or processor?

<table>
<thead>
<tr>
<th>Guiding questions</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did you take the initiative to start collecting or processing in any other way personal data?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Did you decide the purpose of the processing?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Did you decide which types of personal data are to be collected and from which types of individuals?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you giving instructions to another entity processing personal data, rather than following instructions from someone else?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you the party mainly benefiting from the result of the processing?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a direct relationship with the individuals concerned (e.g. a contract or employment)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you monitor other entities’ execution of the service?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your enterprise visible to the individuals concerned? (Visibility comes with expectations from the individuals) The lower the visibility towards the individuals, the more likely you are a processor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you the enterprise with the highest professional expertise?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The more you have indicated ‘yes’, the more likely you are a controller. Mainly ‘no’ answers indicate that you are probably acting as a processor. If you answered “yes” on the second question, you are a controller in any way.

3.3.2.2. Or joint controller?

<table>
<thead>
<tr>
<th>Guiding questions</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you have a common objective and purpose with other parties regarding the processing?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you using the same set of personal data for this processing as another controller?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have you designed the process with another controller?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Do you have common information management rules with another controller?

In case you have indicated ‘yes’ once or more, you are most likely processing personal data as a joint controller.

3.3.3. Obligations and liability

If your enterprise is acting as a controller, you will carry the highest level of compliance responsibility: you will not only have to comply with all the data protection principles as well as all other GDPR requirements, you will also need to be able to demonstrate compliance.

[Link – Accountability’ under the ‘data protection principles]

3.3.3.1. For Data controller

[Link – demonstrate compliance? where is this?]
Controller obligations under the GDPR

Comply with the GDPR
Take appropriate technical and organisational measures to ensure implementation of the data protection principles and data protection by design and default.

Records of processing activities
Document how, for which purpose(s) and on which ground(s) you are processing personal data (if necessary).

Data breaches
Notify your data protection authority within 72 hours after becoming aware and notify the individuals concerned without undue delay (Exemptions are possible)

Demonstrate compliance
Document all measures taken to comply with the GDPR in order to be able to prove these efforts and their effectiveness. Also include a review and update policy in regard of these measures.

Choice of data processer(s)
If you work with a processor, opt for one who provides sufficient guarantees in light of the GDPR requirements. Also put in place a written data processing agreement.

Ensure security of processing
Implement adequate technical and organisational measures that correspond to the specific risk(s).

Prior risk assessment (always) and DPIA (under certain circumstances)

Designation and proper involvement of a DPO (if necessary)

Cooperate with your data protection authority

Additionally, as a controller you are responsible for the compliance of your processor(s). Below you can find a short summary of all controller obligations under the GDPR.

3.3.3.2. For data processor

New under the GDPR is that processors also carry a limited number of specific legal obligations, however, a lower level of compliance responsibility will be applicable. In a scenario where your enterprise acts as a processor, your obligations are the following.

As a processor you can only process data in accordance with the controller’s instructions, unless you must process data pursuant to a legal obligation. If the latter is not the case and instructions were disobeyed, you will be requalified as a controller.

If a processor is responsible for a breach, it will be legally liable and individuals or supervisory authorities can bring claims for compensation and damages.
3.3.3.3. For joint controllers

In a situation of joint controllership, you will also have to fulfil all obligations aimed at controllers. For an overview of all these obligations, see section on Data controller.

[Link - For Data controller]

Additionally, as a joint controller, you will need to draw up an agreement to establish clear arrangements with the other controller(s) regarding the division of duties, tasks and responsibilities, unless these are already determined by EU or Member State law.

A contact point should also be designated for individuals concerned, to which they can turn in case of questions or complaints.

Regardless of the agreement between joint controllers, joint controllership implies joint liability: each controller can be held fully liable, vis à vis affected individuals, for the entire damage caused. The data subject is thus entitled to bring a claim against whichever of the joint controllers he or she wishes. This is to ensure that the data subject is effectively compensated.

Afterwards, the joint controller who paid the compensation can seek to recover damages from any other joint controllers involved in the joint processing. An exemption exists only if the controller is not in any way responsible for the harm.

3.3.4. Data processing agreements
In practice, many companies turn to third parties to process personal data – also SMEs!

Think of an email client, a cloud storage service or website analytics software. In all these situations, the GDPR requires you to put in place a data processing agreement with all the third-party services providers.

A data processing agreement is a legally binding document between the controller and the processor, in writing or in electronic form. It governs the specificities of data processing (which type of data will be processed, for which purpose, on which ground will the processing take place etc.), as well as the relationship between the controller and the processor – including the rights and obligations. Besides the fact that a data processing agreement is required by law, it also assures you that the data processor you are using is qualified and competent.

**READ MORE**

There are eight topics that need to be included in a data processing agreement:

1. The processor will only process personal data according to documented instructions of the controller – unless there is a Union or Member State law applicable to the processor
2. All persons authorised to have access to the personal data, are committed to confidentiality
3. The processor will ensure security of personal data by taking all reasonable, appropriate technical and organisational measures under article 32 GDPR.
4. The processor will not subcontract data processing activities to another processor, unless instructed to do so by the controller (in that case a data processing agreement will also need to be drafted with the sub processor in question)
5. By taking the possible and appropriate technical and organisational measures, the processor will assist the controller in fulfilling the latter’s obligation to respond to request for exercising data subject’s rights
6. Based on the nature of processing and the information available to the processor, the processor will also assist the controller in maintaining GDPR compliance with regard to security of processing (article 32) and the obligation to consult the data protection authority before undertaking high-risk processing (article 36)
7. The processor will delete all personal data after completion of services relating to processing or will return the data to the controller (choice of the controller)
8. The processor will provide the controller all information necessary to demonstrate compliance and will allow the controller to carry out an audit and will aid if requested to do so.

The European Data Protection Board (**EDPB**) wants companies to do more than just simply reiterate the GDPR provisions, it encourages to specifically define processes around the processor’s obligations. For example, determine specific steps for the processor to address an access request by an individual or to describe in detail the purpose and nature of the processing activities carried out on behalf of the controller, as well as the type of data processed, categories of individuals concerned and the duration of the processing. The Board also suggests including the list of the sub-processors as an annex to the agreement.
By not entering into a data processing agreement in cases where this is required, you will risk a fine!

For the Danish template, please visit the SMOOK website.

Time for action -

- Before engaging in any processing activities, **make sure to assess whether you are a controller, processor or joint controller** in relation to the processing activities taking place.
- In case you are working with a processor, **draft a data processing agreement** between yourself and this processor, including certain mandatory provisions.
- In case you are acting as a processor, make sure you **do not go beyond the controller’s instructions** as this potentially constitutes a violation of data protection legislation, resulting in your enterprise being liable.
4. MENU 1 – HANDBOOK – COMPLIANCE

4.1. Where to start compliance?

4.1.2. In a nutshell

With all GDPR obligations, it can be quite difficult to see the wood for the trees and understand where to start with the implementation.

Don’t panic, you are at the right place.

Here we will provide you with a step-by-step guide on how to become GDPR compliant.

This implementation should be a general matter of common sense and organisation in your enterprise, not only a technical or legal project.

4.1.2. Follow the guide

[Links to specific processing situations, rights under the GDPR, appointment of a DPO, DPIA, etc.]

4.2. Consequences of GDPR non-compliance

4.2.1. In a nutshell
Not complying with the GDPR implies that you are unlawfully processing personal data of the persons concerned and or not taking the required safety measures.

This may mainly result in:

**A. Data breaches and theft of sensitive information such as trade secrets**

Many obligations following from the GDPR have as a purpose to ensure that you process personal data in a thoughtful way, adequately protection your (personal) data and entire ICT infrastructure against undesired access, both from within as from the outside.
This means that by complying with the GDPR, you will also better secure and protect your company against cyberattacks, data breaches, etc. Furthermore, duly organising the way data is used and accessed in your company, will also protect other sensitive business information and trade secrets from being easily accessed by unauthorized persons and/or leaked to third parties.

B. Complaints by customers, clients and employees

Citizens are becoming more and more aware of their privacy, of the importance of data protection and of the obligations of businesses with regards to data protection.

This means that also your clients, customers and employees may disapprove if you do not treat their personal data in a GDPR compliant way and my complain about this, to you, to third parties, to social media or to the government.

They may also try to use this against you, for example if there is a disagreement or a dispute about something related to your relationship with these persons, they may try to use your non-compliance in their favour. For example, by threatening to file a complaint at the data protection authority.

C. Administrative audits and administrative fines

The data protection authorities may start an audit, triggered by a complaint or on their own initiative, when they notice that some of your publicly available information or communications appears to be non-compliant.

In that case, you will have to demonstrate that you comply with all provisions of the GDPR, which will take time and effort. And if non-compliance is established, this may result in administrative GDPR fines, which may in theory amount up to 20 million euros (or 4% of the yearly worldwide turnover, if that amount is higher). In practice the altitude of the fines will be much lower and will depend on the kind of infringement and the effort you have already put in complying with the GDPR, but this is of course not something you want to test.

D. Other local criminal fines and criminal charges under national law

Depending from the countries in which you are active, local laws may impose criminal prosecution and fines in case of non-compliance.

E. You may become ineligible to participate to public tenders or to work for clients or customers who must be GDPR compliant themselves

When you provide services to public authorities or to customers or clients in regulated sectors, they will often impose on their suppliers to be GDPR compliant. Non-compliance may therefore exclude you from being able to participate to such projects or calls.

F. Negative publicity
Not being GDPR compliant may cause negative publicity, for example to clients who care about their privacy, by being called out by activists on social media or by being mentioned in the press when a data breach occurs.

📝 Time for action –

Start today with your GDPR compliance. Don’t know where to start? Read our section on "Where to start compliance?"
4.3. Should my company appoint a DPO?

4.3.1. In a nutshell

Under certain conditions, the GDPR obliges companies to appoint a DPO. DPO stands for “data protection officer”. The primary role of a DPO is to ensure that your company processes personal data of your staff, customers, providers or any other individuals in compliance with the applicable data protection rules. In light thereof, a DPO should assists your company to monitor data protection compliance, provide information and advice on your data protection obligations and act as a direct contact point for individuals with regard to all issues related to processing of their personal data and the exercise of their rights under the GDPR, as well as a contact point for the competent Data Protection Authority. As the DPO forms an integral part of the organisation, it is ideally placed to guarantee data protection compliance.

READ MORE

The fact that your company qualifies as a micro-enterprise or an SME does not – as such – free you from the potential obligation to appoint a DPO. The GDPR employs a risk-based approach in this context: the provisions on data protection officers (articles 37 – 39 GDPR) – while not explicitly mentioning the word ‘risk’ – do link the obligation to designate a DPO to the nature, scope and purposes of data processing operations and not to quantitative characteristics (e.g. number of employees) of the entity processing personal data. Mostly, micro-enterprises process personal data for managing their relations with employees, (potential) customers and suppliers, which likely qualifies as low risk. Nevertheless, small companies often also use personal data for (direct) marketing purposes or make use of new and more invasive data processing technologies which means that the provisions on the appointment of a DPO are also relevant for micro companies.

4.3.2. Should I appoint a DPO?

There are four situations in which a DPO must be appointed:
Important to note is that, even in case your company is not obliged to designate a DPO under the aforementioned criteria, you are still entitled to do so on voluntary basis.

4.3.3. **How to appoint a DPO?**

The DPO may either be a **staff member** of your company (or of your processor) appointed within the company, or you can **outsource** the position by means of a service contract with an individual or an organisation outside of the company.

Before appointing your DPO, you need to check whether the candidate has the necessary **(professional) qualifications**. All the statutory requirements, tasks and duties listed below should be fulfilled irrespective of whether the DPO is appointed internally or externally and on a mandatory or voluntary basis.

4.3.3.1. **Independence**
4.3.3.2. Data protection expert

When choosing your DPO, assess whether the candidate has expert knowledge of data protection law and practices, as well as the ability to fulfil DPO tasks. Knowledge in the relevant business sector and the functioning of the organisation represented by the DPO should also be taken into account.

4.3.3.3. Adequate resources

You must provide adequate resources to enable the DPO to meet its GDPR obligations and to maintain its expert level of knowledge. This concerns not only financial resources, but also time, infrastructure, staff and support through other services (e.g. HR and IT).

4.3.3.4. No conflict of interest

It is not prohibited to combine the position of DPO with another position but all risks of conflict of interests should be assessed and mitigated on a case by case basis.

Example:

A company’s head of the IT department monitors all user accounts and controls the right of access to the IT infrastructure possessing rights of remote access to users' device. The same person should not hold the position of DPO because a DPO should monitor whether the head of IT's activities of processing users’ data are compatible with GDPR requirements which likely results in a conflict of interest in case one person holds both positions mentioned above.

4.3.3.5. Secrecy or confidentially

---

23 See details at Guidelines on Data Protection Officers p.p.14 Sec.3.2
The DPO should not disclose any information relating to the performance of his or her tasks, except for two situations:

- The obligation to directly report on the fulfilment of the tasks agreed upon to the highest management level of your company
- Requests for information by the competent data protection authority or any other public authority or body in accordance with EU or national law.

! It is allowed to appoint more than one DPO for your company, as well as to appoint one single DPO for several companies depending on their organisational structure and size (e.g. a group of companies, several public authorities of the same sector or associations)!

! Note that the DPO is not responsible for the duty to ensure compliance with privacy and data protection laws, it remains mainly your company’s duty!

🛠 Time for action –

- In case of any doubts concerning the necessity to appoint a DPO, it is recommended to appoint a DPO.
- Check national law before appointing a DPO or deciding not to do so, as additional requirements potentially exist regarding the procedure of designation or notification.
- Do not forget to make the contact details of the DPO publicly available (e.g. on your website) and communicate them to the competent Data Protection Authority.
- Ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- Give the DPO appropriate access to personal data, processing activities and other services within the company so that he or she can receive essential support, input or information.
- In case you decide not to follow the DPO’s advice, document the reasons justifying this decision.

4.3.4. Further reading


The UK Data Protection Authority has designed a useful tool to help you decide whether you should appoint a DPO. You can consult the tool here: https://ico.org.uk/for-organisations/does-my-organisation-need-a-data-protection-officer-dpo/.
4.4. Should my company carry out a DPIA?

4.4.1. In a nutshell

A data protection impact assessment (DPIA) consists of a set of assessments to be carried out by your company before starting your processing operations. A DPIA serves as a tool to systematically analyse, identify and minimise (not necessarily eliminate) the data protection risks of a single processing operation or a set of similar processing operations within your company. This assessment allows you to determine if the level of risk is acceptable in relation to the benefits pursued by the planned project.

‘Risk’, through the lens of data protection law, refers to the likelihood and severity of any physical, material or non-material negative impact on the individual concerned or society at large, taking into account the nature, scope, context and purposes of processing!

4.4.2. When to conduct a DPIA?

4.4.2.1. High risk processing operations

A DPIA is not always required under the GDPR. However, the mere fact that your company qualifies as a micro-enterprise or an SME does not – as such – give you a free pass. The obligation to carry out a DPIA is tied to the notion of ‘high risk’: if the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals, a DPIA is required.

To decide whether a project poses a high data protection risk, the article 29 Working Party (WP 29) – now European Data Protection Board (EDPB) – provides a rule of thumb: a processing activity that meets 2 or more out of the 9 criteria enlisted below most likely constitutes a high risk to the rights and freedoms of the individuals concerned and therefore requires a DPIA to be carried out.
In some cases, you could still consider that a processing activity meeting only 1 of the 9 criteria requires a DPIA.

Example:

<table>
<thead>
<tr>
<th>Processing activity(s)</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing personal data gathered across social media platforms to create marketing profiles.</td>
<td>Evaluation or scoring</td>
</tr>
<tr>
<td></td>
<td>Matching or combining of datasets</td>
</tr>
<tr>
<td></td>
<td>Large scale processing</td>
</tr>
<tr>
<td>3 out of 9 criteria are met 🡪 DPIA necessary!</td>
<td></td>
</tr>
</tbody>
</table>

To find out if you are required to carry out a DPIA, check out our pre-DPIA template.

**LINK - Is my enterprise allowed to process personal data?**

**4.4.2.2. National DPIA lists**
The GDPR instructs national data protection authorities (DPAs) to draw up their own lists of processing operations which are subject to the requirement for a DPIA. Additionally, they are free to also make a list of processing operations which do not require a DPIA. If your DPA has such a list, it is important to check this list before starting any data processing operations. National DPIA lists can be found here.

4.4.2.3. Uncertainty

In case it is not entirely clear whether the processing activities performed by your company are likely to result in a high risk to the rights and freedoms of individuals, it is advised to carry out a DPIA. Taking into account that no criteria nor lists can be considered exhaustive as there could always be high risk processing situations that are not foreseen by law or by national DPAs, it is safest to carry out a DPIA in any case.

Moreover, conducting a DPIA should also be seen as a way of complying with the accountability obligations under the GDPR. It helps you to keep an oversight on the processing activities taking place within your company by documenting risks and demonstrating compliance with the data protection rules. Hence, it is good practice to perform a DPIA for any major project which requires the processing of personal data, even if not obliged.

4.4.3. How to conduct a DPIA?

After identifying the need for a DPIA, the following steps should be taken:

1. A systematic description of the envisaged processing operations and the purposes of the processing. If you rely on ‘legitimate interest’ as the lawful basis for the processing, this interest should be included in the DPIA

2. Conducting a DPIA is your company’s responsibility, whenever you are acting as a data controller. Nevertheless, you should consult your DPO, if appointed, as well as other actors

3. An assessment of the necessity and proportionality of the processing operations: (1) Is the processing of personal data in the planned manner necessary to achieve the envisaged purpose(s)? (2) Is the interference with the rights and freedoms of the individuals concerned not disproportionate in relation to the pursued purpose(s)?

4. An assessment of the risks to the rights and freedoms of data subjects (e.g. privacy)

5. An identification of the measures envisaged to address the risks (e.g. safeguards and security measures) and a demonstration of compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned

6. Keeping records of the outcomes

7. Periodical reviewing: processing activities are dynamic and can evolve quickly which could cause new risks to the rights of individuals. For that reason, you should periodically reassess whether the DPIA that was conducted before, still corresponds to the processing activities taking place within
your company at that time. If there is no DPIA in place, you should check whether the processing activities at that time do result in high risks to the rights and freedoms of individuals. In that case, a DPIA is necessary.

For templates to help you carry out a data protection impact assessment, please visit the SMOOK website.

4.4.4. When to consult the DPA?

If the DPIA indicates that the planned processing operations are high risk and find that it is not possible to implement measures to mitigate the identified risks, you should consult the competent DPA before starting to process any personal data.

In case of such a prior consultation, the DPA will advise you how to limit the risks relating to your processing. If your company implements the suggested measures, you will be allowed to start the planned processing. On the other hand, it is also possible that the DPA advises you to completely abandon the planned processing.

When you are able to identify mitigation measures that are able to cover the risks in a sufficient manner, no prior consultation of the DPA is required.

✏️ Time for action –

- Assess whether planned and existing processing activities are likely to result in a high risk.
- A DPIA is a living tool so update your DPIA when the circumstances surrounding the processing have significantly changed.
- Check the DPIA lists of the national DPAs.
- Ask for DPO’s advice if your company has appointed one.
- Do not forget to document your DPIA.
4.5. **When to still check national law?**

4.5.1. **In a nutshell**

This section of the Handbook highlights situations where national data protection law should still be consulted. Even though the GDPR aims to harmonise data protection law across the EU, in several cases the Regulation does allow Member States to adopt national laws which deviate from or supplement the GDPR. In practice, this means that for some data protection aspects you will encounter different rules from one Member State to the next.

! If you operate in more than one Member State, it is important that you consider the possible differences in national legislation!

A distinction should be made between areas where Member States must have national or regional laws and areas where Member States may have such laws.

4.5.2. **Areas in which Member States must have local laws**

- Personal data and freedom of expression: the exception for processing for journalistic purposes and purposes of academic, artistic or literary expression. Member States remain responsible for determining the balance between the right to privacy and the right to freedom of expression. If you are working in the media sector, note that you should carefully consider the fact that the rules in this area will differ from one Member State to the next.

- Personal data contained in official documents: Such personal data may be processed in order to reconcile public access to official documents with the right to the protection of personal data. Member States are responsible to balance the right to privacy and the need to process personal data where this is necessary in the public interest.

4.5.3. **Areas in which Member States may have national or local laws**

- Professional secrecy and its reconciliation with the right of personal data protection. Member States are free to put in place specific obligations regarding professional secrecy in certain sectors (e.g. law firms or banks).

- Processing for scientific, historical or statistical purposes: Member States can restrict data subject’s rights (to access, rectification, restriction of processing and to object) because they threaten to render impossible or seriously impair the achievement of those purposes, under the condition of setting out appropriate safeguards and if there is no risk of breaching the privacy of the data subject.

- Seeing that employment laws of Member States mostly remain outside the scope of legislative competence of the EU, the GDPR leaves room for Member States to create laws governing the relationship between the GDPR and national employment law. In practice, if your company operates in multiple Member States, you will face different requirements with respect to the processing of personal data of employees.

- Personal data of deceased persons

- Children’s age of consent
- Special categories of data
- Genetic, biometric or health data
- The use of surveillance camera’s
- Rules about Data Protection Officers
- National identification numbers (any other identifier of general application). Member States are free to set their own rules regarding the processing of national ID numbers.
- Under certain conditions churches and religious establishments are allowed to impose rules on the processing of personal data

✍ Time for action –

Consider which Member States’ laws apply to your operations and go check national data protection law for additional or more specific obligations.
4.6. Data breaches: now what?

4.6.1. In a nutshell

4.6.1.1. Personal data breach

Any of the following situations are data breaches:

- The personal data you process is, seen, received, accessed or accessible by/to unauthorized persons
  - Examples:
    - a file with personal data is sent to the wrong person.
    - an unauthorized person has had access to your systems and may have been able to access, copy, view, destroy, etc. personal data.
    - a database with personal data was open for the public to access it and you cannot determine with certainty whether it was accessed or not.
• some employees had “read-only” access to personal data to which they were not allowed to have access and you cannot determine with certainty if they accessed it or not.
• an account of an employee has been hacked and you cannot determine with certainty if the hacker accessed the personal data that the employee has access to.

• The personal data is **lost, destroyed or damaged**.
  
  o “destruction”: the data no longer exists or no longer exists in a form that is of any use to the controller.
  o “damaged”: personal data has been altered, corrupted, or is no longer complete.
  o “lost”: the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession.
  o Examples:
    
    ▪ a laptop or storage media is lost (such as a USB-stick), even if the device is encrypted.
    ▪ a file that contains personal data cannot be retrieved.
    ▪ a file with personal data is encrypted by ransomware.
    ▪ the password of an encrypted file with personal data is lost and there are no other, accessible copies of the file.

4.6.1.2 **Notification to the data protection authority**

• The controller must notify data breaches to the data protection authority within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons (e.g. the data were encrypted).

• If the breach is not notified within 72 hours, the controller must inform the data protection authority of the reasons for the delay.

• A notification may be made in phases, i.e. the available information can be part of the initial information and additional information can be added to the file later.

• The notification must include at least the following information:
  
  o the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
  o the name and contact details of the data protection officer or other point of contact from which further information can be obtained, the likely consequences of the breach.
  o the measures taken or proposed by the controller to address the data breach including, where appropriate, measures to mitigate any possible adverse effects.

• The controller must adequately document all personal data breaches, including the related facts, effects and the remedial measures taken.

4.6.1.3 **Notification to the persons concerned**

• When a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the controller must inform the data subjects of the breach without undue delay.
• The controller must describe, in clear and plain language, the nature of the personal data breach and indicate:

  o The name and contact details of the data protection officer or other point of contact from which further information can be obtained, the likely consequences of the personal data breach.
  o The measures taken or proposed by the controller to address the breach including, where appropriate, measures to mitigate any possible adverse effects.

• If the controller does not inform the data subjects of the breach, the supervisory authority, after having assessed the risk posed by the breach, may require it to do so.

• The controller does not need to inform the data subjects of the personal data breach if:

  o it has implemented appropriate technical and organisational protection measures which were applied to the personal data affected by the breach, in particular measures, such as encryption, that render the personal data unintelligible to any person who is not authorised to access them;
  o it has subsequently taken measures to ensure that a high risk to the rights and freedoms of the data subjects is no longer likely to materialise; or
  o doing so would involve disproportionate efforts, in which case it shall make a public communication or take similar measures to ensure that the data subjects are informed in an equally effective manner.

• The processor’s role. The processor must notify the controller without undue delay after learning of a personal data breach.

4.6.1.4. A data breach policy

Establish a data breach policy in which you describe how your employees should react when a data breach occurs, who they should inform etc. And make sure that you inform your employees about the content of this policy.

4.6.1.5. A record of data breaches

A record of data breaches must be established. In this record, you should not only note the data breaches that required notification, but also data breaches that remained below the notification threshold.

✏️ Time for action –

  • Assess the technical and operational security measures in place within your organisation and make the appropriate adjustments, if necessary.
  • Establish a data breach policy and a record of data breaches
  • Have your systems tested regularly by an external party?
  • Put in place an appropriate data breach notification procedure.
  • Train your employees and contractors in security awareness.

4.6.2 Sources

Art. 33-34 GDPR
Guidelines wp250rev01
5. MENU 1 – HANDBOOK – GDPR PRINCIPLES AND RIGHTS

5.1. Principles relating to the processing of personal data

5.1.1. In a nutshell

The GDPR (article 5) sets out seven key principles underpinning the processing of personal data by any entity, including micro-enterprises or SMEs. Therefore, (1) lawfulness, fairness and transparency, (2) purpose limitation, (3) data minimization, (4) accuracy, (5) storage limitation, (6) integrity and confidentiality, as well as (7) accountability are relevant guidelines for you to keep personal data of your customers, employees and suppliers safe.

5.1.1.1. Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the individual. Personal data can only be processed lawfully if it is covered by a “lawful basis”.

The processing of personal data must be fair, appropriate, reasonable and proportional in relation to the individuals concerned. This means that an enterprise processing personal data must weigh its own interests against those of the individuals concerned before starting the processing.

Transparency requires your enterprise to be open and clear about the processing of personal data. The person concerned should be made aware why their data is being processed, of the risks, of their rights and of other important aspects.

5.1.1.2. Purpose limitation

Personal data may only be collected when linked to a concrete purpose. According to the purpose limitation principle, the purpose(s) should be specific, explicit and legitimate (in accordance with...
the law). In addition, collected data must only be processed in a way that is compatible with the initial goal of collection.

💡 Lawfully collected data for a given purpose cannot be used anew for purposes defined over time.

If you originally collected the data based on legitimate interest, contract or vital interests, the personal data can only be used for another purpose after checking whether the new purpose is compatible with the original purpose.

Elements to consider when assessing compatibility of purposes:

- Is there a link between the original purpose and the new purpose?
- the context in which the data was collected (what is the relationship between your enterprise and the individual?);
- What type and nature of data does it concern? (e.g. sensitive data?);
- What are the possible consequences of further processing for the individual concerned?
- Are there any appropriate safeguards in place, e.g. encryption or pseudonymisation?

If your enterprise originally collected the data based on consent or based on a legal obligation, you are not allowed to further process the data beyond what is allowed by the original consent or the legal provision(s). In this scenario, further processing requires obtaining new consent or a new legal basis.

5.1.1.3. Data minimisation

The data minimisation principle requires an enterprise to only collect personal data which is truly necessary for the specified processing purposes.

Therefore, it is useful to identify, in advance, the minimum amount of personal data needed to fulfil the enterprise’s purpose.

E.G: To perform a delivery, a footwear manufacturer collects its customers’ addresses, though it must not collect, for example, customers’ age as they are not related to the initial purpose of data collection.

5.1.1.4. Accuracy

According to the GDPR’s accuracy principle, legal entities, including micro-enterprises, must ensure that personal data they keep is accurate and updated, to the extent that is reasonable. This is because, under certain circumstances, inaccurate data could cause significant negative effects to the individual, especially when dealing with special categories of data (e.g. health or political beliefs).

E.G: Inaccurate data provided to a credit information bureau on a person's debt can negatively affect that person’s future chances to obtain a loan.

The extent to which data should be kept accurate depends on the purpose of data processing. For example, in case of a medical record, every possible step must be taken to ensure that the records
are up to date, while an enterprise should not take extreme actions (e.g. tracking customers) to update information in a less important context, such as marketing.

E.G: The enterprise should update an employee’s payroll data if it gives the employee a pay rise, or a customer’s delivery address to ensure that the purchased products are delivered to the right place.

5.1.1.5. Storage limitation

The storage limitation principle requires that personal data must not be maintained for longer than is necessary to fulfil the goal of their collection. Data must be erased when the data processing purpose is achieved. This means that storing any data longer than necessary is not permitted.

5.1.1.6. Integrity and confidentiality

Protection of personal data against unauthorized or unlawful processing, accidental loss, destruction or damage is at the core of the principle of integrity and confidentiality. The GDPR requires to ensure that personal data is not available to everyone within an organisation, but only to those who have to work with the data. Personal data must also be protected against any external or third actors.

The intensity of security measures is directly linked to the potential risk of data processing operations. (The GDPR follows risk-based approach)

💡 Note that before deciding what measures are appropriate to guarantee data security, your enterprise should assess potential information risks depending on the enterprise’s size, on the amount and nature of the processed personal data, as well as on how the data are used!

5.1.1.7. Accountability

The principle of accountability anticipates two obligations: an obligation to ensure compliance and the ability to prove it.

All the necessary technical and organisational measures should be adopted, and evidence thereof should be kept. There is no list of specific means to prove GDPR compliance, but the GDPR does – under certain circumstances – require you to keep records of your data processing activities, to appoint a DPO and to conduct DPIAs. The foregoing could serve as proof of compliance.

📝 Time for action –

Assess carefully what is your enterprise’s lawful basis for personal data collection:

- If all your enterprise’s data processing operations are brought to the attention of the individuals concerned;
- If personal data is only being collected for specific and currently existing processing purposes and not for unclear future needs;
- If your enterprise only processes the minimum amount of data necessary to fulfil its processing purpose(s);
- If the personal data held by your enterprise collected is accurate and updated;
• If all personal data for which the purpose(s) of their collection is achieved or personal data which is not relevant anymore, is deleted;
• If personal data is only accessible to individuals within the enterprise who actually need to have access;
• If your enterprise has made the necessary technical and organisational efforts to meet the GDPR principles;
• If your enterprise keeps records of its processing activities.
5.2. What rights do persons have under the GDPR

5.2.1. In a nutshell

The persons whose data is being processed remain in control of their own personal data. Therefore, you must:

1. Inform them if you process their data, what data you process, on what legal bases you process their data, etc
2. and, upon their request:
   a. correct their data
   b. entirely or partly stop using their data
   c. delete their data and “forget” them
   d. provide them with a machine-readable copy of their data, to allow them to use it with another service provider (a competitor of yours)
   e. stop using their data for marketing purposes or automated decision-making, including profiling

The GDPR grants several rights to individuals in order to empower them to exercise more control over the processing of their personal data, including allowing them to understand how and why their data is being processed.

In general, requests relating to these rights should be complied with (or at least answered) within 30 days.

These requests can be submitted to you both orally and in writing.

5.2.2. The different rights

The following rights will be discussed in the following topics:
5.2.2.1 Right to be informed

5.2.2.1.1 In a nutshell

Individuals must be informed about the collection and use of their personal data. This information should be communicated at the following moments:

- At the time you collect their personal data from them.
- If you obtained the personal from someone else, at the latest one month after obtaining the data.

This information should mainly be provided via your privacy policy (see below).

Essentially, you must inform individuals about the following:

- Why, how and for how long you will process their personal data?
- With whom do you share the data?
- What are their rights?
- How will you protect their data?

The information must be easily accessible and written in clear and simple language. To assess whether these conditions are fulfilled, you should consider your target audience.
When you collect personal data of an individual, you must clearly inform that person that you will process his or her data.

In most cases, this happens via a form or an agreement by which the personal data is collected, including a clear reference to your privacy policy which contains further information.

Hereafter, an example of disclaimer:

“We will only process your personal data for the purposes mentioned above. We will not share your personal data with third parties other than for this purpose. Please read our Privacy Policy [link to your privacy policy] for more information on how we protect and process your personal data.”

Your privacy policy should contain the information as indicated under “A waterproof privacy policy”.

When using personal data for marketing communication, you should always inform the individuals about the way you process their data.

Based on the GDPR and on other applicable legislations, every commercial email should:

- Contain:
  - a link to your privacy policy,
• Be clearly identifiable as a commercial email. If such purpose would not clearly result from the format/design of the email, the commercial purpose must be mentioned explicitly in the header of the email (e.g. by explicitly mentioning “advertising” or “commercial message” in the header of the email).
• Ideally (but not mandatory) mention why you are sending emails to this person (for example: "You are receiving this email because you have indicated in the past that you wish to be informed about our products")
• Depending on the country/countries in which you operate, other/different obligations may be applicable.

Considering the above, the footer of your emails may need to contain the following message to be compliant (for example):

“Your privacy is important to us; we process your data in accordance with the relevant privacy rules. If you wish to no longer receive our e-mails, you can unsubscribe at any moment by clicking on this link (insert link). Please find more information on how we process your data in our Privacy Policy (insert link).

© 2019 – Company and legal form – Address, Country, Company registration number – phone number and email address”

---

5.2.2.2 Right of access

5.2.2.2.1 In a nutshell
Any individual has the right to know if you are processing his or her personal data, to obtain information about that processing and to obtain a copy of the data concerned.

You must be able to grant requests of individuals to access their data.

5.2.2.2.2. What to provide

When you process personal data of an individual in the capacity of a controller, you must provide that individual with the following information:

1) That you are processing his or her data  
2) A copy of the data  
3) Additional information

READ MORE

5.2.2.2.2.1. A copy of the data

You must provide a copy of the processed personal data to the individual. In principle, you have to grant this request free of charge. Where additional copies are requested, you may charge a “reasonable fee”, based on the actual costs.

If the access request is made by electronic means, the data must be provided in a commonly used electronic form (except if the individual requests otherwise).

By providing a copy of the data, you should not infringe the rights of others. So, if the data would give insights in the personal data of others, you must balance their rights against each other and evaluate if the data can be released to the applicant or not.

5.2.2.2.2. Additional information

You must specifically provide the following information to the individual:
• A copy of the personal data being or to be processed
• The categories of personal data concerned
  for example: contact data, financial data, purchase history, etc
• The purposes of the processing
  for example: to be able to deliver specific services, to be able to perform payment, marketing
  purposes, etc.
• The recipients or categories of recipients to whom the personal data have been or will be disclosed. And in particular recipients in third countries
  for example: your hosting provider (such as Amazon Web Services), your e-mail provider (such as Microsoft), your accountant, etc
• Where possible, the period for which the personal data will be stored or, if this information is not known, the criteria used to determine this period
• The data subject's right to request from the controller the rectification or deletion of personal data or a restriction on the processing of his or her personal data and to object to such processing
• The right to lodge a complaint with a supervisory authority.
• Where the personal data are not collected from the data subject, any available information as to their source
• The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
• The appropriate safeguards taken by the controller regarding transfers of personal data to third countries
• Regulated professions (e.g. doctors, lawyers, etc.) must ensure that access to personal data in the electronic mail system complies with any professional secrecy codes by which they are bound

The above information must be provided free of charge. If the individual requests additional copies, a reasonable administrative fee may be charged. If possible and feasible considered the circumstance and costs, it is recommended to provide remote access to a secure system allowing the individual to directly access his or her personal data.

READ MORE

If you process a large quantity of information about the individual, you can request that the individual specifies the information or processing activities to which his or her request relates.

If you process the personal data electronically, you should also, if reasonably possible, allow for individuals to request their access electronically. If the access request is submitted to you by
electronic means, you must provide the information in a commonly used electronic form, unless the individual requests otherwise.

If the access request would adversely affect your rights or the rights of a third party, you can refuse to provide certain information (such as trade secrets or information of other persons that is private).

5.2.2.3. **Right to request rectification**

5.2.2.3.1. **In a nutshell**

Individuals whose personal data you process are entitled to have their personal data corrected if it is inaccurate.

READ MORE

Personal data of individuals may be erroneous or outdated.

Besides your own obligation as a business to keep the personal data accurate (your “accuracy” obligation), the individuals whose data you process, are entitled to demand that you correct their personal data.

The rectification of inaccurate personal data concerning an individual, must be done without undue delay upon the individual’s request.

Depending on the purposes of the processing, the individual also has the right to have incomplete personal data completed.

5.2.2.4. **Right to request erasure or deletion of data – the right to be forgotten**

5.2.2.4.1. **In a nutshell**
Under some circumstances individuals whose personal data you process, have the right to have their personal data erased or deleted.

**READ MORE**

You must erase personal data of individuals upon their request if:

- you do not need the personal data any longer for the purpose for which it was originally collected or processed
- the consent upon which your processing is based, is withdrawn
- an individual object to processing by you of his/her personal data, when you rely on your legitimate interest for such processing and you cannot invoke an overriding legitimate interest to continue this processing
- the request relates to personal data processed for direct marketing purposes and the individual objects to such processing
- you are processing the personal data unlawfully
- you have to erase it to comply with a legal obligation
- you process the personal data to offer information society services to a child.

If you have to delete the personal data but you already made it public, then you should take all “reasonable steps” to inform the other parties which are processing the personal data that, the personal data, any links to, and copies or replications of those personal data, must be erased. What “reasonable steps” must be undertaken, needs to be evaluated taking account of the available technology and the cost of implementation.

Exception: personal data must not be erased (and third parties must not be informed), if and to the extent that the processing of the personal data is necessary:

- to exercise the right of freedom of speech and information
- to comply with a legal obligation under EU or Member State law to which the controller is subject or to perform a task carried out in the public interest or in the exercise of official authority vested in the controller
- for reasons of public health.
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the provisions of the GDPR insofar as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of the processing; or
• to establish, assert or defend legal claims.

Time for action –
- Ensure you can recognise a request for erasure and understand when the right applies
- Decide how to record requests you receive verbally and ensure that your personnel are aware of this method
- Ensure that you and your personnel are aware of the information you need to provide to individuals and when you can refuse a request
- Have processes in place to ensure that you can respond to a request for erasure without undue delay and within one month of receipt.
- Be aware of the circumstances when you can extend the time limit to respond to a request.
- Understand that there is an emphasis on the right to erasure if the request relates to data collected from children.
- Have procedures in place to inform any recipients if you erase any data you have shared with them.
- Have appropriate methods in place to erase information.

5.2.2.5. Right to impose a restriction on processing

5.2.2.5.1. In a nutshell

Under certain circumstances, individuals whose personal data you process, have the right to ask you to stop using their personal data, without deleting it.

READ MORE

Individuals can request that, even though you can keep storing their personal data, you no longer use it.

In most cases, such a request will relate to a situation under which a person wants to maintain the proof that you process his or her data, but is of the opinion that you are not allowed to process it.

(a) An individual can demand the “restriction of the processing” of his or her data in the following circumstances:

(i) The individual challenges the accuracy of the personal data. The processing has to be restricted for a period enabling you to verify the accuracy of the personal data.
the processing is unlawful and the individual requests the restriction of their use, instead of the erasure of the personal data.

(iii) you no longer need the personal data for the purposes of the processing, but the individual requires the personal data for the establishment, exercise or defence of legal claims.

(iv) the individual objects to processing but you want to verify if you have legitimate grounds to keep processing that override the right of the individual for not having his/her personal data processed. Pending the verification of such legitimate interest, the processing of such personal data must be restricted.

5.2.2.5.2. If the processing of specific personal data is restricted, you can only process it in the following ways:

1. storing the personal data
2. processing for the establishment, exercise or defence of legal claims
3. processing for the protection of the rights of another natural or legal person
4. processing for reasons of important public interest of the European Union or of a member state of the EU
5. other processing is only allowed with the individual's consent

5.2.2.5.3. Clearly indicate in the system that the processing of the personal data in question is restricted. Some methods to restrict processing are:

1. making the selected data unavailable to users
2. removing published data from a website
3. transferring the selected data to another processing system
4. marking/tagging the data in a way that avoid that it’s being used (for instance in mailing lists which checks the tags before using the data) or moving the data to a “do-not-use”-mailing list
5. etc.

If you lift the restriction of the processing (and start to process it (again)), you must inform the individual thereof before the restriction of processing is lifted.

5.2.2.6. Right to data portability

5.2.2.6.1. In a nutshell
Customers and individuals whose personal data you process in an automated way, based on their consent or an agreement with them, are allowed to obtain a structured digital copy of the data they provided to you, to allow them to provide this data to another service provider (competitor) and have the third party use the data to provide its services or products.

READ MORE

The purpose of the right to data portability is to allow (mainly) customers whose personal data you process to easily switch to your competitors, while being able to keep using the data they have provided to you.

5.2.2.6.1.1. Who can exercise the right to data portability?

Any individual whose personal data you process by automated means, based on:

- an agreement, i.e. your customers and clients
- consent

5.2.2.6.1.2. What data do you have to provide to the individual?

The personal data that the individual has provided you with, this means:

- all the data the individual has knowingly and actively provided to you, such as his/her name, address, age, etc. provided through forms, through communication, by allowing you to obtain certain information at other instances, etc.
- all the data the individual had indirectly provided to you by using your services or devices, such as (if you collect this data) his/her purchase history, usage history, location data, etc. This second part only relates to the raw data, not the personal data you have inferred or derived from the data provided by the individual, such as a customer profile or an internal credit rating.

By providing such data, you may not adversely affect the rights and freedoms of third parties. This means that you must take care that you, for example, do not violate the privacy of other persons, by providing the individual and especially the other company with the personal data. Or infringe third party’s intellectual property rights by doing so. In this case, you should find a way that complies to the greatest extent with both rights (i.e. transferring the data but obfuscating or leaving out the data that infringes third party rights).
5.2.2.6.1.3 How do you have to provide the data?

You must provide the data in a structured, commonly used and machine-readable format.

If technically feasible, the individual can request that the you directly transfer his/her data from your system to the system of your competitor.

5.2.2.7 Right to object to the processing

5.2.2.7.1 In a nutshell

In general, individuals have the right to object against the processing of their personal data, when you are doing so based on legitimate interest or public interest or for the purpose of direct marketing. You must inform individuals whose data you process of this right.

READ MORE

1. Individuals have the right to object against the processing of their personal data, based on grounds relating to his or her specific situation, if:
   a. the processing is based on:
      i. your legitimate interest,
      ii. public interest, including profiling based on these grounds.

You do not have to stop processing in these cases if you demonstrate to have compelling legitimate grounds to continue processing which override the interests of the individual or for the establishment, exercise or defence of legal claims.

b. the processing relates to direct marketing, including profiling in relation to direct marketing
c. the purpose of the processing is scientific or historical research or has statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

2. Individuals whose personal data you process must be informed of this right:
   a. Information must be provided at the latest at the time of your first communication with the individual.
   b. This information must be
5.2.2.8. Right not to be subject to automated individual-decision making (including profiling)

5.2.2.8.1. In a nutshell

Individuals are entitled to demand that decisions that affect them, are made (at least in the end) by humans.

READ MORE

1. Individuals have the right not to be subject to decisions based solely on automated processing, including profiling, if such decision produces legal effects concerning them or similarly significantly affects them.

2. This right does not apply if the automated decision:
   (i) is necessary to enter into or perform a contract between you and the individual. For example, a bank will still be allowed to refuse you a loan if the computer says that you are not eligible.
   (ii) is authorised by the law applicable to you and such law lays down suitable measures to safeguard the individual’s rights, freedoms and legitimate interests; or
   (iii) is based on the individual’s express consent.

3. If the exceptions (i) or (iii) above apply and you are allowed to make automated decisions with legal effect, you must:
   (i) implement suitable measures to safeguard the individual's rights and freedoms and legitimate interests
   (ii) at least provide the right for the individual to obtain human intervention from your part, to express his or her point of view and to contest the decision

4. Automated decisions cannot be based on special categories of personal data, unless:
   (i) explicit consent was provided by the individual, OR
   (ii) processing is necessary for reasons of substantial public interest, AND
   (iii) suitable measures or in place to protect the individual’s interests.

5.2.3. The individuals’ rights under the GDPR
5.2.3.1. In a nutshell

When an individual exercise his rights under the GDPR, you must generally satisfy this request within 1 month.

READ MORE

5.2.3.1.1. Response time

- Within one month from receipt of the request of an individual you must:
  - either comply with the request
  - either inform the individual that the period is extended
  - either inform the individual that his/her request is refused

- Extension of the period
  - The one-month period may be extended by two additional months, if such extension is justified by the complexity and number of requests.

5.2.3.1.2. Refusing a request

If a request is unjustified, you must inform the individual that you will not comply with it, providing the reasons for not taking action and informing the individual that he/she is entitled to lodge a complaint with the supervisory authority and seek judicial redress.

5.2.3.1.3. Costs? Can you charge for satisfying the individual’s request?

Communications with an individual and actions taken regarding the individual’s rights shall be free of charge.

If an individual submits manifestly unfounded or excessive requests (for example repeated requests) you can either charge a reasonable fee or refuse to act on a request. It will be up to you to be able to prove that a request was manifestly unfounded or excessive.

5.2.3.1.4. How to provide the requested information to an individual?
If the request is sent to you by electronic means, you should provide the answer and the requested information by electronic means where possible, except if the data subject requests otherwise.

5.2.2.1.5. Keep in mind that the above described rights of individuals under the GDPR are not absolute. Some rights can only be exercised if specific conditions are met or under specific restrictions.

✏️ Time for action –

Put in place appropriate procedures to respond to requests of data subjects. The following factors should be considered: contact person for data protection requests, clear internal allocation of responsibilities, standard letters for refusal to act/extension.

Work closely with IT. It is important that your IT systems ensure compliance with the data subjects' rights (including the possibility to erase data)
6. MENU 1 – HANDBOOK – PROCESSING SITUATIONS

The purpose of this section is to address common practical concerns of micro-enterprises and to grant swift access to these topics by including them in the list under the menu button. This way, companies looking for an answer to one of these specific issues, will be able to navigate there directly and efficiently from anywhere within SMOOK.

The following subsections on specific processing situations will also be available to print or download as single factsheets (e.g. in pdf.).

6.1. Customers’ personal data

6.1.1. In a nutshell

Your customers provide their personal data to you for one or more specific purposes. This means that you cannot use this personal data for anything else (purpose limitation).

To a certain extent, you are however allowed to use your customers personal data to market products like the one they purchased from you. To be allowed to do this, you must however specifically make sure (1) that they are offered the possibility to refuse that their data is used for such marketing (opt-out) and (2) that they can easily unsubscribe from further receiving such marketing at any moments.

All the general requirements of course also apply, such as informing your customers on how you will process their personal data through your privacy policy.

6.1.2. Limited use of personal data

Under the GDPR you can only use personal data for the purpose for which it was provided to you (purpose limitation) and you cannot collect more information than required for such purpose (data minimisation).

This means in practice that, you cannot require your customers to communicate, for example, the following information if you do not strictly need this information to sell them your product or deliver your service:

1. Date of birth: if you want to obtain this to be able to send your customer a birthday card, than you should make this field optional (not mandatory) and explain why you request this information in so called meta-information (“providing your data of birth allows us to send you a card and/or promotion on your birthday”).
2. Gender: we understand that it is useful to know the gender of your customers to be able to know how to address them and maybe to be able to profile them. You cannot make this field mandatory, however. You can request the information adding in the meta-information “By choosing your gender, we know how to address you and we may be able, if allowed, to better define interesting products and opportunities for you”.
3. Names of their children and/or significant other,
4. Etc.

6.1.3. Sending marketing to existing customers and clients
You can send marketing to your existing customers, relying on your legitimate interest. This is called the “soft opt-in” for existing customers. You can only do this if the following conditions are met:

1. the customer must be given, the possibility to oppose against receiving such marketing, at the time that you receive their personal information
2. the customer must be given the opportunity to oppose further receiving marketing from you, every time they receive marketing communication. In practice this is solved by adding an “unsubscribe” button to every marketing email.
3. the marketing must relate to products or services similar or related to the products bought by such customer. For example, if you have a bakery you can send information about new products in the bakery to existing customers. If, besides the bakery, you also own a butcher’s shop that is not part of the same shop, then you cannot use data obtained from customers of the bakery, to send them information about your butcher’s shop.

Furthermore, of course, the fact that you are marketing your products to these customers, must be mentioned in your privacy policy.

### 6.1.4 General obligations with regards to personal data

In addition to the specific requirements above, all the other general requirements with regards to such processing also apply, such as duly informing your clients, protecting and securing their personal data, respecting their rights, etc.

### 6.1.5 Processing personal data on behalf of your customers or clients

If your customers provide personal data to you that they are processing and which you need to process on their behalf, you become a data processor.

This means that you will have to enter into a data processing agreement with them and that you can only use this data to perform your services. Follow the links for more information.

### 6.1.6 Legal bases to process your customers’ or clients’ personal data

In general, you will process your customers personal data based on the following legal grounds:

1. Contractual obligation: if you need to process their personal data to be able to perform your obligations. For example, if you need to deliver something to a customer, you need their name and address to be able to do so.
2. Legal obligation: if you are required by law to process specific information. For example, if your customer is subject to VAT, you’ll need to process their VAT-number by law.
3. Legitimate interest: if you have a legitimate interest to process some personal data of your customer, that overrides the interest of your customer not to have its personal data processed. This applies, for example, to the processing to send marketing to your existing customers and to the processing of contact details of employees of your customer.
4. Consent: if you need to rely on consent to be allowed to process personal data of your customer. You will need consent if, for example, you want to send your customers personalized information (marketing) or if you want to send marketing that is not covered by the soft opt-in described above.
Time for action –

Make sure that:

- you don’t use personal data of (contact persons at) your customers in other ways than allowed,
- you inform your customers about the ways you process their data,
- you use the correct legal bases to process your customer’s personal data,
- that your privacy policy contains the right mentions if you are using your customer’s personal data for marketing purposes,
- a data processing agreement is in place when you process personal data on behalf of your customers.

6.2. Suppliers’ personal data

6.2.1. In a nutshell?

Personal data from (contact persons at) your suppliers can only be used within the context of your agreement and relationship with them.

You will of course also need to use and store some of this information for tax and other administrative purposes.

6.2.2. General

In the same way as you cannot use personal data from customers or clients for any purpose, you cannot use personal data relating to suppliers for other purposes than the purposes for which you obtained these data (purpose limitation).

When you process personal data of contact persons (employees or other) of your supplier, your legal basis to do so is “legitimate interest”, because you do not have a direct contract with these employees.

In addition to the specific requirements above, all the other general requirements with regards to such processing also apply, such as duly informing your suppliers about your privacy policy, protecting and securing their personal data, respecting their rights, etc.

6.2.3. Legal bases to process your suppliers’ personal data

In general, you will process your suppliers’ personal data based on the following legal grounds:

1. Contractual obligation: if you need to process their personal data to be able to perform your obligations. For example, if you need to provide access to your supplier, you need their name to be able to do so.
2. Legal obligation: if you are required by law to process specific information. For example, if you are subject to VAT, you’ll need to process their VAT-number by law.
3. **Legitimate interest:** if you have a legitimate interest to process some personal data of your supplier, that overrides the interest of your supplier not to have its personal data processed. This applies, for example, to the processing of contact details of employees of your supplier.

4. **Consent:** if you need to rely on consent to be allowed to process personal data of your customer. You will need consent if, for example, you want to send marketing material to your suppliers.

🔗 **Time for action –**

**Make sure that:**

- you don’t use personal data of (contact persons at) your suppliers in other ways than allowed,
- you use the correct legal bases to process your customer’s personal data,
- you inform your suppliers about the ways you process their data.

6.3. **Data protection in an employment context**

6.3.1. **In a nutshell**

If you have employees, your use of their personal data is also governed by the GDPR, besides any national provisions that apply to your employer-employee relationship.

This means that you cannot just record or monitor your employees or obtain information about them from public sources or third parties, if this does not happen in compliance with the GDPR.

A particularity with employees is furthermore that it is very difficult to rely on their “consent” to process their information, because you as an employer are in a hierarchical position towards your employees. Consequently, most consents that they would give you, would not be “free” consents and therefore cannot be considered as a valid consent for you to process their personal data.

The other way around, you must ensure that your employees and staff:

1. deal safely with ICT and personal data,
2. understand the importance of data protection.

These reciprocal rights and obligations of your employees are laid down in the ICT Policy, the Data Policy and the Employee Privacy Policy.

These policies inform and teach your employees about the importance of data protection and the points of attention they need to apply when using your ICT infrastructure and/or handling personal data and about how their own personal data is processed.

Furthermore, you also have an obligation to make sure your employees are aware of the importance of privacy and data protection, by raising awareness about this subject, for example by organizing trainings and information campaigns.

6.3.2. **National law always applies**
When dealing with employees you should always consider that employment law is mainly governed by national law. Therefore, you will have to apply the principles of the GDPR in combination with the applicable national law provisions.

### 6.3.3 Rules and policies

Essentially, the rights and obligations will be governed by the following policies:

1. **ICT Policy**, in which you describe how the employees must use and are allowed your ICT infrastructure (including the devices and software) and how they can be monitored while using these.
2. **Data Policy**, in which you describe how your employees should handle personal data.
3. **Employee Privacy Policy**, which is in its essence a regular privacy policy, adapted to your relationship with your employees.
4. **Camera Surveillance Policy**.

These documents do not have to be separate documents and can all be part of one or more broader documents.

For these documents to be binding, it is most likely required under your national employment law that your work rules and/or employment contracts are amended accordingly.

### 6.3.4 No consent

You should avoid relying on your employees’ consent to process their personal data.

Your employees are supposed to be your subordinates, are in a weaker bargaining position than you as their employer and are therefore considered not to be able to refuse their consent. Most consents provided by an employee will therefore not be considered as “free” consents and will therefore be void.

The only situation in which you, as an employer, can rely on your employees’ consent, is when the consent relates to a clearly minor and unimportant matter, under which the employee cannot fear in any way that refusing their consent may be held against them later on.

### 6.3.5 Raising awareness

As an employer, it is your duty to ensure and prove (because of your accountability obligation) that you have duly raised awareness among your employees about the importance of data protection and privacy.

Therefore, you should not only organize trainings and information campaigns, but also make sure that you can prove that these happened.

### 6.3.6 Job applicants

You must also inform job applicants about how and why you will process their personal data.
These job applicants do not have access to your “employee privacy policy” so ideally you include the provisions related to job applicants in your public privacy policy.

Note that you:

• cannot retain information about applicants eternally (data minimisation and storage limitation), generally a maximum retention period of 2 years appears to be acceptable, except if specific circumstance justify a longer retention period or if you obtain consent to retain this personal data for a longer period,
• that you can only request information from them that is relevant for the job (data minimisation) and allowed by law. If you want to obtain sensitive information of your applicants, such as an extract of their criminal record, you will in many EU countries only be allowed to do so if you have a legal obligation or entitlemet to request this information,
• can only use public sources (such as social media posts and profiles) to evaluate the candidate, if the use of such sources is mentioned in your privacy policy,
• should add a notice under each job posting in which you (very) briefly describe that/how you will process the applicant’s personal data and refer to your privacy policy for further information.

6.3.7 Legal bases to process your employees’ personal data

In general, you will process your employees’ personal data based on the following legal grounds:

• Contractual obligation: if you need to process their personal data to be able to perform your obligations. For example, you need to know their name and address to be able to enter an employment contract with them.
• Legal obligation: if you are required by law to process specific information. For example, in many countries you may be required by law to process the employee’s social security number and information about their family, for example to communicate with the social security service.
• Legitimate interest: if you have a legitimate interest to process some personal data of your employee of job candidate, that overrides the interest of your employee/candidate not to have its personal data processed. This applies, for example, when you access public information about applicants.
• Consent: if you need to rely on consent to be allowed to process personal data of your employee. As described above, it should be avoided as much as possible to process personal data of an employee or of a job applicant based on their consent.

6.3.8 How can you ensure that your employees process personal data, and make use of your ICT environment, in a secure way?

In this blog post on the SMOOTH website, you can find several practical tips and guidelines on how you can organize your ICT environment in a secure way.

✍️ Time for action –
• Verify if you comply with the requirements above and implement the described policies.
• Make sure to also verify national legislation.

6.4. Camera surveillance

6.4.1. In a nutshell

When you use surveillance cameras to safeguard your buildings and/or company, you must also take the GDPR into account, besides any national provisions that may apply to different situations in which you can use surveillance cameras.

By filming locations where people may pass by, you are gathering personal information such as their images and their behaviour. If smart cameras are used that allow, for example, facial recognition or license plate recognition, sensitive information such as biometric information is also processed.

6.4.2. Check national law

Note that the use of (surveillance) cameras will first and foremost be governed by national law. Your national law may prohibit the use of specific or all cameras in all or some circumstance (for example when continuously filming public places), may impose specific requirements (for example in an employment context), may require that the used surveillance cameras are notified to and/or registered with the government, may require that the police has access to the images upon simple demand, may require that a specific pictogram is displayed to inform persons who may be filmed, etc.

6.4.3. From a GDPR point-of-view the following specific requirements apply

• The public/employees must be informed/notify of the video surveillance in a clear and effective way.
• Obligations to employees must be fulfilled (e.g. information provided, and provisions included in the company’s privacy policy and work rules).
• The company must comply with certain obligations relating to the processing, access to and storage of the images
• The company must make sure to add this processing in its record of processing activities and in its (public) privacy policy.

6.4.4. Informing/notifying the public

Most countries require the use of a specific pictogram at the entrance of a place where camera surveillance is organized.

For example, in Belgium, the following pictogram must be placed, on which specific information must be mentioned:
In general, the pictogram will have specific requirements with regard to the size, the material, the visibility, the information mentioned on the pictogram, etc.

From a GDPR point of view, any such notification must make it sufficiently clear to the persons being filmed:

- Who is responsible for the surveillance camera?
- The website where the applicable privacy policy (with more information about the video surveillance) can be consulted.

### 6.4.5 Obligations to employees

- When employees may be filmed, specific requirements under national law will most likely apply, which may impose specific limitations and requirements, specific information obligations towards employees and specific procedures to be followed before the surveillance cameras can be used.
- This information must also be included in the company’s employee privacy policy.

### 6.4.6 Obligations relating to the processing, access to and storage of images

Depending on your national legislation, specific obligations may apply, such as:

1. Surveillance cameras directed at an entrance door must be oriented in such a way that the (indirect) recording of public space is kept to a strict minimum.
2. Real-time viewing of the images of surveillance cameras is only allowed to be able to establish criminal acts at the time of the act. It is also allowed to show a publicly visible screen, on which the recorded images can be viewed in real time.
3. Images may be recorded only to gather evidence of a nuisance, criminal behaviour or acts that cause damage and to identify the perpetrators of such acts, the witnesses thereto or the victims thereof.
4. Footage may be stored for a maximum period of one month, unless it is established that it contains images related to a crime.
5. Persons may only be filmed after the required notification has been made and the pictograms affixed. Entering a room where a clearly visible pictogram is displayed is considered implied consent to be filmed.
6. The right to access and search the recorded images must be limited and a record kept of these actions.
7. Persons who have access to the images must be bound by a duty of confidentiality and discretion.
8. Images may not be recorded that violate the right to privacy of individuals or for the purpose of gathering information about philosophical, religious or political convictions, trade union membership, ethnic or socio-economic background, sexual orientation or the health of individuals.
9. All persons filmed have the right to view the video footage in which they appear, provided they can provide enough details in order to locate the images in question.
10. Etc.
In addition to such specific obligations, the obligations laid down in the privacy legislation and the GDPR also apply, considering the sensitive nature of video surveillance.

6.4.7. A record

- Pursuant to the GDPR, a record of processing activities must be kept for the processing of personal data, including video surveillance.
- National law may require that an additional record is established, in which specific information about the video surveillance is registered, for example:
  - an indication of the type of place that is under surveillance;
  - a technical description of the surveillance cameras as well as, for fixed cameras, their location, where applicable indicated on a map;
  - for temporary or mobile surveillance cameras, a description of the areas under surveillance by the cameras and the time periods during which the cameras are in use;
  - the means of providing information about the processing;
  - the place where the images are processed; and
  - whether viewing in real time is organised or not and, where applicable, the way it is organised.

6.4.8. Criminal sanctions

National legislation may impose criminal sanctions on the infringement of the video surveillance legislation.

📝 Time for action –

Verify if your surveillance cameras comply with national law, if all the required policies and notifications are in place and if the persons concerned have been duly informed.

6.5. Direct marketing

6.5.1. What is direct marketing?

Direct marketing is an advertising strategy that is deployed by many companies. It allows you to directly target the promotion of your products or services, in order to trigger an action (e.g. to visit a website or to buy something) in a selected group of consumers that have been identified as potential buyers. Electronic direct marketing frequently takes the form of emails, texts, picture messages, video messages, voicemails, direct messages via social media or any similar message stored electronically.

By targeting end-users with electronic direct marketing communications, companies are processing personal data as defined in the GDPR. However, the rules governing direct marketing communications are not only to be found in the GDPR, additionally the ePrivacy Directive (to be replaced by the ePrivacy Regulation) imposes specific rules in case of direct marketing communications.

6.5.2. How to justify direct marketing?
In the context of direct marketing, consent is key! Under the ePrivacy legislation, you need to obtain consent from the targeted individual before sending direct marketing communications in electronic form – marketing texts, emails or calls. The ePrivacy legislation prevails over the GDPR and therefore limits the possibility for controllers to rely on another legal basis in the list of article 6 GDPR. For the interpretation of consent the legislator has pointed to the strict interpretation to be found in the GDPR. **LINK TO CONSENT SECTION.** This means that consent needs to be:

**READ MORE**

- **Freely given** – You should provide the individuals concerned with a genuine choice to consent to marketing. Coercing or unduly incentivizing people into consenting – for example by tying negative consequences to the refusal of consent – is thus prohibited.

- **Specific** – Consent needs to be specifically given for your company and the type of marketing communication (e.g. email, text message…) you are using. Consent should not be bundled up as a condition of service unless it is necessary for that service.

- **Informed** – You should inform the individuals concerned in a clear and prominent way to ensure that they fully understand that a certain action will be taken as consent and what exactly they are consenting to. In practice, you should avoid giving information in a hidden (due to placement or size) manner or by way of lengthy, complicated privacy policies that are difficult to understand.

- **Unambiguous indication of wishes expressed by a statement or a clear affirmative action** – Consent should be provided by way of a clear positive indication of agreement, such as clicking an icon, subscribing to a service, sending an email or making a phone call, but also oral confirmation is possible. In other words, consent needs to take the form of an ‘opt-in’, ruling out the use of pre-ticked opt-in boxes, as well as opt-out boxes and any other form of consent derived from silence, inactivity or default settings.

**Example:**

Upon request, a small building company provides potential clients with brochures setting out information about how the company works, the materials it works with etc. The request needs to be made by filling in an online form. Through this online form, the company also asks for the persons’ home address and email address, not only to be able to deliver the brochure but also to send them marketing messages about upcoming projects and events in the future. The company only allows the requesting individuals to opt-out of receiving marketing messages in case they
untick three boxes covering marketing emails, post and text messages. However, unticking all three boxes results in the fact that the brochure will not be sent. This practice is not GDPR compliant.

Not valid: “By registering, you agree to receiving email marketing messages from us. If you do not want to receive such messages, tick here: 0”

6.5.3. Additional obligations when relying on ‘direct marketing’:

Essential here is that, through the accountability principle, the GDPR requires you to be able to demonstrate that you have obtained consent for direct marketing. This means that you must keep evidence of who, when, how, and what you told people in the context of requesting consent. Also, very important in this regard is that the individuals concerned have the right to withdraw their consent at any time. Moreover, you need to make sure they can withdraw consent equally as easy compared to the granting of consent.

6.5.4. When is no consent needed?

Important to know is that under certain conditions you are still allowed to process contact details for direct marketing purposes when you did not obtain consent, however, only in cases where the exemption to the ‘opt-in consent rule’ – referred to as the ‘soft opt-in’ – is applicable. The exemption exists when three conditions are met:

While the ePrivacy legislation provides an exemption to the necessity for direct marketing, it does not relieve you from the obligation to ground your processing on one of the legal bases listed in
article 6 GDPR (LINK). The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. This means that, when invoking the soft opt-in, you still have to perform the legitimate interest balancing exercise (LINK).

! With regard to personal data bases that pre-existed the GDPR, it is not necessary for individuals to give consent again if the manner in which consent has been given complies with the conditions of the GDPR!

6.5.5. **Best practice:**

The clearest way to obtain consent is to make us of an ‘opt-in box’ that individuals concerned can tick in case they wish to receive direct marketing through specific channels (e.g. email, text messages...).

Example: Tick the boxes if you would like to receive information about our products and any special offers by post 0 / by email 0 / by telephone 0 / by text message 0 / by recorded call 0.

🔧 Time for action –

- Ask for consent when you engage in direct marketing
- Check whether your consent requests are clear and prominent
- Be transparent regarding who is sending the marketing messages
- As individuals have the right to withdraw consent at any time, ensure that all direct marketing holds information on this right and provides the possibility to withdraw consent (e.g. unsubscribe button)
- Make sure you keep clear records of what an individual has consented to, as well as when and how consent was obtained. This is necessary to demonstrate GDPR-compliance in the event of a complaint.

6.6. **Health data**

Health data are personal data concerning the physical or mental health of a person, including the provision of health care services, which reveal information about a person’s health status in the past, present or future. This category of data is marked as a special category of personal data under the GDPR, because of its ‘sensitive’ nature: unlawful processing of health data may cause serious consequences to a person’s rights and freedoms. Therefore, health-related data are subject to a stricter data processing regime than non-sensitive data: you will not always be allowed to process data revealing information on the health status of persons.

6.6.1. **What/Where is health data?**
6.6.2. Can I process health data?

In principle, the processing of health data – like any other special category of personal data – is prohibited. But even though the processing of health data is deemed to be riskier than processing regular personal data, processing health data can be necessary in various aspects of our life.

Therefore, the GDPR foresees several exceptions to the prohibition. First, health data can only be processed when there is a lawful basis to do so under article 6. (LINK TO SECTION ON LAWFUL BASIS) Additionally, one of the situations mentioned in article 9 needs to be present (LINK TO SECTION ON SPECIFIC CATEGORIES OF PERSONAL DATA UNDER CONSENT).

READ MORE

The most relevant exceptions from a small company’s point of view are:

1. Explicit consent: see section on specific categories of personal data

Explicit consent will not be a valid ground for the processing of health data in situations where medical treatment is necessary and the patient does not have the possibility to refuse the processing of his or her health data.

Explicit consent could be a valid legal basis to process health data for medical research or in the context of insurance companies.

2. Employment, social security and social protection law

If your company employs staff members you are almost inevitably processing health data about these employees because considering employment, social security and social protection law certain obligations and rights exist that require the processing of health data. For instance, employers can process health data of their employees (or their family members) for the purpose of sick leave management or to reimburse medical aids. On the other hand, processing health data within the framework of a pre-recruitment medical examination or an annual medical visit will not always be
allowed under the GDPR, only if a legal obligation or right in this regard exists in EU or national law or in a collective agreement.

3. Individual health care purposes

Medical treatment is inextricably linked with the processing of health data. Health data can be processed in case it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. However, processing in these situations is only allowed where carried out by healthcare professional subject to an obligation of professional secrecy, or by another person subject to an equivalent obligation.

! If your company processes data concerning health, you will bear an extra burden as these data require a higher standard of protection than non-sensitive personal data. In each situation, appropriate safeguards need to be in place!

📝 Time for action –

- Assess whether there is a way to avoid the processing of health data.
  - Is the processing of health data necessary to achieve its underlying aim?
  - Is the aim pursued by the processing of health data proportionate regarding the restriction of the concerned person’s rights and freedoms?
- Check whether EU or national law set additional requirements or prohibitions for health data processing.
- Provide all the necessary information to the individual whose health data your company is going to process in a way that is understandable to the person.
- Implement sufficient technical and organisational safeguards (e.g. pseudonymisation, separate storage of health data, restriction on the number of persons that have access to health data) to ensure that health data is adequately protected and is not subject to unauthorised disclosure or other unlawful processing activity.
- Don’t forget to consider the principles of personal data processing [link to section on data processing principles].
- In case of doubts concerning the permissibility of the planned processing activities or the necessary safeguards, consult your DPO (if your company has one) or your DPA [link to ‘How to contact my DPA?’].

6.7. Websites: Cookies and similar technologies

6.7.1. In a nutshell

Most websites make use of specific information technologies that collect and process information related to the webpage or to the visitor. These tools can be referred to as cookies or other tracking technologies and serve as a memory tool, able to recognize users’ online behaviour and remember their actions.
Since usage of these information technology tools could be privacy-intrusive for the website visitor, you will have to take into account a number of consent and information obligations before placing your first cookie: provide clear and understandable information to the individuals concerned, obtain their consent (not always necessary) and refrain from using personal data in a manner that is incompatible with the initial purpose of collection.

6.7.2. What are cookies?

Cookies are virtually invisible text files that a website may store on its visitors’ computers or mobile devices at the time they access the website. Cookies allow the website to track, collect, and store any (personal) data that companies request.

Cookies, as such, are a storage medium and are therefore not personal data in themselves. Nevertheless, cookies identifiers are personal data because personal data can be stored in them. When cookies can identify an individual, they are considered personal data. As ‘personal data’, their processing is subject to the GDPR and needs to be grounded on a legal basis and respect the data protection rules and principles.

There can be different reasons for companies to make use of cookies:

- to improve the performance of functions and services,
- to improve user experience or
- to monitor users’ digital behaviour to serve them targeted advertising.

Below, a list the most common types of cookies:

- **First party cookies**: Cookies that are set directly by the website accessed by the user.
- **Third party cookies**: Cookies that are set by a domain other than the one the visitor is using.
- **Session cookies**: Cookies that are temporarily placed in the website visitor’s device and that expire at the end of a browser session. These cookies recognise and link the actions of a website visitor during a browsing session.
- **Persistent cookies**: Cookies that are stored on the website visitor’s device for a specified period that is longer than one session. These cookies can recognise the visitor’s device for future website visits and remember its preferences or activities on that website, or even transfer this information to another websites.
6.7.3 Obligation to obtain consent

Cookies are mainly regulated by the ePrivacy Directive. Based on this directive, consent from the user for the storage of, or access to, certain types of cookies is required. Consent under ePrivacy Directive should be interpreted in line with the GDPR (freely given, specific, informed, unambiguous and based on an affirmative action). Additionally, in case you make use of any type of tracking devices, you must be able to prove that you have obtained your visitors’ consent.

! Scrolling down or swiping through a website or application cannot be considered to be a valid expression of consent to the use of cookies !

Ask for consent the first time you set cookies, you do not have to repeat it every time the same person visits your website. However, devices may be used by different people so you may want to repeat this process at regular intervals.

Exemptions from the consent obligation

Consent is not required for the implementation of all cookies. The ePrivacy Directive provides an exemption for:

- Cookies used for the sole purpose of carrying out the transmission of communication
- Cookies that are strictly necessary to provide a service over the internet that is explicitly requested by the user. The implementation of the cookies needs to be essential to provide the user with the service in question. Cookies that are solely helpful or convenient – or that are also used to achieve other objectives – cannot be considered as strictly necessary cookies and thus can only be stored onto the user’s device based on valid consent.

The following cookies can be exempted from the consent requirement, provided that they are not used for additional purposes:

- User input cookies (session-id), for the duration of a session or persistent cookies limited to a few hours in some cases;
- Authentication cookies used for authentication services, for the duration of a session;
- User centric security cookies used to detect authentication abuses, for a limited persistent duration;
- Multimedia content player session cookies, such as flash player cookies, for the duration of a session;
- Load balancing session cookies, for the duration of a session;
- User-Interface customization persistent cookies, for the duration of a session (or slightly more);
- Third party social plug-in content sharing cookies, for logged in members of a social network if they are not also used for user tracking purposes.

6.7.4 Information obligation

When you want to make use of cookies or other tracking technologies, you need to provide the user with clear and comprehensive information about this use. The information needs to be provided in a manner that is suitable for the user and before or at the time of requesting consent. This means that you will have to implement a cookie policy on your website, providing all the
information that is necessary for users to take an informed decision on whether or not to consent to the use of cookies.

A cookie policy should:

- Make sure that the language used in the cookie policy, corresponds to the language of the people targeted by the website!

Good practice - Use a layered approach in order to keep the cookie policy short and simple: basic information about cookie usage should be contained in the first layer. This first layer should give the user the option to accept or refuse all cookies, or to configure options for the usage of different cookies (opt-out). When choosing the last option, the user should be directed to a more detailed cookie notice (second layer) with information (name, type of cookie, technical details, specific purpose and retention period) for each (group of) cookies.

6.7.5 Storage period

A limited storage period should be set for each (type of) cookie. It is also recommended to periodically review the cookies you use because the storage period of cookies or other tracking technologies must be proportionate and limited to what is necessary to achieve the planned purpose. The storage period can also not exceed the period for which valid consent was given.

📝 Time for action –

- Check what cookies or other tracking technologies your online service already uses or intends to use and identify what information is processed by each cookie
- Confirm the purposes of each cookie and remove cookies you do not need
- Identify strictly necessary cookies, communication cookies and cookies for which consent is required
- Put in place a cookie policy to provide the necessary information concerning your company’s use of cookies and other technologies
- Implement a GDPR-compliant consent mechanism, including the ability to refuse non-essential cookies
- Keep records of users’ consent to implementing cookies for an appropriate period of time
- Ensure compliance with the GDPR where information obtained and processed through cookie storage can be considered as personal data
- Avoid the use of third-party cookies or other tracking technologies as much as possible

6.8. Social media to promote my business

In today’s digital age, most companies rely on social media to promote their business. They usually have their own ‘page’ or account on one or more social networking websites. Additionally, some companies feature social media plug-ins on their own website, to generate more traffic their way. Making use of social media brings along certain legal consequences. What exactly this means for your role and responsibilities under data protection law, will be discussed in this section.

6.8.1. Fan page hosted on social media

Most likely you are the administrator of a (fan) page for your company on a social networking website. This inevitably brings along processing of personal data. In this context, processing is essentially carried out by the social networking site, placing cookies and processing the information stored in the cookies. By creating such a page, you give the social networking site the opportunity to place cookies on the computers of visitors, from which you benefit by obtaining statistics useful to manage and promote your activities. Regardless of the fact that you often do not have factual or legal influence on the purposes and means of processing, you will be considered to be involved in the production of the statistics through defining the criteria for the statistics and designating the persons whose personal data is to be made use of by the social networking site. The fact that you only receive the statistics in anonymized form and do not have access to the actual personal data concerned, does not take away the fact that you will be considered to have an influence on the processing of personal data for the purpose of producing statistics based on visits to the fan page.

Consequently, as an administrator of a fan page hosted on a social networking site you contribute to the processing of the personal data of your visitors and under the GDPR you will be seen as a
joint controller – together with the social networking site. This is only the case for those processing activities which consist in the collection by the social networking site of personal data on your page. This results in the shared responsibility to inform visitors of the page about the fact that information of them was collected via cookies.

The existence of joint responsibility does not necessarily imply equal responsibility of you and the social network operator. The level of responsibility must be assessed taking into account all relevant circumstances of the particular case: if your joint processing only relates to the collection of data from visitors of your page and to the processing of this data for statistical purposes (and not to the use of the data by the social networking site for its own analysis and advertising unrelated to your company) you will likely only carry responsibility for these processing activities.

The GDPR specifies that joint controllers need to determine their respective responsibilities under data protection law in a transparent manner. For more information on what this means, see LINK TO DPA SECTION. Following from joint controllership, individuals will be free to choose to turn to your company or the social networking site to obtain full damages. If you are not able to prove that you are not responsible for the event giving rise to the damage, the social networking site is allowed to claim back part of the compensation corresponding to your responsibility for the damage.

Time for action –

• As a fan page administrator, you will need to conclude a joint controller agreement with the hosting social networking site. In this agreement, each party’s responsibilities need to be set out, including visitors’ rights and information obligations. E.g. Facebook has put in place a joint controller addendum with which you will have to agree in case you would like to create a Facebook page for your company.

• Comply with the controller obligations in the GDPR: inform visitors about the identity of the joint controllers, the purpose of the processing, the legal basis relied upon, data retention periods and all data processing activities and their rights (e.g. access, rectification, erasure). Also make sure that visitors can exercise these rights.

• To the extent possible, put in place measures to ensure adequate protection of your page’s visitors and their personal data.

• Data processed for the purpose of providing targeted advertising will require visitors’ consent.

6.8.2. Social plugins
Often companies embed social plugins on their website to obtain certain commercial benefits. Social plugins are buttons – such as a ‘like button’ or a ‘share button’ – which allow visitors to share their experiences on other websites with friends on certain social networking sites. When a visitor consults a website featuring plugins, his or her personal data are transmitted to the social networking site. It allows companies to optimise the publicity for its goods or services by increasing visibility on social media.

**READ MORE**

If you feature a third-party plugin on you website, you most likely will be a joint data controller together with the social media company concerned in respect of the collection of personal data of the website visitors and the transmission of this data to the social networking site. This is because both parties have an economic interest and you jointly determine the means and purposes of the processing of the personal data that were transferred to the social networking site. You will, however, not be a controller regarding the processing after the transmission of the data carried out by the social networking site alone, as you do not determine the purposes and means of those operations.

In respect of such operations involving the processing of personal data of visitors to your website, you will also carry a list of responsibilities under the GDPR.

**Time for action –**

- At the time of the collection of their personal data, you must provide certain information to your visitors, including for example your identity and the purposes of the processing.
• In case you rely on consent of the individuals concerned, you only are required to obtain prior consent for operations for which you act as a (joint) controller (i.e. the collection and transmission of the data).
• In cases where the processing of personal data is justified by relying on necessity for the purposes of a legitimate interest, the Court finds that each of the (joint) controllers, namely you as the operator of a website and the provider of a social plugin, must pursue a legitimate interest through the collection and transmission of personal data in order for those operations to be justified in that regard. It is not enough if only one of the joint controllers is pursuing a legitimate interest through the collection and transmission of personal data.

6.9. A waterproof privacy policy

6.9.1. In a nutshell

Your privacy policy is the instrument through which you inform your (contacts at) existing and potential customers, clients, suppliers, website visitors, prospects, employees and job candidates how you will use and protect their personal data.

Consequently, the privacy policy must be available to these persons for them to be able to acknowledge the policy.

Ideally, you work with (at least) two different privacy policies:

• an internal privacy policy, for your employees, internal consultants and anyone who provides services within your company,
• a public privacy policy, for anyone who has no access to your internal documents, such as suppliers, prospects, customers, job candidates, etc.

It is of course possible to have more different policies, if your activities would require so.

Every privacy must contain many mandatory mentions, adapted to the persons whose data you are processing and to the ways you process their data.

You can find a template privacy policy via this link.

6.9.2. The privacy policy must obligatorily contain the following information:

- the (categories of) personal data that you process
- the use you make of that data
- how you protect and safeguard that data
- how you collect that data
- which legal basis you rely to process data
- which third parties receive such data
- the places (countries) where those data are processed
- the rights which can be exercised by the persons concerned (e.g. right of access, right of forgetting, right of rectification, etc.)
- who your company is and how it can be reached, including by e-mail
- how long data is kept (retention policy)
- the right of data subjects to file complaints with the data protection authority
A Privacy Policy is sometimes also called a privacy statement or a privacy notice, but we recommend to use “privacy policy” because the other definitions can also refer to the short informational pieces of text that inform the persons concerned of the existence of a privacy policy and some specific aspects of the intended processing.

6.9.3 Details and readability

Your privacy policy should be sufficiently specific and detailed to allow the persons concerned to actually understand what happens with their data and what they can expect.

On the other hand, the GDPR also prescribes that the information you provide should be “concise” and “legible”.

Therefore, it is recommended to have a so called “layered” privacy policy:

- The first “layer” is a very short overview of the principles you apply which allows the persons concerned to establish “in the blink of an eye” what major principles you apply when processing their personal data.
- The second “layer” contains all information. This can be a different document, or this additional information can (for example) appear by clicking on a “read more” button under the short description of the first layer.

To enhance readability, it is also strongly recommended to design your policy in a way that

1. it can be easily read. Avoid for example to use a small font and arrange the text in a logical way, that enhances a comfortable readability.
2. to add icons, symbols and/or images to the policy to visually support and show the content of the privacy policy.

6.9.4 Location of and references to your privacy policy

It is not enough to “have” the required privacy policies, it is also required to make sure that the persons concerned are informed of the existence of it before you start processing.

1. The internal privacy policy that applies to your employees will have to be communicated to them in accordance with your local employment law. It may be required that reference is made to such “employee privacy policy” in your work rules and/or employment contracts. You will also need to communicate it to any other inhouse service providers to whom the privacy policy applies.
2. The external/public privacy policy is ideally put on your website, with fixed link referring to it in (at least) both the footer of your website and in your cookie banner.

Furthermore, you will need to refer to your public privacy policy each time you obtain personal data of someone and each time you use such personal data to communicate. This means that you should have a link or url in (for example) all your outgoing emails, below forms (webforms and paper forms), job announcements, etc.
Finally, it is not sufficient to just refer to the privacy policy. When you obtain personal information of a person, you must also briefly describe what you will do with it.

6.9.4.1 A form to subscribe to a newsletter can, for example, look like this:

“If you wish to (stay updated on similar offers/our product range/receive our newsletter/…), please fill in your personal details below:

- E-mail address (obligatory):
- Gender: man/woman/other/I wish to not give this info
- Name (obligatory):
- Surname (obligatory):
- Company
- Sector
- ...

( ) I wish to receive the (name company) newsletter / e-mails customized to my profile / information and I therefore give permission to process my data and e-mails automatically.

( ) I give my permission to transfer my data to third (commercial) partners, which were carefully selected by (company), in order to receive additional information, based on my interests.

Send/confirm/subscribe [button]

You can unsubscribe from these e-mails or modify your preferences at any time.

We respect your privacy and do not disclose your data to third parties. For more information, please find our Privacy Policy in this link (insert link).

6.9.4.2 And the footer of your emails can, for example, look like this:

“Your privacy is important to us; we process your data in accordance with the relevant privacy rules. This e-mail was sent to (e-mail address) because you are a registered user of our website (...). If you wish to no longer receive our e-mails, you can unsubscribe at any moment by clicking on this link (insert link). Please find more information on how we process your data in our Privacy Policy (insert link).

© [year] – [name and legal form of your company] – [address of your company], [VAT number and/or company registration number]

Time for action –

Use our template privacy policy to draft your internal and public privacy policies.

Once you have drafted your privacy policies, you can verify their completeness via our tool SMOOTEXT.

6.10. Consent and children’s data
The GDPR explicitly recognises that children deserve specific protection of their personal data and introduces additional rights and safeguards for children. SMOOK will share some best practices for companies that process – or might process – children’s personal data.

READ MORE

If you provide information society services (e.g. web shops, video-sharing platforms, social networking sites, search engines etc.) to a child while relying on consent as the legal basis for the processing, you need to undertake reasonable efforts to obtain and verify parental consent when it concerns users below the age of 16. Reasonable effort should be determined by considering existing technology and the circumstances such as resources and level of risk. Depending on the Member State where you operate, a different age limit may apply as Member States can lower the age limit for parental consent down to 13 years old.

Take note that this rule only applies if the services are offered directly to the child, meaning that they either exclusively address children or explicitly focus on them.

Also, it does not mean that you always must obtain parental consent for users under the chosen age limit. Only if you make your service available to children, and you rely on consent as your lawful basis (e.g. for any non-core processing, cookies or similar technologies or processing of special category data).

6.11. Useful link

ICO has issued a code on Age appropriate design: a code of practice for online services, which provides practical guidance on how to ensure your online services appropriately safeguard children’s personal data. Following this code will assist you to process children’s data fairly.


📝 Time for action –

In case you offer information society services directly to children, go check out your national post-GDPR law to find out up until which age parental consent should be obtained.

National age limits for parental consent:
When you do not directly offer content to children, but rather offer services that are likely to be accessed by children (<18 y/o), you will have to take additional measures to protect their best interest.

7. MENU 1 – HANDBOOK – RELATIONSHIP TO E-PRIVACY

7.1. In a nutshell

When processing personal data, two major EU legislative instruments are of potential relevance to your operations: the GDPR and the e-Privacy Directive. As it is important to know which instrument to turn to under which circumstances, you need to be able to distinguish them and their scopes of application.

The goal of the GDPR is to protect fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and to ensure the free movement of personal data within the Union. The goal of the e-Privacy Directive is also to protect fundamental rights and freedoms of the public, but in particular the right to privacy and confidentiality specifically with respect to processing personal data in light of the use of electronic communication networks. Finally, the e-Privacy Directive also aims to ensure the free movement of such data and of electronic communication equipment and services in the Union.

! In other words, the e-Privacy Directive particularises and complements the GDPR regarding the processing of personal data in the electronic communication sector!
In the event of processing personal data, there are three possible scenarios regarding the (lack of) interplay between both instruments:

**THE GDPR DOES NOT APPLY, BUT THE E-PRIVACY DIRECTIVE POTENTIALLY DOES**

- When the data that is being processed is not personal data (e.g. company emails that do not hold the name of natural persons or phone numbers of automated customer services of legal persons etc.)
- When it concerns processing, activities mentioned in the list of article 2(2) and (3) of the GDPR
- When the processing activities do not fall under the territorial scope of the GDPR

**THE E-PRIVACY DIRECTIVE DOES NOT APPLY, BUT THE GDPR POTENTIALLY DOES**

- In general, the e-Privacy directive does not apply, unless:
  - it concerns an electronic communications service
  - which is offered over an electronic communications network
  - the service and network are publicly available (so not corporate networks that are only accessible to employees for professional purposes)
  - and are offered in the EU
- Website operators or other businesses do not fall under the scope of the Directive (except when it concerns articles 5(3) (cookie rules) and 13 (direct marketing rules))
THE GDPR AND THE E-PRIVACY DIRECTIVE BOTH APPLY

• It is possible for processing activities to fall within the material scope of both legal instruments:
  o In case of the use of cookies which collect personal data
  o In case of direct marketing practices
  o In case providers of electronic communications services process personal data of natural persons using their services and additionally specific rules – e.g. on subscriber directories, itemised billing, calling line identification – apply
  o In case traffic or location data are generated by electronic communications services in case personal data is involved

For situations in which both legal instruments apply, the GDPR acknowledges that the e-Privacy Directive should prevail and that it does not impose additional obligations on natural or legal persons in relation to processing in light of the provision of publicly available electronic communications services in public communication networks in the EU. This is only for situations in which specific obligations exist within the e-Privacy Directive. In other cases, where it does not specify anything, the more general rules of the GDPR will govern the situation.

7.2. What about enforcement?

National data protection authorities are competent to enforce the GDPR (LINK). The sole fact that part of a processing operation falls within the scope of the e-Privacy directive, does not affect the competence of data protection authorities under the GDPR. However, data protection authorities are not automatically competent considering e-Privacy.

The latter depends on whether the national law of your country designates the data protection authority as competent authority under the e-Privacy Directive. It is only then that the data protection authority has the competence to directly enforce national e-Privacy rules in addition to the GDPR.

✏️ Time for action –
In case you are processing data within the context of providing publicly available electronic communications services in EU public communication networks, do not forget to check first whether you, and how to, comply with the e-Privacy Directive.
1. MENU 2 – THE DEVELOPERS BEHIND SMOOK

SMOOK has been developed under the SMOOTH-project.

The consortium of the SMOOTH-project is made up of technology partners, data protection authorities, innovation and research institutions, associations representing European SME’s and a standardization body organisation.

In total, it consists of 12 organisations, coming from 5 different EU countries (Spain, Belgium, Poland, Latvia and France) and the United Kingdom, which have joint effort and expertise to create tools to help small companies to adopt the GDPR.

The aim of the SMOOTH project is twofold:

1. **To create awareness** regarding the importance of being compliant with the GDPR, as many micro-enterprises may disregard their obligations in this respect.
2. **To assist micro-enterprises** in effectively adopting the GDPR.

A SMOOTH cloud platform will be set up and will use machine learning, text and data mining, and advance online auditing methods to automatically generate a bespoke GDPR compliance report for the most critical aspects for micro-enterprises.

Likewise, SMOOTH will provide useful materials for solving those identified GDPR aspects that are not properly covered. All this will positively contribute to reinforcing citizens’ rights, while avoiding potential fines for the micro-enterprises.
### 2. MENU 2 – GDPR GLOSSARY

<p>| <strong>Cookies</strong> | Small text files created by a website that are stored in the user's computer either temporarily for that session only or permanently on the hard disk. Cookies provide a way for the website to recognize you and keep track of your preferences. |
| <strong>Cookie banner</strong> | A cookie notice in the form of a banner that appears on websites upon the user’s first visit to the site and that asks for consent to use cookies. |
| <strong>Cookie notice</strong> | A notification message or document to inform users about the presence of cookies and/or to obtain users’ consent to place these cookies on their devices. |
| <strong>Customers or clients</strong> | Those people with whom you have a business relationship. |
| <strong>Data breach</strong> | A security incident in which personal data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. |
| <strong>Data controller</strong> | A person, company, or other body that determines the purpose and means of personal data processing (alone or jointly with another person, company or body). |
| <strong>Data processor</strong> | A person or an organization processing personal data on behalf of, and solely as instructed by, a controller. E.g. suppliers, social secretariats, accountants, ICT-providers, marketing support, etc. |
| <strong>Data protection authorities (DPA)</strong> | Independent public authorities that supervise the application of the data protection law, based on investigative and corrective powers. |
| <strong>Data protection impact assessment (DPIA)</strong> | A tool to assist in identifying, assessing and minimizing the data protection risks relating to a processing activity. This is obligatory for high risk processing. |
| <strong>Data protection officer (DPO)</strong> | A position within an enterprise where the primary task is to ensure that personal data of staff, customers, providers or any other individuals is processed in compliance with the GDPR. |
| <strong>Data retention policy</strong> | A policy in which you define how long you will keep each type of data and the length of retention is being justified. |
| <strong>Information society service</strong> | Any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of a service (e.g. commercial websites, social media). |
| <strong>Legal/Lawful basis</strong> | Article 6 of the GDPR exhaustively lists the grounds based on which the processing of personal data could be justified (consent, necessary for a contract or the performance thereof, legal obligation, to protect someone’s vital interests, task in the public interest, legitimate interest). |
| <strong>Legitimate interest assessment</strong> | An assessment of the necessity of your processing, its impact on individuals' rights and interests and whether the rights and freedoms of individuals override your company's legitimate interests. |</p>
<table>
<thead>
<tr>
<th>Micro-enterprise</th>
<th>Companies with less than 10 employees and an annual turnover of no more than €2 million.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data</td>
<td>Any information relating to an identified or identifiable natural person. (An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person)</td>
</tr>
<tr>
<td>Processing</td>
<td>Any operation or set of operations performed on (sets of) personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.</td>
</tr>
<tr>
<td>Recordkeeping</td>
<td>The obligation to keep records of data processing activities to ensure that enterprises dealing with personal data can be held accountable for keeping personal data safe.</td>
</tr>
<tr>
<td>Special categories of data</td>
<td>Personal data that needs more protection because it is sensitive (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data and data concerning health, sex life and sexual orientation).</td>
</tr>
</tbody>
</table>
### 3. MENÚ 2 – TEST YOUR GDPR AND EPRIVACY KNOWLEDGE

<table>
<thead>
<tr>
<th></th>
<th>What is the main aim of the GDPR?</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Giving citizens back control over their personal data by and to “harmonize” the different national data protection laws across the EU to facilitate the free movement of personal data</td>
</tr>
<tr>
<td>b.</td>
<td>To make sure the police cannot process your data without your consent</td>
</tr>
<tr>
<td>c.</td>
<td>To restrict online advertising</td>
</tr>
</tbody>
</table>

**Answer A**

In an increasingly digitized society, the GDPR aims to give citizens back the control over their personal data by providing them with greater protection and rights, as well as to harmonize the 28 different data protection laws across Europe, in order to facilitate the free traffic of personal data in the EU.

**LINK** - Click here for more information on the reasons behind the GDPR.

<table>
<thead>
<tr>
<th></th>
<th>Which companies have to comply with the GDPR?</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Only companies who have an establishment in the EU</td>
</tr>
<tr>
<td>b.</td>
<td>Companies who are established in the EU and companies who target EU citizens</td>
</tr>
<tr>
<td>c.</td>
<td>All companies worldwide</td>
</tr>
</tbody>
</table>

**Answer B**

Both, companies who are established in the EU and companies who target EU citizens, have to respect the rules in the GDPR.

**LINK** - Click here for more information on when the GDPR applies.

<table>
<thead>
<tr>
<th></th>
<th>An American business traveler in Spain orders a product from an online store which is also based in Spain. This traveler is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>not protected under the GDPR</td>
</tr>
<tr>
<td>b.</td>
<td>protected under the GDPR</td>
</tr>
</tbody>
</table>

**Answer B**

The processing of the traveler’s personal data is undertaken by an enterprise established in the EU, hence the processing is regulated by the GDPR, regardless if he might have the product delivered in the US.

**LINK** - Click here for more information on when the GDPR applies.

<table>
<thead>
<tr>
<th></th>
<th>Is data collected before May 2018 subject to the GDPR?</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Yes</td>
</tr>
<tr>
<td>b.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Answer A**
Yes, any personal data that you currently are processing is subject to the GDPR, regardless of when they were initially collected.

5 Which of the following data are not personal data? (more than one answer is possible)
   a. Statistics of the number of visits to a website, tracked via cookies
   b. License plates
   c. IP addresses
   d. The purchase history of a specific customer

Answer A

Cookies tracking the number of visits to a website (statistics) are not personal data. License plates and IP addresses are personal data because personal data is all data that makes it possible to designate a person uniquely, even if you are not the person who can. Data that relates to an identifiable person is also personal data, hence a purchase history is personal data as long as it is possible to find out who it relates to.

[LINK - Click here for more information on what is personal data and what is not.]

6 When does an EU company need to comply with the GDPR?
   a. When they are processing personal data
   b. Only when they are storing personal data
   c. Both

Answer C

The main criterion triggering GDPR applicability is whether or not a company processes personal data. The term processing is very broad and covers any operation involving personal data: storage, collection, recording, structuring, consulting, usage, transmission...

[LINK - Click here for more information on what constitutes processing of personal data under the GDPR.]

7 When processing personal data...
   a. The GDPR requires enterprises to always obtain consent of the person who’s personal data are being processed
   b. Consent is only one out of an exhaustive list of lawful bases on which enterprises can rely to justify their processing activities and, hence, is not always necessary
   c. Consent is never necessary under the GDPR

Answer B

Consent is only one out of an exhaustive list of lawful bases on which enterprises can rely to justify their processing activities (see articles 6 and 9 GDPR) and, hence, is not always necessary. For each processing...
activity you should always choose a legal basis for processing, depending on which basis is most suitable for the situation.

[Link] - Click here for more information on how to choose a legal basis.

8. By embedding a Facebook “like button” – a social plug-in – on your website, you become a controller of the data that is being processed?
   a. No
   b. Yes, you become the only controller
   c. Yes, you become a joint controller together with Facebook

Answer C

You become a joint controller to the extent you jointly determined the purposes and means for which data was collected by the “like button”.

[Link] - Click here for more information on the data protection consequences of using social media to promote your business.

9. Under the GDPR, consumers have the right to be informed by companies who are processing their personal data. What does this mean?
   a. Companies need to provide a web page with a list of all the personal data they hold about each customer to which customers can navigate to find information
   b. Companies need to provide access to their systems by providing data subject with a user ID and password
   c. Companies need to provide their data subjects with the information on what data they are collecting, what they are going to do with it, how long they are going to keep it and who will have access to it.

Answer C

Companies need to provide their data subjects with the information on what data they are collecting, what they are going to do with it, how long they are going to keep it and who will have access to it.

[Link] - Click here for more information on individuals’ rights you need to take into account.

10. What information should you give individuals before processing their data for marketing purposes?
    a. Why their data are being processed
    b. The name and contact details of your enterprise
    c. How long the data will be stored
    d. All of the above
Answer D

Article 13 of the GDPR provides a long list of information that should be provided to the individuals concerned before you as an enterprise can start processing their personal data.

LINK - Click here for more information on the data protection consequences for direct marketing.

11 In the event of an access request by an individual concerned, what kind of information should you give access to (if requested)?

   a. The reason behind the processing
   b. who else has access to the data
   c. Where the data is stored
   d. All of the above

Answer D

You should be able to provide the individual concerned with all this information, and this needs to happen without undue delay or in any case within one month of receipt of the request.

LINK - Click here for more information on the rights you should grant to individuals whose data you want to process.

12 Can companies informally engage a processor?

   a. Yes, because in any case the controller will be the responsible actor under the GDPR
   b. No, there always needs to be a contractual agreement between the controller and the processor

Answer B

There always needs to be a data processing agreement when engaging a processor.

LINK - Click here for more information on how to draft a data processing agreement.

Results & messages:

<7/12 Oops! It seems that you are still struggling with the GDPR...but no need to worry! You can always have a look at the content in this handbook, which is tailor-made to guide micro-enterprises towards GDPR compliance.

7-9/12 Not bad! However, it seems that you are still struggling with a number of GDPR aspects. If you want to learn more about these issues, go check out SMOOK!

10-11/12 Good job! You already seem to be fairly GDPR-literate. For those GDPR aspects that remain unclear, go check out SMOOK! The content of this handbook allows you to quickly navigate to topics of your interest.

12/12 Congratulations! You seem to have mastered the GDPR. If you still have questions, go check out SMOOK, where you can also find examples and templates.
Annex II - Final text version of SMOOK website application, with some graphics included
Annex II.1 A few screenshots to demonstrate the look and feel of the website

**Legal obligation**

When you need to process personal data to comply with a legal obligation, you can rely on the "legal obligation" as legal basis for your processing activities.

The GDPR has also foreseen the possibility to justify your personal data processing activities in case you find yourself in a situation where processing is necessary for compliance with a legal obligation of the controller.

To be able to rely on this lawful basis, the obligation to process personal data must be **imposed by EU law or the applicable national law of an EU Member State** (including secondary legislation or a binding decision of a public authority) and must be **mandatory**.

**Example:**

A real estate agency processes personal data of its clients (name, date and place of birth, address) to conduct a client analysis in light of money laundering. Under the GDPR, real estate agencies can justify this personal data processing based on the legal obligation to which they are subject in the money laundering law.

**Legitimate interest**

Sometimes personal data processing is necessary to pursue legitimate interests of the enterprise (or a third party). Those legitimate interests can serve as a lawful basis for processing, provided that the interests and (fundamental) rights of the
The GDPR (article 5) sets out seven key principles underpinning the processing of personal data by any entity, including micro-enterprises or SMEs. Therefore, these principles are relevant guidelines for you to keep personal data of your customers, employees and suppliers safe.

7 Principles of personal data processing

1. Lawfulness, Fairness and Transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability
PROCESSING SITUATIONS

Customers’ personal data

Your customers provide their personal data to you for one or more purposes. This means that you cannot use this personal data for anything else (limited use).

To a certain extent, you are however allowed to use your customer’s personal data to market products like the one they purchased from you. To be in compliance, you must however specifically make sure that they are offered the option (1) to unsubscribe from receiving further marketing at any moment and (2) the unsubscribe is used for such marketing (opt-out).

All the general requirements of course also apply, such as informing your customer on how you will process their personal data through your privacy policy.
What about enforcement?

National data protection authorities are competent to enforce the GDPR. The sole fact that part of a processing operation falls within the scope of the e-Privacy directive, does not affect the competence of data protection authorities under the GDPR. However, data protection authorities are not automatically competent considering e-Privacy.

The latter depends on whether the national law of your country designates the data protection authority as competent authority under the e-Privacy Directive. It is only then that the data protection authority has the competence to directly enforce national e-Privacy rules in addition to the GDPR.

Time for action!

In case you are processing data within the context of providing publicly available electronic communications services in EU public communication networks, do not forget to check first whether you, and how to, comply with the e-Privacy Directive.
Test your GDPR and ePrivacy knowledge

What is the main aim of the GDPR?

- Give citizens control over their personal data and facilitate data exchange
- To make sure the police cannot process your data without your consent
- To restrict online advertising

About the Handbook
Privacy and cookies

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 786741. The accreditation reflects SMOOTH’s consortium view and neither the European Commission or any associated party is responsible for any use that may be made of the information it contains.

05/02/2022  Revision: 03  Project Nº: 786741  Page 183 of 345
For the GDPR to be applicable, personal data needs to be:
- Entirely or partly, processed by automated means;
- Part of a filing system, or intended to be part of a filing system, when processing does not happen by automated means.

What constitutes “personal data”

When is a person “identifiable”?
Should my company appoint a DPO?

Are you a public authority or body?

Yes

No

There are four situations in which a DPO must be appointed:

1. Public authority/ body
   Where the processing is carried out by a public authority or body.
2. Regular and systematic monitoring
   Where the processing activities are carried out for the purpose of monitoring the activities of a public authority or body.
SMOOTH Community feeds

SMOOTH project [twitter feed]

Join the SMOOTH Community at FUNDINGBOX to get support on GDPR

---

SMOOTH Final event: Easy and Affordable GDPR Compliance Solutions for European Micro-Enterprises...
January 19, 2021

SMOOTH Final event: Easy and Affordable GDPR Compliance Solutions for European Micro-Enterprises...
January 19, 2021

Watch the video of the webinar: SMOOTH GDPR Platform and pilot opportunities for micro-enterprises... 
November 30, 2020

Discover how to make use of cookies and implement successful cookie policy and banners. Watch the vid...
November 24, 2020

Join the SMOOTH Market Pilot to become GDPR-compliant for free! Register before 31 December 2020...
November 17, 2020

Webinar: How to make use of cookies and...
Annex II.2 The website (full text)

The GDPR Regulation in a nutshell

A brief History


However, since 1995, the internet has grown immensely and the way data is being used, collected and stored has fundamentally changed.

Data is everywhere

Therefore, a revision of the Data Protection Directive was long overdue. This time, the EU opted for a regulation instead of a directive. This means that the GDPR – as one unified data protection regulation – directly applies in all EU member states, harmonising national data protection laws across the EU.

Although GDPR-compliance is still widely perceived as an administrative burden by many companies, there is also a reverse side to the coin: it creates new business opportunities and value in the future digital economy.

- **Take back control** – as its primary objective, the GDPR strives to give back the control of personal data to all citizens in the EU. Therefore, improving their overall sense of trust and security.
- **GDPR in the Digital Age** - by simplifying the monitoring environment for international businesses, through the standardisation of the regulation within the EU, the GDPR facilitates the international data flows.
- **A fair competition** - by creating the same set of rules between companies established in the EU, and those based outside the EU, the GDPR puts an end to distortion of competition.

The most important novelties introduced by the GDPR:

- Extended territorial scope;
- New basic principles;
- New obligations – for processors too;
- New rights for data subjects;
- Rules on children’s consent;
- High fines – up to 20 million or 4% of the total worldwide turnover.
The GDPR in a nutshell

Scope

What?

For the GDPR to be applicable, personal data needs to be:

- Entirely or partly, processed by automated means;
- Part of a filing system, or intended to be part of a filing system, when processing does not happen by automated means.

1/ Personal data

What constitutes “personal data”? [video animation]

When is a person “identifiable”?
[Read more]

The context in which the data is being collected is also very important.

One single piece of data (E.G. hair colour, occupation, car…) might not be enough to identify a natural person as such. Now should the data be combined with other data; this might change the situation. Enterprises that collect multiple types of data on people should take this into account.

Anonymizing and pseudonymizing data are encouraged by the GDPR. The difference between these techniques is that pseudonymous data merely reduces likability but still allows for some form of re-identification (E.G. encryption or when the identifiers are replaced by individual codes), while anonymous data cannot be re-identified (linked to persons) at all.

💡 Any data or information - which have had their identifiers removed (anonymization) or replaced (pseudonymization) - will still be considered being a “personal data” for the purposes of the GDPR.

N.B. Information which is truly and fully anonymous even before being processed is not covered by the GDPR.

What is not “personal data”? [Read more]

Information about a deceased person, cookies tracking the number of visits to a website without identifying the visitors (statistics), data about companies or public authorities or any other data from which it is not
possible to directly or indirectly link it to a person are not to be considered as personal data.

However, a nuance should be added regarding information about individuals acting as sole traders, employees, partners and enterprise directors when the information relates to them as individuals and where they are individually identifiable. In that case, it does concern “personal data”. This means that a work email address containing the business partner’s name (E.G. adam.johnson@enterprise.com) is personal data, while a generic email address (E.G. contact@enterprise.com) is not.

Special categories of data

The GDPR make a distinction between ‘regular’ personal data and special categories of data. The latter require extra protection because of their sensitive nature. Therefore, processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation are, in principle, prohibited.

However, a limited number of exceptions to this rule is provided by the legislator.

2/ Processing

“Processing” is defined very broadly under the GDPR:

- Any operation or set of operations;
- Which is performed on personal data or on sets of personal data;
- Whether or not by automated means.

Recording – Collecting – Organising – Structuring – Adapting or altering – Storing – Retrieving – Consulting – Disclosing by transmission – Using – Disseminating or otherwise making available – Aligning or combining – Erasing or destructing – Restricting

When you pseudonymize or anonymize personal data, you are also processing in the sense of the GDPR.

What does not constitute “processing” under the GDPR?
The GDPR does not apply to certain activities such as processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities (e.g. when collecting names and telephone numbers of attendees of a party at your house).

In the absence of processing activities or personal data, the GDPR will not apply.

Where?

For the GDPR to apply your enterprise, it should fall under the territorial scope of the Regulation. Article 3 defines this territorial scope based on two main criteria:

- The "establishment criterion" - Your enterprise is established in the Union.

  The GDPR applies if your enterprise – operating either as controller or as processor – is established in the Union, regardless of whether the processing takes place in the Union or not. An enterprise is established in the Union if it has a stable presence there, which exercises real and effective activities considering the nature of the economic activity carried out by the enterprise.

- The "targeting criterion" - Your enterprise is established outside the Union, but is processing data of individuals in the Union.

  The GDPR also applies when your enterprise – operating either as controller or as processor – is not established in the Union but does process personal data of individuals who are in the Union, where the processing activities are related to:
  
  - The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  - The monitoring of their behaviour, as far as their behaviour takes place within the Union.

Thus, under certain conditions the GDPR has extraterritorial applicability.

Need an example?

A start-up established in the USA, without any business presence or establishment in the EU, provides a city-mapping application for tourists. The city-mapping application processes personal data concerning the location of customers in the city...
they are visiting, in order to offer targeted advertisement for places to visit, such as restaurant, bars, shops and hotels.

The application is available for tourists while they visit New York, San Francisco, Toronto, London, Paris or even Rome. The US start-up, via its city mapping application, is offering services to individuals in the Union (London, Paris or Rome). The processing of the EU-located data subjects’ personal data in connection with the offering of the service falls within the scope of the GDPR. (Source: EDPB Guidelines 3/2018 on the territorial scope of the GDPR)

What if your enterprise is established in the EU but you work with a processor to which the GDPR does not apply?

[Read more]

If you as a controller, subject to the GDPR, choose to use a processor located outside of the Union and not subject to the GDPR, it will be necessary for you to ensure that the processor processes the data in accordance with the GDPR, just as if the processor is subject to the GDPR, but with some extra requirements. Compliance with the GDPR requires that processing by a processor shall be governed by a contract or other legal act. You will thus need to ensure that a contract – a data processing agreement – is put in place with the processor addressing all the requirements set out in Article 28(3) GDPR.

[Link - Data processing agreements]

What if the processor falls under the GDPR, but your enterprise does not?

[Read more]

Your enterprise – as a non-EU controller – will not become subject to the controller obligations under the GDPR. A “non-EU controller” will not become subject to the GDPR simply because it chooses to use a processor in the Union. The processor however will need to comply with the GDPR if he meets the criteria for GDPR applicability.

Who?

The GDPR protects natural persons regarding processing of personal data and rules relating to the free movement of personal data protection of natural persons. For SMEs it often concerns personal data of clients, suppliers and employees.

The GDPR applies to controllers and processors – which can be natural persons, legal persons, government bodies, etc. irrespective of their size, sector, number of employees or turnover.

[Link – SMEs & the GDPR]

[Link - Is my company a data controller or a data processor]
Is my enterprise allowed to process personal data?

In a nutshell

For any processing activity of personal data, it is required to identify one or more valid ground(s) under the GDPR – known as a ‘lawful basis’ – to justify the collection, use and other forms of processing of personal data.

In today’s business world, companies may conduct several processing operations for different purposes. This entails that SMEs may rely on different legal bases for their different processing activities. It is however not possible to rely on more than one lawful basis for the same processing activity.

Article 6 of the GDPR provides an exhaustive list of the possible lawful bases:

- Contract
- Legal obligation
- Legitimate interest
- Consent
- (Vital interest)
- (Task carried out in the public interest or in the exercise of official authority)

Since the first 4 grounds for lawful processing are the most common in the context of SME’s businesses, we will only further elaborate on these grounds.

- **Contract**

  When you need to process personal data to comply with your contractual obligations, you can rely on the lawful basis “contract”.

  Some contractual obligations cannot be performed without collecting and processing certain personal data. This is often the case for SMEs, which process personal data of their customers, employees or suppliers in order to be able to carry out a contract with them.

  Contract can also be used as a lawful basis by enterprises carrying out pre-contractual requests from potential clients (e.g., when a potential client asks a home repair company to provide a quote to paint his house). Only situations where requests originate from the potential clients, and were not the initiative of the controller or any third party, are covered.

  “Contractual necessity” should be interpreted strictly. This means that you must be able to demonstrate that processing personal data is objectively necessary for a purpose that is integral to the performance of the contract or for addressing the pre-contractual request (e.g. name of the contracting partner, contact data of a customer or client, delivery address etc.). On the contrary, processing which is useful, yet not objectively necessary, for performing the contractual service or for taking relevant pre-contractual steps will not be covered, even if it is necessary for your other business purposes.
To decide whether you can rely on “contractual necessity” to justify your enterprise’s processing activities, it is essential that you determine the precise substance and fundamental objective of the contract. Then, you need to be able to demonstrate how the main object of the contract cannot be performed without the specific processing of the personal data in question. Detailed background checks of potential customers or clients – such as health checks by an insurance company or credit reference checks by a bank – are not to be considered as necessary steps made at the request of the potential customer or client.

This does not mean that such processing activities are per definition illegal, the lawful bases of “consent”, “legitimate interest” or “legal obligation” could be applicable.

Example:

A customer goes to a small enterprise selling electronics and there he learns that the laptop he was planning to buy is currently out of stock. The customer orders the laptop and asks for it to be delivered to his home address when available. To be able to deliver the laptop – and thus perform the contract – it is necessary for the enterprise to process the customer’s name and address. If after the delivery of the laptop the enterprise wants to process the customer’s data to send promotional e-mails, this processing cannot be considered objectively necessary for the contract’s performance. In practice this means that the enterprise must resort to a different lawful basis that could be appropriate for processing for marketing purposes (e.g. consent or legitimate interest).

💡 The fact that certain personal data processing is included in a contract does not automatically mean that the processing is necessary for its performance!

Legal obligation

The GDPR has also foreseen the possibility to justify your personal data processing activities in case you find yourself in a situation where processing is necessary for compliance with a legal obligation of the controller.

To be able to rely on this lawful basis, the obligation to process personal data must be imposed by EU law or the applicable national law of an EU Member State (including secondary legislation or a binding decision of a public authority) and must be mandatory.

A contract, a voluntary unilateral engagement or a public-private partnership are examples that can never qualify as a legal obligation in this sense, when processing personal data beyond what is required by law.
It is important that the legal obligation on which you want to base your processing does not leave room for discretion as to the manner of compliance. This rules out provisions in instruments such as general policy guidelines. The legal obligation must be sufficiently clear regarding the processing of personal data it requires, referring explicitly to the nature and object of the processing. If this is not the case, you will have to look for another lawful basis for your processing.

Examples of valid legal obligations could be:

- A legal obligation of banks to consult an official list of registered debtors;
- An obligation on employers to report salary data of their employees to social security or tax authorities by using the employee’s social security number;
- An obligation on financial institutions to report suspicious transactions to the competent authorities under anti-money-laundering rules.

### Legitimate interest

Sometimes personal data processing is necessary to pursue legitimate interests of the enterprise (or a third party). Those legitimate interests can serve as a lawful basis for processing, provided that the interests and (fundamental) rights of the individual concerned are not overriding such interests.

A legitimate interest is a clearly articulated benefit to your enterprise, to third parties or to society, that results from processing personal data in a lawful way. It must concern a real and present interest that is expected in the very near future, ruling out interests that are too vague or speculative. An interest can be considered as legitimate if it is in accordance with the applicable EU and national law.

The objective of the “legitimate interest” ground is to give controllers the necessary flexibility for situations where there is no undue impact on data subjects. In other words, it should not be a wildcard.

There exists no exhaustive list of what a legitimate interest can be but the GDPR and the “Art. 29 Working Party” (now: European Data Protection Board) give some examples:

- Processing to prevent fraud
- Ensuring the health and safety of staff
- Employee monitoring for safety or management purposes
- Physical, IT and network security
- (Direct) marketing and other forms of advertising
- Unsolicited non-commercial messages, including for political campaigns or charitable fundraising
• Exercise of the right to freedom of expression or information, including in the media and the arts
• Scientific research
• Historical, scientific or statistical purposes

Thus, a broad range of interests could potentially qualify as a “legitimate interest”. However, merely having a legitimate interest does not automatically mean that you are lawfully processing personal data. There should be a case-by-case assessment for every single personal data processing activity that is to be justified on the ground of “legitimate interest”.

When you decide to justify your personal data processing by relying on the legitimate interest ground, make sure to perform the 3-step assessment – or, the legitimate interest assessment (“LIA”).

How to conduct a LIA?

Based on the accountability and transparency principles, it is necessary to document and keep records of the legitimate interest assessment. This allows you to prove you conducted a LIA and to justify your decision to rely on “legitimate interests” for your processing activities.

* Insert (link to) ICO’s LIA template here*

**Link – Principles relation to the processing of personal data**

* Consent

You could be allowed to process personal data when the persons concerned have given you their consent to do this.

“Consent” in the sense of the GDPR presents individuals with real choice and control. It should put individuals in charge, build trust and engagement, as well as positively benefit your enterprise’s reputation.

For the consent to be valid it should be freely given, specific, informed, and unambiguous.

A common misconception is that “consent” is the main basis for data processing. Although it plays an important role, it is certainly not excluded that, depending on the context, other lawful bases are more appropriate. Because of the strict, cumulative requirements for valid consent under the GDPR, it is better to be cautious about the use of "consent" and to merely fall back on this when no other lawful basis is better suited.

To be able to rely on “consent” as a lawful basis under the GDPR, it should be:
Freely given:

This implies that a genuine choice to agree or not should exist for the person whose consent is requested. It rules out situations in which an imbalance of power or a dependency exists between you and the individual concerned, as this often leads to fear of negative consequences of the refusal of consent.

In case you are processing in the capacity of a public authority or an employer, you will need to be extra cautious when relying on consent!

Freely given consent also excludes the possibility of “bundling consent”. Consent cannot be made a condition for the provision of a contract or service since “consent” and “contract” are two distinct lawful grounds for processing personal data. Therefore, bundling consent with the acceptance of terms or conditions does not constitute valid consent under the GDPR.

Example: An SME selling bicycles processes address details of its customers in order to fulfil its contractual obligation to deliver the bicycles that were ordered to the correct locations. However, if this SME only delivers the bicycles under the condition that customers agree to processing their e-mail addresses for the purpose of sending promotional mail, it is not obtaining GDPR-compliant consent.

There should be “granularity” in obtaining consent: individuals should be free to choose for which individual processing activities and purposes to grant consent and for which not.

You should separate the different purposes of your processing activities and obtain consent for each of these activities while providing individuals with the choice to only agree to one of the processing activities!

Example: The owner of a local real estate agency asks for its clients consent to process their telephone numbers when they make an appointment to check out a certain property. The purpose thereof is to be able to contact the potential clients in case they are late. Moreover, the owner wants to sell these telephone numbers to renovation companies who will use the information for marketing purposes. Consent for both processing activities is asked, however, without the choice to solely agree to one of these processing activities. Consequently, this consent is invalid.

For consent to be freely given it should not result in any detriment. You should ensure that no negative consequences – such as costs or a downgrade of the service – follow from a refusal or withdrawal of consent.

Example: A company selling goods online wants to start targeting its advertisements to certain (groups) of people. Therefore, it asks the visitors
of its website to consent to the tracking of their online behaviour. If visitors do not grant their consent, the company is not allowed to ‘punish’ them by providing them with a less favourable experience, for example banning them from opting for the fast delivery option.

- **Specific**

  GDPR-compliant consent should also be used for a *specific purpose*. From that it follows that consent may not be given as a general authorization to process the personal data for any purpose.

  🗣 A request for consent must be specific, separated from information relating to other matters, important and may not be hidden behind lengthy terms and conditions.

- **Informed**

  When relying on consent to justify the processing of personal data, you should always make sure that you *provide individuals with the necessary information, allowing them to make a meaningful choice*. This is also in line with the transparency principle, one of the main principles upon which the GDPR is built.

  [Link – Principles relation to the processing of personal data > Transparency principle]

  **What kind of information should you provide?**

  - The identity of the controller (your enterprise) and the purposes of the processing for which the personal data are intended
  - The type of data that will be collected and used;
  - The existence of the right to withdraw consent;
  - If the data is to be transferred to, or processed by, other controllers who wish to rely on the original consent, these controllers should all be named. (it is not necessary to name processors)
  - The information that is part of your privacy policy.

  **How should you provide this information?**

  **Requests for consent need to be intelligible, easily accessible, using clear and plain language.** To decide this, it is essential that you consider your audience. Many of the required information will be provided through your privacy policy, to which you provide a link in your consent request.

- **Unambiguous**

  A final requirement for valid consent is that it should be *unambiguous*. This means that consent should be *obtained by statement or a clear affirmative action to avoid confusion.*
<table>
<thead>
<tr>
<th>Do’s</th>
<th>Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require the ticking of an unticked box to obtain consent</td>
<td>Do not interpret silence or inactivity as consent</td>
</tr>
<tr>
<td>Provide individuals with the possibility to actively choose technical settings to allow the use of cookies or other conduct that clearly indicates that the individual accepts the proposed processing</td>
<td>Do not use pre-ticked boxes</td>
</tr>
</tbody>
</table>

🔗 Time for action - draft an informed consent form.

An informed consent form is a document setting out specific information about the personal data processing you undertake and for which you want to obtain the individual’s consent. All the information set out above should be included and all the requirements for obtaining valid consent should be considered in the drafting of this document.

Besides the 4 requirements for valid consent, it is of the utmost importance that your company can grant and accommodate individuals’ right to withdraw consent.

Read more

- Allow individuals to exercise the right to withdraw consent at any time.
- Information on the right to withdraw consent and on how to exercise it should be provided upon request for consent.
- Withdrawing consent should be made as easy as giving consent and should not require undue effort. Changing to another electronic interface (website, app or email) just for withdrawing consent is not allowed.

  E.G. Consent obtained through ticking a box on a website, should not have to be withdrawn by contacting a call center

  It should not necessarily take place through the same action

- Withdrawing consent should not lead to any detriment for the individual concerned.

  E.G. no fee, no lowering of service levels

mlink In principle, data processed on the basis of consent needs to be deleted when consent is withdrawn or is no longer valid, unless another lawful basis can be relied upon to justify the continued processing of the personal data.
Subsequent to the accountability principle, companies must keep records to prove consent was validly obtained. The records should allow them to easily identify (and prove to the supervisory authority where needed):

- Who: Which individuals gave consent?
- When was consent obtained?
- How was consent obtained?
- What: To what exactly did the individuals agree?
Special categories of personal data

Special category data is personal data that is deemed more sensitive, and hence, in need of more protection. Processing such data could create more significant risks to a person’s fundamental rights and freedoms (e.g. unlawful discrimination).

The GDPR lists 10 special categories of personal data:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for id purposes);
- Health
- Sex life
- Sexual orientation.

In principle, the processing of special categories of personal data is prohibited (Art. 9(1)GDPR). This general prohibition is lifted only if – additional to a lawful basis for your processing – one of the specific conditions exhaustively listed in the GDPR (Art. 9(2)) is satisfied. Any other processing of special categories of personal data is unlawful.

Therefore, before starting to process sensitive data you must determine whether any of the GDPR justification grounds apply and you should document it.

Link – Processing Situations > XXXX

Read more

[Not all legal bases are relevant for SMEs, you will most commonly be able to rely on the following grounds:

- Explicit consent of the individual whereby the individual will indicate that he or she understands and agrees that special categories of personal data will be processed (unless prohibited under national law!).

This form of consent is even stricter than the usual high standard of consent under the GDPR, which requires all consent to represent a specific, informed and unambiguous indication of the individual’s wishes. Explicit consent requires the strongest form of agreement by additionally requiring the person concerned to give an express statement of consent (E.G. by way of a written statement) while referring to the element of the processing that requires explicit consent.

In practice, this means that consent inferred from a person’s actions is not a form of explicit consent. This does not exclude pre-written consent statements, as long
as you ensure that individuals can clearly indicate they agree with the statement (E.G. by ticking a box or signing the statement).

 Explicit consent can also be obtained orally, but in that case a record of the script should be kept!

• Processing in the field of employment, social security and social protection law if authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

• Processing necessary for the establishment, exercise or defence of legal claims.

• Processing for individual health care purposes
  ▪ Processing necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. SMEs should assess whether specific EU or national legislation is adopted authorizing them to process the data.
  ▪ Processing pursuant to a contract with a health professional, carried out by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies. E.g. doctors or psychologists

Time for action -

• It is very important to still check the national law of the country in which you are processing special categories of data, as the GDPR leaves room for Member States to introduce additional conditions and safeguards.

• Due to the sensitive nature of these types of personal data, it is important to place special emphasis on data security! Appropriate technical and organisational measures should be put in place, such as access restrictions, encryption, etc.
Specific rules for consent & children

Useful link

**Link – Consent and children’s data**

---

**Is my enterprise a data controller or data processor?**

**In a nutshell**

Every time you process personal data, you will do so either as a data controller or as a data processor. It is very important to know in which of these roles you are operating for each and every data processing activity you undertake. This is because the legal obligations you will bear, differ according to this qualification.

This section aims to clarify when your company will qualify as a data controller, or rather a processor.

**When am I a data controller or a data processor?**

[Video animation]

*Controller or processor? [pop-up window]*

<table>
<thead>
<tr>
<th>Guiding questions</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did you take the initiative to start collecting or processing in any other way personal data?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Did you decide the purpose of the processing?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Did you decide which types of personal data are to be collected and from which types of individuals?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you giving instructions to another entity processing personal data, rather than following instructions from someone else?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td>Are you the party mainly benefiting from the result of the processing?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a direct relationship with the individuals concerned (e.g. a contract or employment)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you monitor other entities’ execution of the service?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your enterprise visible to the individuals concerned? (Visibility comes with expectations from the individuals) The lower the visibility towards the individuals, the more likely you are a processor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you the enterprise with the highest professional expertise?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The more you have indicated ‘yes’, the more likely you are a controller. Mainly ‘no’ answers indicate that you are probably acting as a processor. If you answered “yes” on the second question, you are a controller in any way.

Or joint controller? [pop-up window]

Guiding questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you have a common objective and purpose with other parties regarding the processing?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you using the same set of personal data for this processing as another controller?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have you designed the process with another controller?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Do you have common information management rules with another controller?

| In case you have indicated ‘yes’ once or more, you are most likely processing personal data as a joint controller. |

**Obligations and liability**

If your enterprise is acting as a controller, you will carry the highest level of compliance responsibility: you will not only have to **comply with all the data protection principles** as well as all other GDPR requirements, you will also need to be able to **demonstrate compliance**.

[Link – Accountability’ under the ‘data protection principles’]

Additionally, **as a controller you are responsible for the compliance of your processor(s)**. Below you can find a short summary of all controller obligations under the GDPR.

**For Data controller**

If your company is acting as a controller, you will carry the highest level of compliance responsibility: you will not only have to comply with all the data protection principles as well as all other GDPR requirements, you will also need to be able to demonstrate compliance.

[Link – demonstrate compliance? where is this?]

Additionally, as a controller you are responsible for the compliance of your processor(s). Below you can find a short summary of all controller obligations under the GDPR.

**For Data processor**

New under the GDPR is that processors also carry a limited number of specific legal obligations, however, a lower level of compliance responsibility will be applicable. In a scenario where your company acts as a processor, your obligations are the following:

As a processor you can only process data in accordance with the controller’s instructions, unless you must process data pursuant to a legal obligation. If the latter is not the case and instructions were disobeyed, you will be requalified as a controller. Further processing data without prior written consent of the controller. If a processor is responsible for a breach, they will be legally liable. Individuals and supervisory authorities can bring claims for compensation and damages.

**For joint controllers**
In a situation of joint controllership, you will also have to fulfil all obligations aimed at controllers.

For an overview of all these obligations, see section on Data controller.

Additionally, as a joint controller, you will need to draw up an agreement to establish clear arrangements with the other controller(s) regarding the division of duties, tasks and responsibilities, unless these are already determined by EU or Member State law.

A contact point should also be designated for individuals concerned, to which they can turn in case of questions or complaints.

Regardless of the agreement between joint controllers, joint controllership implies joint liability: each controller can be held fully liable, vis-à-vis affected individuals, for the entire damage caused. The data subject is thus entitled to bring a claim against whichever of the joint controllers he or she wishes. This is to ensure that the data subject is effectively compensated.

Afterwards, the joint controller who paid the compensation can seek to recover damages from any other joint controllers involved in the joint processing. An exemption exists only if the controller is not in any way responsible for the harm.
Data processing agreements

In practice, many companies turn to third parties to process personal data – also SMEs!

Think of an email client, a cloud storage service or website analytics software. In all these situations, the GDPR requires you to put in place a data processing agreement with all the third-party services providers.

A data processing agreement is a legally binding document between the controller and the processor, in writing or in electronic form. It governs the specificities of data processing (which type of data will be processed, for which purpose, on which ground will the processing take place etc.), as well as the relationship between the controller and the processor – including the rights and obligations. Besides the fact that a data processing agreement is required by law, it also assures you that the data processor you are using is qualified and competent.

There are eight topics that need to be included in a data processing agreement:

1. The processor will only process personal data according to documented instructions of the controller – unless there is a Union or Member State law applicable to the processor
2. All persons authorised to have access to the personal data, are committed to confidentiality
3. The processor will ensure security of personal data by taking all reasonable, appropriate technical and organisational measures under article 32 GDPR.
4. The processor will not subcontract data processing activities to another processor, unless instructed to do so by the controller (in that case a data processing agreement will also need to be drafted with the subprocessor in question)
5. By taking the possible and appropriate technical and organisational measures, the processor will assist the controller in fulfilling the latter’s obligation to respond to request for exercising data subject’s rights
6. Based on the nature of processing and the information available to the processor, the processor will also assist the controller in maintaining GDPR compliance with regard to security of processing (article 32) and the obligation to consult the data protection authority before undertaking high-risk processing (article 36)
7. The processor will delete all personal data after completion of services relating to processing or will return the data to the controller (choice of the controller)
8. The processor will provide the controller all information necessary to demonstrate compliance and will allow the controller to carry out an audit and will aid if requested to do so.

The European Data Protection Board (EDPB) wants companies to do more than just simply reiterate the GDPR provisions, it encourages to specifically define processes around the processor’s obligations. For example, determine specific steps for the processor to address an access request by an individual or to describe in detail the purpose and nature of the processing activities carried out on behalf of the controller, as well as the type of data processed, categories of individuals concerned and the duration of the processing. The Board also suggests including the list of the subprocessors as an annex to the agreement.
By not entering into a data processing agreement in cases where this is required, you will risk a fine!

*Insert Danish DPA template here*

**Time for action [pop-up window]**

- Before engaging in any processing activities, **make sure to assess whether you are a controller, processor or joint controller** in relation to the processing activities taking place.
- In case you are working with a processor, **draft a data processing agreement** between yourself and this processor, including certain mandatory provisions.
- In case you are acting as a processor, make sure you **do not go beyond the controller’s instructions** as this potentially constitutes a violation of data protection legislation, resulting in your enterprise being liable.

**SMEs & the GDPR**

The application of the GDPR depends on **the nature of your enterprise or organisation activities**, not on its size.

The GDPR introduces a **risk-based approach** into data protection law. This means that activities posing high risks to individuals’ rights and freedoms, **regardless whether they are carried out by an SME or by a large corporation**, trigger the application of more stringent rules.

Nevertheless, the GDPR encourages the Union institutions and bodies, Member States and their supervisory authorities, to take account on the specific needs micro, small and medium-sized enterprises may have regarding **the application of this Regulation**.

Additionally, the Regulation also recognises the specific situation of micro and small companies (to a limited extend) by allowing, under certain conditions, that **some of the obligations of the GDPR do not apply to certain SMEs**.

- The obligation to appoint a **DPO** does not apply to SMEs when processing is not their main business and the processing does not pose specific threats to individuals’ rights and freedoms. Indicators for such threats are for example (1) processing sensitive data or criminal records (2) monitoring individuals or (3) large scale processing.

**Link - Should my company appoint a DPO?**

- Companies with fewer than 250 employees do not have to keep records of their processing activities unless they regularly process personal data, pose a threat to individuals’ rights and freedoms, or process sensitive data or criminal records.

**Link - Recording and managing content**
Consequences of GDPR non-compliance

1. **In a nutshell?**

Not complying with the GDPR implies that you are unlawfully processing personal data of the persons concerned and or not taking the required safety measures.

This may mainly result in:

- inadequate protection of personal data, data breaches and theft of sensitive company information, such as trade secrets
- complaints from your employees
- complaints from customers and clients
- administrative audits conducted by the data processing authorities
- administrative fines may be imposed, which may, in worst case rise up to 20 million euro
- other local fines and criminal charges under national law
- you may become ineligible to participate to public tenders or to work for clients or customers who have to be GDPR compliant themselves
- negative publicity

2. **More information**

(a) Data breaches and theft of sensitive information such as trade secrets [Read more]

Many obligations following from the GDPR have as a purpose to ensure that you process personal data in a thoughtful way, adequately protection your (personal) data and entire ICT infrastructure against undesired access, both from within as from the outside.

This means that by complying with the GDPR, you will also better secure and protect your company against cyberattacks, data breaches, etc. Furthermore, duly organising the way data is used and accessed in your company, will also protect other sensitive business information and trade secrets from being easily accessed by unauthorized persons and/or leaked to third parties.
(b) Complaints by customers, clients and employees

Citizens are becoming more and more aware of their privacy, of the importance of data protection and of the obligations of businesses with regards to data protection.

This means that also your clients, customers and employees may disapprove if you do not treat their personal data in a GDPR compliant way and my complain about this, to you, to third parties, to social media or to the government.

They may also try to use this against you, for example if there is a disagreement or a dispute about something related to your relation with these persons, they may try to use your non-compliance in their favour. For example by threatening to file a complaint at the data protection authority.

(c) Administrative audits and administrative fines

The data protection authorities may start an audit, triggered by a complaint or on their own initiative, when they notice that some of your publicly available information or communications appears to be non-compliant.

In that case, you will have to demonstrate that you comply with all provisions of the GDPR, which will take time and effort. And if non-compliance is established, this may result in administrative GDPR fines, which may in theory amount up to 20 million euros (or 4% of the yearly worldwide turnover, if that amount is higher). In practice the altitude of the fines will be much lower and will depend on the kind of infringement and the effort you have already put in complying with the GDPR, but this is of course not something you want to test.

(d) Other local criminal fines and criminal charges under national law

Depending from the countries in which you are active, local laws may impose criminal prosecution and fines in case of non-compliance.

(e) You may become ineligible to participate to public tenders or to work for clients or customers who have to be GDPR compliant themselves

When you provide services to public authorities or to customers or clients in regulated sectors, they will often impose on their suppliers to be GDPR compliant.
Non compliance may therefore exclude you from being able to participate to such projects or calls.

(f) Negative publicity [Read more]

Not being GDPR compliant may cause negative publicity, for example to clients who care about their privacy, by being called out by activists on social media or by being mentioned in the press when a data breach occurs.

3. Time for action [pop-up window]

Start today with your GDPR compliance. Don’t know where to start? Read our section on “Where to start compliance?”
Data breaches: now what?

1. **In a nutshell?** [Illustration/Infographic]

A **personal data breach** means any accidental or unlawful unauthorised disclosure, loss, destruction, alteration of, or access to, personal data you process in any way, including during transmission or storage.

A personal data breach must:

- **be notified to the data protection authority** within 72 hours, **unless** the personal data breach is unlikely to result in a risk to the rights and freedoms of the concerned persons
- **only be communicated to the concerned persons**, **if** the breach is likely to result in a high risk to the rights and freedoms of the concerned persons

Furthermore, you should of course also take all reasonable measures to avoid further risks and to avoid that the breach may be reproduced.

To demonstrate your compliance, you should have a **record of data breaches** and a **data breach policy**.

2. **More information**

   (a) **Personal data breach** [Read more]

Any of the following situations are data breaches:

(i) The personal data you process is seen, received, accessed or accessible by/to unauthorized persons

    1. examples:

       a. a file with personal data is sent to the wrong person

       b. an unauthorized person has had access to your systems and may have been able to access, copy, view, destroy, etc. personal data

       c. a database with personal data was open for the public to access it
and you cannot determine with certainty whether it was accessed or not

d. some employees had “read-only” access to personal data to which they were not allowed to have access and you cannot determine with certainty if they accessed it or not

e. an account of an employee has been hacked and you cannot determine with certainty if the hacker accessed the personal data that the employee has access to

(ii) The personal data is lost, destroyed or damaged

1. “destruction”: the data no longer exists or no longer exists in a form that is of any use to the controller.

2. “damaged”: personal data has been altered, corrupted, or is no longer complete.

3. “lost”: the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession.

4. examples:

   a. a laptop or storage media is lost (such as a USB-stick), even if the device is encrypted

   b. a file that contains personal data cannot be retrieved

   c. a file with personal data is encrypted by ransomware

   d. the password of an encrypted file with personal data is lost and there are no other, accessible copies of the file

(b) Notification to the data protection authority

(i) The controller must notify data breaches to the data protection authority within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons (e.g. the data were encrypted).

(ii) If the breach is not notified within 72 hours, the controller must inform the data protection authority of the reasons for the delay.
(iii) A notification may be made in phases, i.e. the available information can be part of the initial information and additional information can be added to the file later.

(iv) The notification must include at least the following information:

1. the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. the name and contact details of the data protection officer or other point of contact from which further information can be obtained; the likely consequences of the breach;
3. the measures taken or proposed by the controller to address the data breach including, where appropriate, measures to mitigate any possible adverse effects.

The controller must adequately document all personal data breaches, including the related facts, effects and the remedial measures taken.

(c) Notification to the persons concerned [Read more]

(i) When a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the controller must inform the data subjects of the breach without undue delay.

(ii) The controller must describe, in clear and plain language, the nature of the personal data breach and indicate:

1. the name and contact details of the data protection officer or other point of contact from which further information can be obtained; the likely consequences of the personal data breach;
2. the measures taken or proposed by the controller to address the breach including, where appropriate, measures to mitigate any
possible adverse effects.

(iii) If the controller does not inform the data subjects of the breach, the supervisory authority, after having assessed the risk posed by the breach, may require it to do so.

(iv) The controller does not need to inform the data subjects of the personal data breach if:

1. it has implemented appropriate technical and organisational protection measures which were applied to the personal data affected by the breach, in particular measures, such as encryption, that render the personal data unintelligible to any person who is not authorised to access them;

2. it has subsequently taken measures to ensure that a high risk to the rights and freedoms of the data subjects is no longer likely to materialise; or

3. doing so would involve disproportionate efforts, in which case it shall make a public communication or take similar measures to ensure that the data subjects are informed in an equally effective manner.

(v) The processor’s role

1. The processor must notify the controller without undue delay after learning of a personal data breach.

(d) A data breach policy [Read more]

Establish a data breach policy in which you describe how your employees should react when a data breach occurs, who they should inform etc. And make sure that you inform your employees about the content of this policy.

(e) A record of data breaches [Read more]
A record of data breaches must be established. In this record, you should not only note the data breaches that required notification, but also data breaches that remained below the notification threshold.

3. **Time for action** [pop-up window]

   (a) Assess the technical and operational security measures in place within your organisation and make the appropriate adjustments, if necessary.

   (b) Establish a data breach policy and a record of data breaches

   (c) Have your systems tested regularly by an external party.

   (d) Put in place an appropriate data breach notification procedure.

   (e) Train your employees and contractors in security awareness.

4. **Sources**

   Art. 33-34 GDPR

   Guidelines wp250rev01
Should my company appoint a DPO?

1. In a nutshell

Under certain conditions, the GDPR obliges companies to appoint a DPO. DPO stands for “data protection officer”. The primary role of a DPO is to ensure that your company processes personal data of your staff, customers, providers or any other individuals in compliance with the applicable data protection rules. In light thereof, a DPO should assists your company to monitor data protection compliance, provide information and advice on your data protection obligations and act as a direct contact point for individuals with regard to all issues related to processing of their personal data and the exercise of their rights under the GDPR, as well as a contact point for the competent Data Protection Authority. As the DPO forms an integral part of the organisation, it is ideally placed to guarantee data protection compliance.

2. More information [Read more]

The fact that your company qualifies as a micro-enterprise or an SME does not – as such – free you from the potential obligation to appoint a DPO. The GDPR employs a risk-based approach in this context: the provisions on data protection officers (articles 37 – 39 GDPR) – while not explicitly mentioning the word ‘risk’ – do link the obligation to designate a DPO to the nature, scope and purposes of data processing operations and not to quantitative characteristics (e.g. number of employees) of the entity processing personal data. Mostly, micro-enterprises process personal data for managing their relations with employees, (potential) customers and suppliers, which likely qualifies as low risk. Nevertheless, small companies often also use personal data for (direct) marketing purposes or make use of new and more invasive data processing technologies which means that the provisions on the appointment of a DPO are also relevant for micro companies.

Should I appoint a DPO? [Read more]

There are four situations in which a DPO must be appointed:
Important to note is that, even in case your company is not obliged to designate a DPO under the aforementioned criteria, you are still entitled to do so on voluntary basis.

**How to appoint a DPO? [Read more]**

The DPO may either be a staff member of your company (or of your processor) appointed within the company, or you can outsource the position by means of a service contract with an individual or an organisation outside of the company.

Before appointing your DPO, you need to check whether the candidate has the necessary (professional) qualifications. All the statutory requirements, tasks and duties listed below should be fulfilled irrespective of whether the DPO is appointed internally or externally and on a mandatory or voluntary basis.

1. **Independence** [Illustration/Infographic]

Important is that the DPO should be able to perform its duties independently. This means that you should refrain from providing instructions regarding the exercise of the DPO’s tasks, as well as from dismissing or penalising the DPO for performing his tasks. Contracts concluded with the DPO should contain appropriate terms to avoid vulnerability of DPO: no unfair termination terms, contractual sanctions, other direct or indirect instruments that may affect independence of DPO.  

---

24 See details at Guidelines on Data Protection Officers p.p. 12
2. **Data protection expert**

When choosing your DPO, assess whether the candidate has expert knowledge of data protection law and practices, as well as the ability to fulfil DPO tasks. Knowledge in the relevant business sector and the functioning of the organisation represented by the DPO should also be taken into account.

3. **Adequate resources**

You must provide adequate resources to enable the DPO to meet its GDPR obligations and to maintain its expert level of knowledge. This concerns not only financial resources, but also time, infrastructure, staff and support through other services (e.g. HR and IT).

4. **No conflict of interest**

It is not prohibited to combine the position of DPO with another position but all risks of conflict of interests should be assessed and mitigated on a case by case basis.

Example:

A company’s head of the IT department monitors all user accounts and controls the right of access to the IT infrastructure possessing rights of remote access to users’ device. The same person should not hold the position of DPO because a DPO should monitor whether the head of IT’s activities of processing users’ data are compatible with GDPR requirements which likely results in a conflict of interest in case one person holds both positions mentioned above.

5. **Secrecy or confidentiality**

The DPO should not disclose any information relating to the performance of his or her tasks, except for two situations:

- The obligation to directly report on the fulfilment of the tasks agreed upon to the highest management level of your company

- Requests for information by the competent data protection authority or any other public authority or body in accordance with EU or national law.

---

25 See details at Guidelines on Data Protection Officers p.p.14 Sec.3.2
3. Time for action [pop-up window]

- In case of any doubts concerning the necessity to appoint a DPO, it is recommended to appoint a DPO.

- Check national law before appointing a DPO or deciding not to do so, as additional requirements potentially exist regarding the procedure of designation or notification.

- Do not forget to make the contact details of the DPO publicly available (e.g. on your website) and communicate them to the competent Data Protection Authority.

- Ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

- Give the DPO appropriate access to personal data, processing activities and other services within the company so that he or she can receive essential support, input or information.

- In case you decide not to follow the DPO’s advice, document the reasons justifying this decision.

Further reading


The UK Data Protection Authority has designed a useful tool to help you decide whether or not you should appoint a DPO. You can consult the tool here: https://ico.org.uk/for-organisations/does-my-organisation-need-a-data-protection-officer-dpo/.
Should my company carry out a DPIA?

1. In a nutshell

A data protection impact assessment (DPIA) consists of a set of assessments to be carried out by your company before starting your processing operations. A DPIA serves as a tool to systematically analyse, identify and minimise (not necessarily eliminate) the data protection risks of a single processing operation or a set of similar processing operations within your company. This assessment allows you to determine if the level of risk is acceptable in relation to the benefits pursued by the planned project.

| 'Risk', through the lens of data protection law, refers to the **likelihood and severity** of any physical, material or non-material **negative impact** on the individual concerned or society at large, taking into account the **nature, scope, context and purposes of processing**! |

2. More information

**When to conduct a DPIA?**

- High risk processing operations [Read more]

A DPIA is not always required under the GDPR. However, the mere fact that your company qualifies as a micro-enterprise or an SME does not – as such – give you a free pass. The obligation to carry out a DPIA is tied to the notion of ‘high risk’: if the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals, a DPIA is required.

To decide whether a project poses a high data protection risk, the article [29 Working Party (WP 29)] – now European Data Protection Board (EDPB) – provides a rule of thumb: a **processing activity that meets 2 or more out of the 9 criteria enlisted below most likely constitutes a high risk to the rights and freedoms of the individuals concerned and therefore requires a DPIA to be carried out.**

1. **Evaluation and scoring** (including profiling and predicting), especially from aspects concerning the individual’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.

   *E.g. building marketing profiles based on people’s behaviour on your website*

2. **Automated decision-making with legal or similar significant effect**

   *E.g. processing that automatically leads to the decision to exclude an individual from your services.*
3. Systematic monitoring

*E.g. monitoring of a publicly accessible area*

4. Sensitive data or data of a highly personal nature

*E.g. Special categories of personal data, data relating to criminal convictions or offences, but also other types of personal data which could be considered sensitive in the broad sense of the word, such as location data or financial data.*

5. Large scale data processing

*E.g. processing in which an extensive number of individuals are concerned (either as a specific number or as a proportion of the relevant population), processing of a large volume and/or variety of data, processing of personal data for a long period of time or processing data with a large geographical extent.*

6. Matching or combining data sets

7. Data concerning vulnerable data subjects

*E.g. data concerning children, employees, elderly etc.*

8. Innovative use or applying new technological or organisational solutions

9. Processing which itself prevents data subjects from exercising a right or using a service or a contract

*E.g. a bank screening its customers against a credit reference database in order to decide whether to offer them a loan.*

In some cases you could still consider that a processing activity meeting only 1 of the 9 criteria requires a DPIA.

**Example:**

<table>
<thead>
<tr>
<th>Processing activitie(s)</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing personal data gathered across social media platforms to create marketing profiles.</td>
<td>Evaluation or scoring</td>
</tr>
<tr>
<td></td>
<td>Matching or combining of datasets</td>
</tr>
<tr>
<td></td>
<td>Large scale processing</td>
</tr>
</tbody>
</table>

3 out of 9 criteria are met 🡪 DPIA necessary!

To find out if you are required to carry out a DPIA, check out our [pre-DPIA template].

- National DPIA lists [Read more]
The GDPR instructs national data protection authorities (DPAs) to draw up their own lists of processing operations which are subject to the requirement for a DPIA. Additionally, they are free to also make a list of processing operations which do not require a DPIA. If your DPA has such a list, it is important to check this list before starting any data processing operations. National DPIA lists can be found here.

- Uncertainty [Read more]

In case it is not entirely clear whether the processing activities performed by your company are likely to result in a high risk to the rights and freedoms of individuals, it is advised to carry out a DPIA. Taking into account that no criteria nor lists can be considered exhaustive as there could always be high risk processing situations that are not foreseen by law or by national DPAs, it is safest to carry out a DPIA in any case.

Moreover, conducting a DPIA should also be seen as a way of complying with the accountability obligations under the GDPR. It helps you to keep an oversight on the processing activities taking place within your company by documenting risks and demonstrating compliance with the data protection rules. Hence, it is good practice to perform a DPIA for any major project which requires the processing of personal data, even if not obliged.

How to conduct a DPIA? [Read more]

After identifying the need for a DPIA, the following steps should be taken:

1. A systematic description of the envisaged processing operations and the purposes of the processing. If you rely on ‘legitimate interest’ as the lawful basis for the processing, this interest should be included in the DPIA

2. Conducting a DPIA is your company’s responsibility, whenever you are acting as a data controller. Nevertheless, you should consult your DPO, if appointed, as well as other actors

3. An assessment of the necessity and proportionality of the processing operations: (1) Is the processing of personal data in the planned manner necessary to achieve the envisaged purpose(s)? (2) Is the interference with the rights and freedoms of the individuals concerned not disproportionate in relation to the pursued purpose(s)?

4. An assessment of the risks to the rights and freedoms of data subjects (e.g. privacy)
5. An identification of the measures envisaged to address the risks (e.g. safeguards and security measures) and a demonstration of compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

6. Keeping records of the outcomes.

7. Periodical reviewing: processing activities are dynamic and can evolve quickly which could cause new risks to the rights of individuals. For that reason, you should periodically reassess whether the DPIA that was conducted before, still corresponds to the processing activities taking place within your company at that time. If there is no DPIA in place, you should check whether the processing activities at that time do result in high risks to the rights and freedoms of individuals. In that case, a DPIA is necessary.

For more information and examples you could check your DPAs website.

*When to consult the DPA? [Read more]*

If the DPIA indicates that the planned processing operations are high risk and find that it is not possible to implement measures to mitigate the identified risks, you should consult the competent DPA before starting to process any personal data.

In case of such a prior consultation, the DPA will advise you how to limit the risks relating to your processing. If your company implements the suggested measures, you will be allowed to start the planned processing. On the other hand, it is also possible that the DPA advises you to completely abandon the planned processing.

When you are able to identify mitigation measures that are able to cover the risks in a sufficient manner, no prior consultation of the DPA is required.

3. **Time for action [pop-up window]**

- Assess whether planned and existing processing activities are likely to result in a high risk.
- A DPIA is a living tool so update your DPIA when the circumstances surrounding the processing have significantly changed.
- Check the DPIA lists of the national DPAs.
- Ask for DPO’s advice if your company has appointed one.
- Do not forget to document your DPIA.
When to still check national law?

1. In a nutshell

This section of the Handbook highlights situations where national data protection law should still be consulted. Despite the fact that the GDPR aims to harmonise data protection law across the EU, in a number of cases the Regulation does allow Member States to adopt national laws which deviate from or supplement the GDPR. In practice, this means that for some data protection aspects you will encounter different rules from one Member State to the next.

! If you operate in more than one Member State, it is important that you take into account the possible differences in national legislation!

2. More information

A distinction should be made between areas where Member States must have national or regional laws and areas where Member States may have such laws.

**Areas in which Member States must have local laws:** [Read more]

- Personal data and freedom of expression: the exception for processing for journalistic purposes and purposes of academic, artistic or literary expression.

  Member States remain responsible for determining the balance between the right to privacy and the right to freedom of expression. If you are working in the media sector, note that you should carefully consider the fact that the rules in this area will differ from one Member State to the next.

- Personal data contained in official documents:

  Such personal data may be processed in order to reconcile public access to official documents with the right to the protection of personal data. Member States are responsible to balance the right to privacy and the need to process personal data where this is necessary in the public interest.

- Penalties
**Areas in which Member States may have national or local laws:** [Read more]

- Professional secrecy and its reconciliation with the right of personal data protection. Member States are free to put in place specific obligations regarding professional secrecy in certain sectors (e.g. law firms or banks).

- Processing for scientific, historical or statistical purposes: Member States can restrict data subject’s rights (to access, rectification, restriction of processing and to object) because they threaten to render impossible or seriously impair the achievement of those purposes, under the condition of setting out appropriate safeguards and if there is no risk of breaching the privacy of the data subject.

- Seeing that employment laws of Member States mostly remain outside the scope of legislative competence of the EU, the GDPR leaves room for Member States to create laws governing the relationship between the GDPR and national employment law. In practice, if your company operates in multiple Member States, you will face different requirements with respect to the processing of personal data of employees.

- Personal data of deceased persons

- Children’s age of consent

- Special categories of data

- Genetic, biometric or health data

**The use of surveillance camera’s**

- Rules about Data Protection Officers

- National identification numbers (any other identifier of general application). Member States are free to set their own rules regarding the processing of national ID numbers.

- Under certain conditions churches and religious establishments are allowed to impose rules on the processing of personal data

3. **Time for action** [pop-up window]

   - Consider which Member States’ laws apply to your operations and go check national data protection law for additional or more specific obligations
Where to start compliance?

In a nutshell

With all GDPR obligations, it can be quite difficult to see the wood for the trees and understand where to start with the implementation.

Don’t panic, you are at the right place.

Here we will provide you with a step-by-step guide on how to become GDPR compliant.

This implementation should be a general matter of common sense and organisation in your enterprise, not only a technical or legal project.

Follow the guide

[link – Specific processing situations]
[link – What rights do persons have under the GDPR?]
[link – Should my enterprise appoint a DPO?]
[link – Should my enterprise carry out a DPIA?]
Principles relating to the processing of personal data

In a nutshell

The GDPR (article 5) sets out seven key principles underpinning the processing of personal data by any entity, including micro-enterprises or SMEs. Therefore, (1) lawfulness, fairness and transparency, (2) purpose limitation, (3) data minimization, (4) accuracy, (5) storage limitation, (6) integrity and confidentiality, as well as (7) accountability are relevant guidelines for you to keep personal data of your customers, employees and suppliers safe.

1. Lawfulness, fairness and transparency

Personal data must be processed legally, fairly and in a transparent manner in relation to the individual. Personal data can only be processed legally if it is covered by a “lawful basis”.

The processing of personal data must be fair, appropriate, reasonable and proportional in relation to the individuals concerned. This means that an enterprise processing personal data must weigh its own interests against those of the individuals concerned before starting the processing.

Transparency requires your enterprise to be open and clear about the processing of personal data. The person concerned should be made aware why their data is being processed, of the risks, of their rights and of other important aspects.

2. Purpose limitation

Personal data may only be collected when linked to a concrete purpose. According to the purpose limitation principle, the purpose(s) should be specific, explicit and legitimate (in accordance with the law). In addition, collected data must only be processed in a way that is compatible with the initial goal of collection.

Lawfully collected data for a given purpose cannot be used anew for purposes defined over time!

If you originally collected the data on the basis of legitimate interest, contract or vital interests, the personal data can only be used for another purpose after checking whether the new purpose is compatible with the original purpose.

Elements to take into account when assessing compatibility of purposes:
o Is there a link between the original purpose and the new purpose?
o the context in which the data was collected (what is the relationship between your enterprise and the individual?);
o What type and nature of data does it concern? (e.g. sensitive data?);
o What are the possible consequences of further processing for the individual concerned?
o Are there any appropriate safeguards in place, e.g. encryption or pseudonymisation?

If your enterprise originally collected the data on the basis of consent or based on a legal obligation, you are not allowed to further process the data beyond what is allowed by the original consent or the legal provision(s). In this scenario, further processing requires obtaining new consent or a new legal basis.

3. Data minimisation

The data minimisation principle requires an enterprise to only collect personal data which is truly necessary for the specified processing purposes.

Link –

Therefore, it is useful to identify, in advance, the minimum amount of personal data needed to fulfil the enterprise’s purpose.

EG: To perform a delivery, a footwear manufacturer collects its customers’ addresses, though it must not collect, for example, customers’ age as they are not related to the initial purpose of data collection.

4. Accuracy

According to the GDPR’s accuracy principle, legal entities, including micro-enterprises, must ensure that personal data they keep is accurate and updated, to the extent that is reasonable. This is because, under certain circumstances, inaccurate data could cause significant negative effects to the individual, especially when dealing with special categories of data (e.g. health or political beliefs).

EG: Inaccurate data provided to a credit information bureau on a person’s debt can negatively affect that person’s future chances to obtain a loan.

The extent to which data should be kept accurate depends on the purpose of data processing. For example, in case of a medical record, every possible step must be taken to ensure that the records are up to date, while an enterprise should not take extreme actions (e.g. tracking customers) to update information in a less important context, such as marketing.

EG: The enterprise should update an employee’s payroll data if it gives the employee a pay rise, or a customer’s delivery address to ensure that the purchased products are delivered to the right place.
5. Storage limitation

The storage limitation principle requires that personal data must not be maintained for longer than is necessary to fulfil the goal of their collection. Data must be erased when the data processing purpose is achieved. This means that storing any data longer than necessary is not permitted.

6. Integrity and confidentiality

Protection of personal data against unauthorized or unlawful processing, accidental loss, destruction or damage is at the core of the principle of integrity and confidentiality. The GDPR requires to ensure that personal data is not available to everyone within an organisation, but only to those who actually have to work with the data. Personal data must also be protected against any external or third actors.

The intensity of security measures is directly linked to the potential risk of data processing operations. (The GDPR follows risk-based approach)

Link –

💡 Note that before deciding what measures are appropriate to guarantee data security, your enterprise should assess potential information risks depending on the enterprise’s size, on the amount and nature of the processed personal data, as well as on how the data are used!

7. Accountability

The principle of accountability anticipates two obligations: an obligation to ensure compliance and the ability to prove it.

All the necessary technical and organisational measures should be adopted and evidence thereof should be kept. There is no list of specific means to prove GDPR compliance, but the GDPR does – under certain circumstances – require you to keep records of your data processing activities, to appoint a DPO and to conduct DPIAs. The foregoing could serve as proof of compliance.

Time for action [pop-up window]

Assess carefully:

What is your enterprise’s lawful basis for personal data collection?

- If all your enterprise’s data processing operations are brought to the attention of the individuals concerned;
- If personal data is only being collected for specific and currently existing processing purposes and not for unclear future needs;
- If your enterprise only processes the minimum amount of data necessary to fulfil its processing purpose(s);
- If the personal data held by your enterprise collected is accurate and updated;
• If all personal data for which the purpose(s) of their collection is achieved or personal data which is not relevant anymore, is deleted;
• If personal data is only accessible to individuals within the enterprise who actually need to have access;
• If your enterprise has made the necessary technical and organisational efforts to meet the GDPR principles;
• If your enterprise keeps records of its processing activities.
Tab - What rights do persons have under the GDPR

a. In a nutshell

The persons whose data is being processed remain in control of their own personal data. Therefore, you must:

(i) **inform them** if you process their data, what data you process, on what legal bases you process their data, etc

and, upon their request:

(ii) **correct** their data

(iii) entirely or partly **stop** using their data

(iv) **delete** their data and “**forget**” them

(v) provide them with a machine-readable **copy of their data**, to allow them to use it with another service provider (a competitor of yours)

(vi) stop using their data for **marketing** purposes or automated decision-making, including profiling

b. More information [illustration] [Read more]

The GDPR grants several rights to individuals in order to empower them to exercise more control over the processing of their personal data, including allowing them to understand how and why their data is being processed.

In general, requests relating to these rights should be complied with (or at least answered) **within 30 days**.
These requests can be submitted to you both orally and in writing.

The following rights will be discussed in the following topics: [Illustration]

1) Right to be informed
2) Right of access
3) Right to rectification
4) Right to erasure
5) Right to restriction of processing
6) Right to data portability
7) Right to object
8) Right to not be subject to a decision based solely on automated processing (incl. profiling)

For each icons/part of the illustration – hover on a read more

1) Right to be informed
   a. In a nutshell

1) Right to be informed

   a. In a nutshell

Individuals must be informed about the collection and use of their personal data. This information should be communicated at the following moments:
- At the time you collect their personal data from them.
- If you obtained the personal from someone else, at the latest one month after obtaining the data.

This information should mainly be provided via your privacy policy (see below).
Essentially, you must inform individuals about the following:
- Why, how and for how long you will process their personal data?
- With whom do you share the data?
- What are their rights?
- How will you protect their data?

The information must be easily accessible and written in clear and simple language. To assess whether these conditions are fulfilled, you should take into account your target audience.

b. Read more

b. Read more read more II

When you collect personal data of an individual, you must clearly inform that person that you will process his or her data.

In most cases, this happens via a form or an agreement by which the personal data is collected, including a clear reference to your privacy policy which contains further information.

Hereafter, an example of disclaimer:

“We will only process your personal data for the purposes mentioned above. We will not share your personal data with third parties other than for this purpose. Please read our Privacy Policy [/add link to your privacy policy] for more information on how we protect and process your personal data.”

Your privacy policy should contain the information as indicated under “A waterproof privacy policy”.

When using personal data for marketing communication, you should always inform the individuals about the way you process their data.

Based on the GDPR and on other applicable legislations, every commercial email should:
- contain:
  - a link to your privacy policy,
  - an unsubscribe link
▪ your company name, address and company registration number
▪ a phone number and electronic address of the company
  o be clearly identifiable as a commercial email. If such purpose would not clearly result from the format/design of the email, the commercial purpose must be mentioned explicitly in the header of the email (e.g. by explicitly mentioning "advertising" or "commercial message" in the header of the email).
  o ideally (but not mandatory) mention why you are sending emails to this person (for example “You are receiving this email because you have indicated in the past that you wish to be informed about our products”)
  o Depending on the country/countries in which you operate, other/different obligations may be applicable.

Considering the above, the footer of your emails may need to contain the following message to be compliant (for example):
“Your privacy is important to us; we process your data in accordance with the relevant privacy rules. If you wish to no longer receive our e-mails, you can unsubscribe at any moment by clicking on this link (insert link). Please find more information on how we process your data in our Privacy Policy (insert link).
© 2019 – Company and legal form – Address, Country, Company registration number – phone number and email address”

c. Time for action [pop-up window]

d. Time for action [pop-up window]
  • Draft a general privacy policy, addressed to customers, business partners, suppliers, third parties, job candidates, etc.
  • Upload the privacy policy on your website
  • Review your forms (online and offline)
  • Review your emails
  • Make sure to take these aspects into account when setting up new forms and mailings
  • Make sure to update your privacy policy when your processing activities change and, in any case, verify it once a year

2) Right of access
• In a nutshell

Any individual has the right to know if you are processing his or her personal data, to obtain information about that processing and to obtain a copy of the data concerned.

You must be able to grant requests of individuals to access their data.

• More information

When you process personal data of an individual in the capacity of a controller, you must provide that individual with the following information:

1) That you are processing his or her data
2) A copy of the data
3) Additional information

(2) A copy of the data

You must provide a copy of the processed personal data to the individual. In principle, you have to grant this request free of charge. Where additional copies are requested, you may charge a “reasonable fee”, based on the actual costs.

If the access request is made by electronic means, the data must be provided in a commonly used electronic form (except if the individual requests otherwise).

By providing a copy of the data, you should not infringe the rights of others. So, if the data would give insights in the personal data of others, you have to balance their rights against each other and evaluate if the data can be released to the applicant or not.

(3) Additional information
You must specifically provide the following information to the individual:

- **A copy** of the personal data being or to be processed
- The **categories of personal data** concerned
  - for example: contact data, financial data, purchase history, etc
- The **purposes** of the processing
  - for example: to be able to deliver specific services, to be able to perform payment, marketing purposes, etc.
- The **recipients** or categories of recipients to whom the personal data have been or will be disclosed. And in particular recipients in third countries
  - for example: your hosting provider (such as Amazon Web Services), your e-mail provider (such as Microsoft), your accountant, etc
- Where possible, the period for which the personal data will be **stored** or, if this information is not known, the criteria used to determine this **period**
- The data subject's **right to request from the controller the rectification or deletion of personal data or a restriction on the processing of his or her personal data and to object to such processing**
- The **right to lodge a complaint** with a supervisory authority.
- Where the personal data are not collected from the data subject, any available information as to their **source**
- The **existence of automated decision-making**, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
- The **appropriate safeguards** taken by the controller regarding transfers of personal data to third countries
- **Regulated professions** (e.g. doctors, lawyers, etc.) must ensure that access to personal data in the electronic mail system complies with any professional secrecy codes by which they are bound

The above information must be provided **free of charge**. If the individual requests additional copies, a reasonable administrative fee may be charged. If possible and feasible considered the circumstance and costs, it is recommended to provide **remote access to a secure system** allowing the individual to directly access his or her personal data.

If you process a **large quantity of information** about the individual, you can request that the individual specifies the information or processing activities to which his or her request relates.

If you process the personal data **electronically**, you should also, if reasonably possible, allow for individuals to request their access electronically. If the access request is submitted
to you by electronic means, you must provide the information in a commonly used electronic form, unless the individual requests otherwise.

If the access request would adversely affect your rights or the rights of a third party, you can refuse to provide certain information (such as trade secrets or information of other persons that is private).

3) Right to request rectification
   a. in a nutshell

Individuals whose personal data you process are entitled to have their personal data corrected if it is inaccurate.

b. more information

Personal data of individuals may be erroneous or outdated.

Besides your own obligation as a business to keep the personal data accurate (your “accuracy” obligation), the individuals whose data you process, are entitled to demand that you correct their personal data.

The rectification of inaccurate personal data concerning an individual, must be done without undue delay upon the individual’s request.

Depending on the purposes of the processing, the individual also has the right to have incomplete personal data completed.

4) Right to request erasure or deletion of data – the right to be forgotten
   a. in a nutshell
Under some circumstances individuals whose personal data you process, have the right to have their personal data erased or deleted.

b. more information

You have to erase personal data of individuals upon their request if:

- you do not need the personal data any longer for the purpose for which it was originally collected or processed
- the consent upon which your processing is based, is withdrawn
- an individual objects to processing by you of his/her personal data, when you rely on your legitimate interest for such processing and you cannot invoke an overriding legitimate interest to continue this processing
- the request relates to personal data processed for direct marketing purposes and the individual objects to such processing
- you are processing the personal data unlawfully
- you have to erase it to comply with a legal obligation
- you process the personal data to offer information society services to a child.

If you have to delete the personal data but you already made it public, then you should take all “reasonable steps” to inform the other parties which are processing the personal data that, the personal data, any links to, and copies or replications of those personal data, must be erased. What “reasonable steps” must be undertaken, needs to be evaluated taking account of the available technology and the cost of implementation.

Exception: personal data must not be erased (and third parties must not be informed), if and to the extent that the processing of the personal data is necessary:

- to exercise the right of freedom of speech and information
- to comply with a legal obligation under EU or Member State law to which the controller is subject or to perform a task carried out in the public interest or in the exercise of official authority vested in the controller
- for reasons of public health;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the provisions of the GDPR insofar as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of the processing; or
5) Right to impose a restriction on processing

a. in a nutshell

Under certain circumstances, individuals whose personal data you process, have the right to ask you to stop using their personal data, without deleting it.

b. more information
Individuals can request that, even though you can keep storing their personal data, you no longer use it.

In most cases, such a request will relate to a situation under which a person wants to maintain the proof that you process his or her data, but is of the opinion that you are not allowed to process it.

(a) An individual can demand the “restriction of the processing” of his or her data in the following circumstances:

(i) The individual challenges the accuracy of the personal data. The processing has to be restricted for a period enabling you to verify the accuracy of the personal data.

(ii) the processing is unlawful and the individual requests the restriction of their use, instead of the erasure of the personal data.

(iii) you no longer need the personal data for the purposes of the processing, but the individual requires the personal data for the establishment, exercise or defence of legal claims.

(iv) the individual objects to processing but you want to verify if you have legitimate grounds to keep processing that override the right of the individual for not having his/her personal data processed. Pending the verification of such legitimate interest, the processing of such personal data must be restricted.

(b) If the processing of specific personal data is restricted, you can only process it in the following ways:

(i) storing the personal data

(ii) processing for the establishment, exercise or defence of legal claims

(iii) processing for the protection of the rights of another natural or legal person

(iv) processing for reasons of important public interest of the European Union or of a member state of the EU

(v) other processing is only allowed with the individual’s consent

(c) Clearly indicate in the system that the processing of the personal data in question is restricted. Some methods to restrict processing are:
(i) making the selected data unavailable to users
(ii) removing published data from a website
(iii) transferring the selected data to another processing system
(iv) marking/tagging the data in a way that avoid that it’s being used (for instance in mailing lists which checks the tags before using the data) or moving the data to a “do-not-use”-mailing list
(v) etc.

If you lift the restriction of the processing (and start to process it (again)), you must inform the individual thereof before the restriction of processing is lifted.

6) Right to data portability

a. in a nutshell

Customers and individuals whose personal data you process in an automated way, based on their consent or an agreement with them, are allowed to obtain a structured digital copy of the data they provided to you, to allow them to provide this data to another service provider (competitor) and have the third party use the data to provide its services or products.

b. more information

The purpose of the right to data portability is to allow (mainly) customers whose personal data you process to easily switch to your competitors, while being able to keep using the data they have provided to you.

(a) Who is allowed to exercise the right to data portability?

Any individual whose personal data you process by automated means, based on:
(i) an agreement, i.e. your customers and clients
(ii) consent

(b) What data do you have to provide to the individual?
The personal data that the individual has provided you with, this means:

(i) all the data the individual has knowingly and actively provided to you, such as his/her name, address, age, etc. provided through forms, through communication, by allowing you to obtain certain information at other instances, etc.

(ii) all the data the individual had indirectly provided to you by using your services or devices, such as (if you collect this data) his/her purchase history, usage history, location data, etc. This second part only relates to the raw data, not the personal data you have inferred or derived from the data provided by the individual, such as a customer profile or an internal credit rating.

By providing such data, you may not adversely affect the rights and freedoms of third parties. This means that you must take care that you, for example, do not violate the privacy of other persons, by providing the individual and especially the other company with the personal data. Or infringe third party’s intellectual property rights by doing so. In this case, you should find a way that complies to the greatest extent with both rights (i.e. transferring the data but obfuscating or leaving out the data that infringes third party rights).

(c) How do you have to provide the data?

You have to provide the data in a structured, commonly used and machine-readable format.

If technically feasible, the individual can request that the you directly transfer his/her data from your system to the system of your competitor.

7) Right to object to the processing

a. in a nutshell

In general, individuals have the right to object against the processing of their personal data,
when you are doing so based on legitimate interest or public interest or for the purpose of
direct marketing. You must inform individuals whose data you process of this right.

b. more information

(a) Individuals have the right to object against the processing of their personal data,
    based on grounds relating to his or her particular situation, if:

    (i) the processing is based on:

        1. your legitimate interest,
        2. public interest,

        including profiling based on these grounds.

        You do not have to stop processing in these cases if you demonstrate to
        have compelling legitimate grounds to continue processing which override
        the interests of the individual or for the establishment, exercise or defence
        of legal claims.

    (ii) the processing relates to direct marketing, including profiling in relation to
         direct marketing

    (iii) the purpose of the processing is scientific or historical research or has
         statistical purposes, unless the processing is necessary for the
         performance of a task carried out for reasons of public interest.

(b) Individuals whose personal data you process must be informed of this right:

    (i) Information must be provided at the latest at the time of your first
        communication with the individual.

    (ii) This information must be

        1. explicitly brought to the attention of the individual
        2. presented clearly
        3. presented separately from any other information

(c) If you provide online services or send e-mails to these individuals, they must be
8) Right not to be subject to automated individual-decision making (including profiling)

a. in a nutshell

Individuals are entitled to demand that decisions that affect them, are made (at least in the end) by humans.

b. more information

(a) Individuals have the right not to be subject to decisions based solely on automated processing, including profiling, if such decision produces legal effects concerning them or similarly significantly affects them.

(b) This right does not apply if the automated decision:

(i) is necessary to enter into or perform a contract between you and the individual. For example, a bank will still be allowed to refuse you a loan if the computer says that you are not eligible.

(ii) is authorised by the law applicable to you and such law lays down suitable measures to safeguard the individual's rights, freedoms and legitimate interests; or

(iii) is based on the individual’s express consent.

(c) If the exceptions (i) or (iii) above apply and you are allowed to make automated decisions with legal effect, you must:

(i) implement suitable measures to safeguard the individual's rights and freedoms and legitimate interests

(ii) at least provide the right for the individual to obtain human intervention from your part, to express his or her point of view and to contest the
(d) Automated decisions cannot be based on special categories of personal data, unless:
(i) explicit consent was provided by the individual,
OR
(ii) processing is necessary for reasons of substantial public interest,
AND
(iii) suitable measures or in place to protect the individual’s interests.

9) Individuals’ rights under the GDPR

a. in a nutshell

When an individual exercises his rights under the GDPR, you must generally satisfy this request within 1 month.

b. more information

(a) Response time

(i) Within one month from receipt of the request of an individual you must:
1. either comply with the request
2. either inform the individual that the period is extended
3. either inform the individual that his/her request is refused

(ii) Extension of the period

(iii) The one-month period may be extended by two additional months, if such extension is justified by the complexity and number of requests.
(b) Refusing a request

If a request is **unjustified**, you must inform the individual that you will not comply with it, providing the reasons for not taking action and informing the individual that he/she is entitled to lodge a complaint with the supervisory authority and seek judicial redress.

(c) Costs? Can you charge for satisfying the individual’s request?

Communications with an individual and actions taken regarding the individual’s rights shall be **free of charge**.

If an individual submits manifestly unfounded or excessive requests (for example, repeated requests) you can either **charge a reasonable fee** or **refuse to act on a request**. It will be up to you to be able to prove that a request was manifestly unfounded or excessive.

(d) How to provide the requested information to an individual?

If the request is sent to you by electronic means, you should provide the answer and the requested information by electronic means where possible, except if the data subject requests otherwise.

(e) Keep in mind that the above described rights of individuals under the GDPR are not absolute. Some rights can only be exercised if particular conditions are met or under specific restrictions.

c. time for action [pop-up window]

Put in place appropriate procedures to respond to requests of data subjects. The following factors should be considered: contact person for data protection requests, clear internal allocation of responsibilities, standard letters for refusal to act/extension.
Work closely with IT. It is important that your IT systems ensure compliance with the data subjects’ rights (including the possibility to erase data)
Specific processing situations

The purpose of this section is to address common practical concerns of micro-enterprises and to grant swift access to these topics by including them in the list under the menu button. This way, companies looking for an answer to one of these specific issues, will be able to navigate there directly and efficiently from anywhere within SMOOK.

The following subsections on specific processing situations will also be available to print or download as single factsheets (e.g. in pdf.).

Customers’ personal data

1. In a nutshell

Your customers provide their personal data to you for one or more specific purposes.

This means that you cannot use this personal data for anything else (purpose limitation).

To a certain extent, you are however allowed to use your customers personal data to market products similar to the one they purchased from you. To be allowed to do this, you must however specifically make sure(1) that they are offered the possibility to refuse that their data is used for such marketing (opt-out) and (2) that they can easily unsubscribe from further receiving such marketing at any moments.

All the general requirements of course also apply, such as informing your customers on how you will process their personal data through your privacy policy.

2. More information

(a) Limited use of personal data [Read more]

Under the GDPR you can only use personal data for the purpose for which it was provided to you (purpose limitation) and you cannot collect more information than required for such purpose (data minimisation).
This means in practice that, you cannot require your customers to communicate, for example, the following information if you do not strictly need this information to sell them your product or deliver your service:

(i) Date of birth: if you want to obtain this to be able to send your customer a birthday card, than you should make this field optional (not mandatory) and explain why you request this information in so called meta-information (“providing your data of birth allows us to send you a card and/or promotion on your birthday”).

(ii) Gender: we understand that it is useful to know the gender of your customers to be able to know how to address them and maybe to be able to profile them. You cannot make this field mandatory however. You can request the information adding in the meta-information “By choosing your gender, we know how to address you and we may be able, if allowed, to better define interesting products and opportunities for you”.

(iii) Names of their children and/or significant other,

(iv) Etc.

(b) Sending marketing to existing customers and clients [Read more]

You are allowed to send marketing to your existing customers, relying on your legitimate interest.

This is called the “soft opt-in” for existing customers.

You can only do this if the following conditions are met:

(i) the customer must be given, the possibility to oppose against receiving such marketing, at the time that you receive their personal information

(ii) the customer must be given the opportunity to oppose further receiving marketing from you, every time they receive marketing communication. In practice this is solved by adding an “unsubscribe” button to every marketing email.

(iii) the marketing must related to products or services similar or related to the
products bought by such customer. For example, if you have a bakery you can send information about new products in the bakery to existing customers. If, besides the bakery, you also own a butcher’s shop that is not part of the same shop, than you cannot use data obtained from customers of the bakery, to send them information about your butcher’s shop.

Furthermore, of course, the fact that you are marketing your products to these customers, must be mentioned in your privacy policy.

(c) General obligations with regards to personal data  [Read more]

In addition to the specific requirements above, all the other general requirements with regards to such processing also apply, such as duly informing your clients, protecting and securing their personal data, respecting their rights, etc.

(d) Processing personal data on behalf of your customers or clients  [Read more]

If your customers provide personal data to you that they are processing and which you need to process on their behalf, you become a data processor.

This means that you will have to enter into a data processing agreement with them and that you can only use this data to perform your services. Follow the links for more information.

(e) Legal bases to process your customers’ or clients’ personal data  [Read more]

In general, you will process your customers personal data based on the following legal grounds:

(i) Contractual obligation: if you need to process their personal data to be able to perform your obligations. For example, if you need to deliver something to a customer, you need their name and address to be able to do so.
(ii) **Legal obligation**: if you are required by law to process specific information. For example, if your customer is subject to VAT, you’ll need to process their VAT-number by law.

(iii) **Legitimate interest**: if you have a legitimate interest to process some personal data of your customer, that overrides the interest of your customer not to have its personal data processed. This applies, for example, to the processing to send marketing to your existing customers and to the processing of contact details of employees of your customer.

(iv) **Consent**: if you need to rely on consent to be allowed to process personal data of your customer. You will need consent if, for example, you want to send your customers personalized information (marketing) or if you want to send marketing that is not covered by the soft opt-in described above.

3. **Time for action** [pop-up window]

Make sure that:

- you don’t use personal data of (contact persons at) your customers in other ways than allowed,
- you inform your customers about the ways you process their data,
- you use the correct legal bases to process your customer’s personal data,
- that your privacy policy contains the right mentions if you are using your customer’s personal data for marketing purposes,
- a data processing agreement is in place when you process personal data on behalf of your customers.

**Suppliers’ personal data**

1. **In a nutshell?**

   Personal data from (contact persons at) your suppliers can only be used within the context of your agreement and relationship with them.
You will of course also need to use and store some of this information for tax and other administrative purposes.

2. **More information**

(a) **General** [Read more]

In the same way as you cannot use personal data from customers or clients for any purpose, you cannot use personal data relating to suppliers for other purposes than the purposes for which you obtained these data (purpose limitation).

When you process personal data of contact persons (employees or other) of your supplier, your legal basis to do so is “legitimate interest”, because you do not have a direct contract with these employees.

In addition to the specific requirements above, all the other general requirements with regards to such processing also apply, such as duly informing your suppliers about your privacy policy, protecting and securing their personal data, respecting their rights, etc.

(b) **Legal bases to process your suppliers’ personal data** [Read more]

In general, you will process your suppliers’ personal data based on the following legal grounds:

(i) **Contractual obligation**: if you need to process their personal data to be able to perform your obligations. For example, if you need to provide access to your supplier, you need their name to be able to do so.

(ii) **Legal obligation**: if you are required by law to process specific information. For example, if you are subject to VAT, you’ll need to process their VAT-number by law.

(iii) **Legitimate interest**: if you have a legitimate interest to process some personal data of your supplier, that overrides the interest of your supplier not to have its personal data processed. This applies, for example, to the
processing of contact details of employees of your supplier.

(iv) Consent: if you need to rely on consent to be allowed to process personal data of your customer. You will need consent if, for example, you want to send marketing material to your suppliers.

3. **Time for action** [pop-up window]

Make sure that:

- you don’t use personal data of (contact persons at) your suppliers in other ways than allowed,
- you use the correct legal bases to process your customer’s personal data,
- you inform your suppliers about the ways you process their data.

**Data protection in an employment context**

1. **In a nutshell?**

If you have employees, your use of their personal data is also governed by the GDPR, besides any national provisions that apply to your employer-employee relationship.

This means that you cannot just record or monitor your employees or obtain information about them from public sources or third parties, if this does not happen in compliance with the GDPR.

A particularity with employees is furthermore that it is very difficult to rely on their “consent” to process their information, because you as an employer are in a hierarchical position towards your employees. Consequently, most consents that they would give you, would not be “free” consents and therefore cannot be considered as a valid consent for you to process their personal data.

The other way round, you must ensure that your employees and staff:
(a) deal safely with ICT and personal data,

(b) understand the importance of data protection.

These reciprocal rights and obligations of your employees are laid down in the ICT Policy, the Data Policy and the Employee Privacy Policy.

These policies inform and teach your employees about the importance of data protection and the points of attention they need to apply when using your ICT infrastructure and/or handling personal data and about how their own personal data is processed.

Furthermore, you also have an obligation to make sure your employees are aware of the importance of privacy and data protection, by raising awareness about this subject, for example by organizing trainings and information campaigns.

2. More information

(a) National law always applies [Read more]

When dealing with employees you should always take into account that employment law is mainly governed by national law. Therefore, you will have to apply the principles of the GDPR in combination with the applicable national law provisions.

(b) Rules and policies [Read more]

Essentially, the rights and obligations will be governed by the following policies:

(i) ICT Policy, in which you describe how the employees have to use and are allowed your ICT infrastructure (including the devices and software) and how they can be monitored while using these.

(ii) Data Policy, in which you describe how your employees should handle personal data

(iii) Employee Privacy Policy, which is in essence a regular privacy policy, adapted to your relationship with your employees.
(iv) Camera Surveillance Policy

These documents do not have to be separate documents and can all be part of one or more broader documents.

For these documents to be binding, it is most likely required under your national employment law that your work rules and/or employment contracts are amended accordingly.

(c) No consent [Read more]

You should avoid to rely on your employees’ consent to process their personal data.

Your employees are supposed to be your subordinates, are considered to be in a weaker bargaining position than you as their employer and are therefore considered not to be able to refuse their consent. Most consents provided by an employee will therefore not be considered as “free” consents and will therefore be void.

The only situation in which you, as an employer, can rely on your employees’ consent, is when the consent relates to a clearly minor and unimportant matter, under which the employee cannot fear in any way that refusing their consent may be held against them later on.

(d) Raising awareness [Read more]

As an employer, it is your duty to ensure and prove (because of your accountability obligation) that you have duly raised awareness among your employees about the importance of data protection and privacy.

Therefore, you should not only organize trainings and information campaigns, but also make sure that you can prove that these happened.
(e) Job applicants [Read more]

You must also inform job applicants about how and why you will process their personal data.

These job applicants do not have access to your “employee privacy policy” so ideally you include the provisions related to job applicants in your public privacy policy.

Note that you:

(i) cannot retain information about applicants eternally (data minimisation and storage limitation), generally a maximum retention period of 2 years appears to be acceptable, except if specific circumstance justify a longer retention period or if you obtain consent to retain this personal data for a longer period,

(ii) that you can only request information from them that is relevant for the job (data minimisation) and allowed by law. If you want to obtain sensitive information of your applicants, such as an extract of their criminal record, you will in many EU countries only be allowed to do so if you have a legal obligation or entitlement to request this information,

(iii) can only use public sources (such as social media posts and profiles) to evaluate the candidate, if the use of such sources is mentioned in your privacy policy,

(iv) should add a notice under each job posting in which you (very) briefly describe that/how you will process the applicants personal data and refer to your privacy policy for further information.

(f) Legal bases to process your employees’ personal data [Read more]

In general, you will process your employees’ personal data based on the following legal grounds:

(i) Contractual obligation: if you need to process their personal data to be able
to perform your obligations. For example, you need to know their name and address to be able to enter into an employment contract with them.

(ii) **Legal obligation**: if you are required by law to process specific information. For example, in many countries you may be required by law to process the employee’s social security number and information about their family, for example to communicate with the social security service.

(iii) **Legitimate interest**: if you have a legitimate interest to process some personal data of your employee of job candidate, that overrides the interest of your employee/candidate not to have its personal data processed. This applies, for example, when you access public information about applicants.

(iv) **Consent**: if you need to rely on consent to be allowed to process personal data of your employee. As described above, it should be avoided as much as possible to process personal data of an employee or of a job applicant based on their consent.

(g) How can you ensure that your employees process personal data, and make use of your ICT environment, in a secure way? [Read more]

In this blog post on the SMOOTH website, you can find a number of practical tips and guidelines on how you can organize your ICT environment in a secure way.

3. **Time for action** [pop-up window]

Verify if you comply with the requirements above and implement the described policies.

Make sure to also verify **national legislation**.

Camera surveillance

1. **In a nutshell?**
When you use surveillance cameras to safeguard your buildings and/or company, you must also take the GDPR into account, besides any national provisions that may apply to different situations in which you can use surveillance cameras.

By filming locations where people may pass by, you are gathering personal information such as their images and their behaviour. If smart cameras are used that allow, for example, facial recognition or license plate recognition, sensitive information such as biometric information is also processed.

2. **More information**

(a) **Check national law**

Note that the use of (surveillance) cameras will first and foremost be governed by national law.

Your national law may prohibit the use of specific or all cameras in all or some circumstance (for example when continuously filming public places), may impose specific requirements (for example in an employment context), may require that the used surveillance camera’s are notified to and/or registered with the government, may require that the police has access to the images upon simple demand, may require that a specific pictogram is displayed to inform persons who may be filmed, etc.

(b) **From a GDPR point-of-view the following specific requirements apply**

(i) The public/employees must be informed/notified of the video surveillance in a clear and effective way.

(ii) Obligations to employees must be fulfilled (e.g. information provided and provisions included in the company’s privacy policy and work rules).

(iii) The company must comply with certain obligations relating to the processing, access to and storage of the images.

(iv) The company must make sure to add this processing in its record of processing activities and in its (public) privacy policy.
(c) Informing/notifying the public

Most countries require the use of a specific pictogram at the entrance of a place where camera surveillance is organized.

For example, in Belgium, the following pictogram must be placed, on which specific information must be mentioned:

In general, the pictogram will have specific requirements with regard to the size, the material, the visibility, the information mentioned on the pictogram, etc.

From a GDPR point of view, any such notification must make it sufficiently clear to the persons being filmed:

(i) Who is responsible for the surveillance camera
(ii) The website where the applicable privacy policy (with more information about the video surveillance) can be consulted.

(d) Obligations to employees

(i) When employees may be filmed, specific requirements under national law will most likely apply, which may impose specific limitations and requirements, specific information obligations towards employees and specific procedures to be followed before the surveillance cameras can be used.

(ii) This information must also be included in the company’s employee privacy policy.

(e) Obligations relating to the processing, access to and storage of images

Depending on your national legislation, specific obligations may apply, such as:

(i) Surveillance cameras directed at an entrance door must be oriented in such a way that the (indirect) recording of public space is kept to a strict minimum.
(ii) Real-time viewing of the images of surveillance cameras is only allowed to be able to establish criminal acts at the time of the act. It is also allowed to show a publicly visible screen, on which the recorded images can be viewed in real time.

(iii) Images may be recorded only to gather evidence of a nuisance, criminal behaviour or acts that cause damage and to identify the perpetrators of such acts, the witnesses thereto or the victims thereof.

(iv) Footage may be stored for a maximum period of one month, unless it is established that it contains images related to a crime.

(v) Persons may only be filmed after the required notification has been made and the pictograms affixed. Entering a room where a clearly visible pictogram is displayed is considered implied consent to be filmed.

(vi) The right to access and search the recorded images must be limited and a record kept of these actions.

(vii) Persons who have access to the images must be bound by a duty of confidentiality and discretion.

(viii) Images may not be recorded that violate the right to privacy of individuals or for the purpose of gathering information about philosophical, religious or political convictions, trade union membership, ethnic or socio-economic background, sexual orientation or the health of individuals.

(ix) All persons filmed have the right to view the video footage in which they appear, provided they can provide sufficient details in order to locate the images in question.

(x) Etc.

In addition to such specific obligations, the obligations laid down in the privacy legislation and the GDPR also apply, taking into account the sensitive nature of video surveillance.

(f) **A record** [Read more]

(i) Pursuant to the GDPR, a record of processing activities must be kept for the processing of personal data, including video surveillance.

(ii) National law may require that an additional record is established, in which specific information about the video surveillance is registered, for example:

1. an indication of the type of place that is under surveillance;
2. a technical description of the surveillance cameras as well as, for fixed cameras, their location, where applicable indicated on a map;

3. for temporary or mobile surveillance cameras, a description of the areas under surveillance by the cameras and the time periods during which the cameras are in use;

4. the means of providing information about the processing;

5. the place where the images are processed; and

6. whether viewing in real time is organised or not and, where applicable, the manner in which it is organised.

(g) Criminal sanctions [Read more]

(i) National legislation may impose criminal sanctions on the infringement of the video surveillance legislation.

3. Time for action [pop-up window]

Verify if your surveillance cameras comply with national law, if all the required policies and notifications are in place and if the persons concerned have been duly informed.

Direct marketing

What is direct marketing?

Direct marketing is an advertising strategy that is deployed by many companies. It allows you to directly target the promotion of your products or services, in order to trigger an action (e.g. to visit a website or to buy something) in a selected group of consumers that have been identified as potential buyers. Electronic direct marketing frequently takes the form of emails, texts, picture messages, video messages, voicemails, direct messages via social media or any similar message stored electronically.

By targeting end-users with electronic direct marketing communications, companies are processing personal data as defined in the GDPR. However, the rules governing direct marketing
communications are not only to be found in the GDPR, additionally the ePrivacy Directive (to be replaced by the ePrivacy Regulation) imposes specific rules in case of direct marketing communications.

**How to justify direct marketing?**

In the context of direct marketing, **consent is key!** Under the ePrivacy legislation, you need to obtain consent from the targeted individual **before** sending direct marketing communications in electronic form — marketing texts, emails or calls. The ePrivacy legislation prevails over the GDPR and therefore limits the possibility for controllers to rely on another legal basis in the list of article 6 GDPR. For the interpretation of consent the legislator has pointed to the strict interpretation to be found in the GDPR. [LINK TO CONSENT SECTION] This means that consent needs to be:

- **a) Freely given** – You should provide the individuals concerned with a genuine choice to consent to marketing. Coercing or unduly incentivizing people into consenting – for example by tying negative consequences to the refusal of consent – is thus prohibited.

  **Example:**
  Upon request, a small building company provides potential clients with brochures setting out information about how the company works, the materials it works with etc. The request needs to be made by filling in an online form. Through this online form, the company also asks for the persons’ home address and email address, not only to be able to deliver the brochure but also to send them marketing messages about upcoming projects and events in the future. The company only allows the requesting individuals to opt-out of receiving marketing messages in case they untick three boxes covering marketing emails, post and text messages. However, unticking all three boxes results in the fact that the brochure will not be sent. This practice is not GDPR compliant.

- **b) Specific** – Consent needs to be specifically given for your company and the type of marketing communication (e.g. email, text message...) you are using. Consent should not be bundled up as a condition of service unless it is necessary for that service.

- **c) Informed** – You should inform the individuals concerned in a clear and prominent way to ensure that they fully understand that a certain action will be taken as consent and what exactly they are consenting to. In practice, you should avoid giving information in a hidden (due to placement or size) manner or by way of lengthy, complicated privacy policies that are difficult to understand.

- **d) Unambiguous indication of wishes expressed by a statement or a clear affirmative action** – Consent should be provided by way of a clear positive indication of agreement, such as clicking an icon, subscribing to a service, sending an email or making a phone call, but also oral confirmation is possible. In other words, consent needs to take the form of an ‘**opt-in**’, ruling out the use of pre-ticked ticked opt-in boxes, as well as opt-out boxes and any other form of consent derived from silence, inactivity or default settings.
Additional obligations when relying on 'direct marketing':

Essential here is that, through the accountability principle, the GDPR requires you to be able to demonstrate that you have obtained consent for direct marketing. This means that you must keep evidence of who, when, how, and what you told people in the context of requesting consent. Also, very important in this regard is that the individuals concerned have the right to withdraw their consent at any time. Moreover, you need to make sure they are able to withdraw consent equally as easy compared to the granting of consent.

When is no consent needed?

Important to know is that under certain conditions you are still allowed to process contact details for direct marketing purposes when you did not obtain consent, however, only in cases where the exemption to the ‘opt-in consent rule’ – referred to as the ‘soft opt-in’ – is applicable. The exemption exists when three conditions are met:

1. Contact details must have been obtained in the context of a sale of a product or a service, or through pre-contractual negotiations. Solely browsing a company’s website does not suffice. On the other hand, requesting a company to order an out-of-stock product or adding it to a basket would be sufficient to trigger the application of the exemption. It is up to you – as a controller – to justify direct marketing in this context and to demonstrate compliance.

2. Data collected in this way can only be used for direct marketing of your own similar products or services. This implies that you can only benefit from the exemption if you are the company that initially collected the contact data, not if you have bought-in marketing lists. In this case, you should not lose sight of the customer’s reasonable expectations.

3. Finally, the targeted individuals should be clearly and distinctly given the opportunity to opt out, easy and free of charge, to this kind of use of their contact details. The option to object has to be presented at the time of the collection of the contact details and at every time you send them a marketing communications. Generally this happens through a link at the bottom of the email. In practice this means that, consumers can be presented with both an opt-in for general marketing communications and an opt-out for marketing communications falling under the ‘soft opt-in exemption’.

While the ePrivacy legislation provides an exemption to the necessity for direct marketing, it does not relieve you from the obligation to ground your processing on one of the legal bases listed in
article 6 GDPR [LINK]. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. This means that, when invoking the soft opt-in, you still have to perform the legitimate interest balancing exercise [LINK].

! With regard to personal data bases that pre-existed the GDPR, it is not necessary for individuals to give consent again if the manner in which consent has been given complies with the conditions of the GDPR!

**To do:** [pop-up window]

- Ask for consent when you engage in direct marketing
- Check whether your consent requests are clear and prominent
- Be transparent regarding who is sending the marketing messages
- As individuals have the right to withdraw consent at any time, ensure that all direct marketing holds information on this right and provides the possibility to withdraw consent (e.g. unsubscribe button)
- Make sure you keep clear records of what an individual has consented to, as well as when and how consent was obtained. This is necessary to demonstrate GDPR-compliance in the event of a complaint.

**Best practice:**
The clearest way to obtain consent is to make us of an ‘opt-in box’ that individuals concerned can tick in case they wish to receive direct marketing through specific channels (e.g. email, text messages,...).

*Example: Tick the boxes if you would like to receive information about our products and any special offers by post 0 / by email 0 / by telephone 0 / by text message 0 / by recorded call 0*

**Health data**

Health data are personal data concerning the physical or mental health of a person, including the provision of health care services, which reveal information about a person’s health status in the past, present or future. This category of data is marked as a special category of personal data under the GDPR, because of its ‘sensitive’ nature: unlawful processing of health data may cause serious consequences to a person’s rights and freedoms. Therefore, health-related data are subject to a stricter data processing regime than non-sensitive data: you will not always be allowed to process data revealing information on the health status of persons.
What/Where is health data?  

- Medical data (e.g. doctor referrals and prescriptions, medical examination reports, laboratory tests, radiographs)
- Medical certificates (e.g. documents certifying medical suitability for work)
- (Electronic) health records
- Administrative and financial data relating to health (e.g. medical appointments scheduling, invoices for healthcare service provision, indication of the number of days of sick leave, sick leave management, forms concerning sick leave or the reimbursement of medical expenses)
- Wearables (e.g. smart watches)
- Medical apps and more general apps (e.g. fitness or running apps)

Can I process health data?

In principle, the processing of health data – like any other special category of personal data – is prohibited. But even though the processing of health data is deemed to be more risky than processing regular personal data, processing health data can be necessary in various aspects of our life. Therefore, the GDPR foresees a number of exceptions to the prohibition. First of all, health data can only be processed when there is a lawful basis to do so under article 6(1). (LINK TO SECTION ON LAWFUL BASIS) Additionally, one of the situations mentioned in article 9(2) needs to be present (LINK TO SECTION ON SPECIFIC CATEGORIES OF PERSONAL DATA UNDER CONSENT). The most relevant exceptions from a small company’s point of view are:

1. **Explicit consent**: [see section on specific categories of personal data][Read more]

   Explicit consent will **not** be a valid ground for the processing of health data in situations where medical treatment is necessary and the patient does not have the possibility to refuse the processing of his or her health data.

   Explicit consent **could** be a valid legal basis to process health data for medical research or in the context of insurance companies.

2. **Employment, social security and social protection law** [Read more]

   If your company employs staff members you are almost inevitably processing health data about these employees because in light of employment, social security and social protection law certain obligations and rights exist that require the processing of health data. For instance, employers are allowed to process health data of their employees (or their family members) for the purpose of sick leave management or to reimburse medical aids. On the other hand, processing health data within the framework of a pre-recruitment medical examination or an annual medical visit will not always be allowed under the GDPR, only if a legal obligation or right in this regard exists in EU or national law or in a collective agreement.
3. Individual health care purposes [Read more]

Medical treatment is inextricably linked with the processing of health data. Health data can be processed in case it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. However, processing in these situations is only allowed where carried out by healthcare professional subject to an obligation of professional secrecy, or by another person subject to an equivalent obligation.

| If your company processes data concerning health, you will bear an extra burden as these data require a higher standard of protection than non-sensitive personal data. In each situation, appropriate safeguards need to be in place! |

**Time for action** [pop-up window]

- Assess whether there is a way to avoid the processing of health data.
  - Is the processing of health data necessary to achieve its underlying aim?
  - Is the aim pursued by the processing of health data proportionate with regard to the restriction of the concerned person’s rights and freedoms?

- Check whether EU or national law set additional requirements or prohibitions for health data processing.

- Provide all the necessary information to the individual whose health data your company is going to process in a way that is understandable to the person.

- Implement sufficient technical and organisational safeguards (e.g. pseudonymisation, separate storage of health data, restriction on the number of persons that have access to health data) to ensure that health data is adequately protected and is not subject to unauthorised disclosure or other unlawful processing activity.

- Don’t forget to take into account the principles of personal data processing [link to section on data processing principles].

- In case of doubts concerning the permissibility of the planned processing activities or the necessary safeguards, consult your DPO (if your company has one) or your DPA [link to ‘How to contact my DPA?’].

**Websites: Cookies and similar technologies**

1. **In a nutshell**
Most websites make use of specific information technologies that collect and process information related to the webpage or to the visitor. These tools can be referred to as cookies or other tracking technologies and serve as a memory tool, able to recognize users’ online behaviour and remember their actions.

Since usage of these information technology tools could be privacy-intrusive for the website visitor, you will have to take into account a number of consent and information obligations before placing your first cookie: provide clear and understandable information to the individuals concerned, obtain their consent (not always necessary) and refrain from using personal data in a manner that is incompatible with the initial purpose of collection.

2. **More information**

**What are cookies?** [Read more]

Cookies are virtually invisible text files that a website may store on its visitors’ computers or mobile devices at the time they access the website. Cookies allow the website to track, collect, and store any (personal) data that companies request.

Cookies, as such, are a storage medium and are therefore not personal data in themselves. Nevertheless, cookie identifiers can be seen as personal data because personal data can be stored in them. When cookies can identify an individual, they are considered personal data. As ‘personal data’, their processing is subject to the GDPR and needs to be grounded on a legal basis and respect the data protection rules and principles.

There can be different reasons for companies to make use of cookies:

- to improve the performance of functions and services,
- to improve user experience or
- to monitor users’ digital behaviour to serve them targeted advertising.

Below, a list the most common types of cookies:

<table>
<thead>
<tr>
<th>First party cookies</th>
<th>Cookies that are set directly by the website accessed by the user.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third party cookies</td>
<td>Cookies that are set by a domain other than the one the visitor is using.</td>
</tr>
</tbody>
</table>
Session cookies | Cookies that are temporarily placed in the website visitor’s device and that expire at the end of a browser session. These cookies recognise and link the actions of a website visitor during a browsing session.

Persistent cookies | Cookies that are stored on the website visitor’s device for a specified period that is longer than one session. These cookies can recognise the visitor’s device for future website visits and remember its preferences or activities on that website, or even transfer this information to another websites.

**Obligation to obtain consent** [Read more]

Cookies are mainly regulated by the [ePrivacy Directive.](#) Based on this directive, consent from the user for the storage of, or access to, certain types of cookies is required. Consent under ePrivacy Directive should be interpreted in line with the GDPR (freely given, specific, informed, unambiguous and based on an affirmative action). Additionally, in case you make use of any type of tracking devices, you must be able to prove that you have obtained your visitors’ consent.

! Scrolling down or swiping through a website or application cannot be considered to be a valid expression of consent to the use of cookies !

Ask for consent the first time you set cookies, you do not have to repeat it every time the same person visits your website. However, devices may be used by different people so you may want to repeat this process at regular intervals.

**Exemptions from the consent obligation**

Consent is not required for the implementation of all cookies. The ePrivacy Directive provides an exemption for:

- Cookies used for the sole purpose of carrying out the transmission of communication

- Cookies that are strictly necessary to provide a service over the internet that is explicitly requested by the user. The implementation of the cookies needs to be essential to provide the user with the service in question. Cookies that are solely helpful or convenient – or that are also used to achieve other objectives – cannot be considered as strictly necessary cookies and thus can only be stored onto the user’s device based on valid consent.

The following cookies can be exempted from the consent requirement, provided that they are not used for additional purposes:

- User input cookies (session-id), for the duration of a session or persistent cookies limited to a few hours in some cases;

- Authentication cookies used for authentication services, for the duration of a session;
- User centric security cookies used to detect authentication abuses, for a limited persistent duration;
- Multimedia content player session cookies, such as flash player cookies, for the duration of a session;
- Load balancing session cookies, for the duration of a session;
- User-Interface customization persistent cookies, for the duration of a session (or slightly more);
- Third party social plug-in content sharing cookies, for logged in members of a social network if they are not also used for user tracking purposes.

**Information obligation** [Read more]

When you want to make use of cookies or other tracking technologies, you need to provide the user with clear and comprehensive information about this use. The information needs to be provided in a manner that is suitable for the user and before or at the time of requesting consent. This means that you will have to implement a cookie policy on your website, providing all the information that is necessary for users to take an informed decision on whether or not to consent to the use of cookies.

A cookie policy should:

✔ Inform users about the presence of cookies
✔ Inform users about which cookies you use
✔ Inform users about what the cookies are doing and why you are using them (e.g. necessary for website usability, to save preferences for a better user experience, analytics for usage statistics, advertising purposes etc.)
✔ Inform users about the publisher of the cookies? Are the collected data shared with other people?
✔ Get the user’s consent to store a cookie on their device

! Make sure that the language used in the cookie policy, corresponds to the language of the people targeted by the website!

**Good practice** - Use a layered approach in order to keep the cookie policy short and simple: basic information about cookie usage should be contained in the first layer. This first layer should give the user the option to accept or refuse all cookies, or to configure options for the usage of different cookies (opt-out). When choosing the last option, the user should be directed to a more detailed
cookie notice (second layer) with information (name, type of cookie, technical details, specific purpose and retention period) for each (group of) cookies.

**Storage period** [Read more]

A limited storage period should be set for each (type of) cookie. It is also recommended to periodically review the cookies you use because the storage period of cookies or other tracking technologies must be proportionate and limited to what is necessary to achieve the planned purpose. The storage period can also not exceed the period for which valid consent was given.

3. **Time for action** [pop-up window]

- Check what cookies or other tracking technologies your online service already uses or intends to use and identify what information is processed by each cookie
- Confirm the purposes of each cookie and remove cookies you do not need
- Identify strictly necessary cookies, communication cookies and cookies for which consent is required
- Put in place a cookie policy to provide the necessary information concerning your company’s use of cookies and other technologies
- Implement a GDPR-compliant consent mechanism, including the ability to refuse non-essential cookies
- Keep records of users’ consent to implementing cookies for an appropriate period of time
- Ensure compliance with the GDPR where information obtained and processed through cookie storage can be considered as personal data
- Avoid the use of third-party cookies or other tracking technologies as much as possible

**Social media to promote my business**

In today’s digital age, most companies rely on social media to promote their business. They usually have their own ‘page’ or account on one or more social networking websites. Additionally, some companies feature social media plug-ins on their own website, to generate more traffic their way.
Making use of social media brings along certain legal consequences. What exactly this means for your role and responsibilities under data protection law, will be discussed in this section.

**Fan page hosted on social media**

Most likely you are the administrator of a (fan) page for your company on a social networking website. This inevitably brings along processing of personal data. In this context, processing is essentially carried out by the social networking site, placing cookies and processing the information stored in the cookies. By creating such a page, you give the social networking site the opportunity to place cookies on the computers of visitors, from which you benefit by obtaining statistics useful to manage and promote your activities. Regardless of the fact that you often do not have factual or legal influence on the purposes and means of processing, you will be considered to be involved in the production of the statistics through defining the criteria for the statistics and designating the persons whose personal data is to be made use of by the social networking site. The fact that you only receive the statistics in anonymized form and do not have access to the actual personal data concerned, does not take away the fact that you will be considered to have an influence on the processing of personal data for the purpose of producing statistics based on visits to the fan page.

Consequently, as an administrator of a fan page hosted on a social networking site you contribute to the processing of the personal data of your visitors and under the GDPR you will be seen as a **joint controller** – together with the social networking site. This is only the case for those processing activities which consist in the collection by the social networking site of personal data on your page. This results in the shared responsibility to inform visitors of the page about the fact that information of them was collected via cookies.

The existence of joint responsibility does not necessarily imply equal responsibility of you and the social network operator. The level of responsibility must be assessed taking into account all relevant circumstances of the particular case: if your joint processing only relates to the collection of data from visitors of your page and to the processing of this data for statistical purposes (and not to the use of the data by the social networking site for its own analysis and advertising unrelated to your company) you will likely only carry responsibility for these processing activities.

The GDPR specifies that joint controllers need to determine their respective responsibilities under data protection law in a transparent manner. For more information on what this means, see [link to DPA section](#). Following from joint controllership, individuals will be free to choose to turn to your company or the social networking site to obtain full damages. If you are not able to prove that you are not responsible for the event giving rise to the damage, the social networking site is allowed to claim back part of the compensation corresponding to your responsibility for the damage.

**Time for action** [pop-up window]

- As a fan page administrator you will need to conclude a **joint controller agreement** with the hosting social networking site. In this agreement, each party’s responsibilities need to be set out, including visitors’ rights and information obligations. *E.g. Facebook has put in place a joint controller addendum with which you will have to agree in case you would like to create a Facebook page for your company.*
- Comply with the controller obligations in the GDPR: inform visitors about the identity of the joint controllers, the purpose of the processing, the legal basis relied upon, data retention periods and all data processing activities and their rights (e.g. access, rectification, erasure). Also make sure that visitors are able to exercise these rights.

- To the extent possible, put in place measures to ensure adequate protection of your page’s visitors and their personal data.

- Data processed for the purpose of providing targeted advertising will require visitors’ consent.

**Social plugins**

Often companies embed social plugins on their website to obtain certain commercial benefits. Social plugins are buttons – such as a ‘like button’ or a ‘share button’ – which allow visitors to share their experiences on other websites with friends on certain social networking sites. When a visitor consults a website featuring plugins, his or her personal data are transmitted to the social networking site. It allows companies to optimise the publicity for its goods or services by increasing visibility on social media.

If you feature a third-party plugin on your website, you most likely will be a joint data controller together with the social media company concerned in respect of the collection of personal data of the website visitors and the transmission of this data to the social networking site. This is based on the fact that both parties have an economic interest and you jointly determine the means and purposes of the processing of the personal data that were transferred to the social networking site. You will, however, not be a controller with regard to the processing subsequent to the transmission of the data carried out by the social networking site alone, as you do not determine the purposes and means of those operations.

In respect of such operations involving the processing of personal data of visitors to your website, you will also carry a list of responsibilities under the GDPR.

**Time for action**

- At the time of the collection of their personal data, you must provide certain information to your visitors, including for example your identity and the purposes of the processing.

- In case you rely on consent of the individuals concerned, you only are required to obtain prior consent for operations for which you act as a (joint) controller (i.e. the collection and transmission of the data).

- In cases where the processing of personal data is justified by relying on necessity for the purposes of a legitimate interest, the Court finds that each of the (joint) controllers, namely you as the operator of a website and the provider of a social plugin, must pursue a legitimate interest through the collection and transmission of personal data in order for those operations to be justified in that regard. It is not sufficient if only one of the joint
controllers is pursuing a legitimate interest through the collection and transmission of personal data.

A waterproof privacy policy

1. **In a nutshell?**

   Your privacy policy is the instrument through which you inform your (contacts at) existing and potential customers, clients, suppliers, website visitors, prospects, employees and job candidates how you will use and protect their personal data.

   Consequently the privacy policy must be available to these persons for them to be able to acknowledge the policy.

   Ideally, you work with (at least) two different privacy policies:

   - an internal privacy policy, for your employees, internal consultants and anyone who provides services within your company,
   - a public privacy policy, for anyone who has no access to your internal documents, such as suppliers, prospects, customers, job candidates, etc.

   It is of course possible to have more different policies, if your activities would require so.

   Every privacy must contain a large number of mandatory mentions, adapted to the persons whose data you are processing and to the ways you process their data.

   You can find a template privacy policy via this link.

2. **More information**

   (a) The privacy policy must obligatory contain the following information:
(i) the (categories of) **personal data** that you process
(ii) the use you make of that data
(iii) how you **protect** and safeguard that data
(iv) how you collect that data
(v) which **legal basis** you rely to process data
(vi) which third parties receive such data
(vii) the places (countries) where those data are processed
(viii) the **rights which can be exercised by the persons concerned** (e.g. right of access, right of forgetting, right of rectification, etc.)
(ix) who your company is and how it can be reached, including by e-mail
(x) how long data is kept (retention policy)
(xi) the **right of data subjects to file complaints** with the data protection authority
(xii) that you are using **cookies, pixels, or other tracking technologies**
(xiii) if you have a **data protection officer**, how it can be reached

A Privacy Policy is sometimes also called a privacy statement or a privacy notice, but we recommend to use “privacy policy” because the other definitions can also refer to the short informational pieces of text that inform the persons concerned of the existence of a privacy policy and some specific aspects of the intended processing.

(b) Details and readability

Your privacy policy should be sufficiently specific and detailed to allow the persons concerned to actually understand what happens with their data and what they can expect.

On the other hand, the GDPR also prescribes that the information you provide should be “concise” and “legible”.

Therefore, it is recommended to have a so called “layered” privacy policy:
(i) The first “layer” is a very short overview of the principles you apply which allows the persons concerned to establish “in the blink of an eye” what major principles you apply when processing their personal data.

(ii) The second “layer” contains all information. This can be a different document or this additional information can (for example) appear by clicking on a “read more” button under the short description of the first layer.

To enhance readability, it is also strongly recommended to design your policy in a way that

1. it can be easily read. Avoid for example to use a small font and arrange the text in a logic way, that enhances a comfortable readability.

2. to add icons, symbols and/or images to the policy to visually support and show the content of the privacy policy.

(c) Location of and references to your privacy policy

It is not enough to “have” the required privacy policies, it is also required to make sure that the persons concerned are informed of the existence of it before you start processing.

1. The internal privacy policy that applies to your employees will have to be communicated to them in accordance with your local employment law. It may be required that reference is made to such “employee privacy policy” in your work rules and/or employment contracts. You will also need to communicate it to any other inhouse service providers to whom the privacy policy applies.

2. The external/public privacy policy is ideally put on your website, with fixed link referring to it in (at least) both the footer of your website and in your cookie banner.

Furthermore, you will need to refer to your public privacy policy each time you obtain personal data of someone and each time you use such personal data to communicate. This means that you should have a link or url in (for example) all your outgoing emails, below forms
(webforms and paper forms), job announcements, etc.

Finally, it is not sufficient to just refer to the privacy policy. When you obtain personal information of a person, you must also briefly describe what you will do with it.

A form to subscribe to a newsletter can, for example, look like this:

“If you wish to stay updated on similar offers/our product range/receive our newsletter/…, please fill in your personal details below:

- E-mail address (obligatory):
- Gender: man/woman/other/I wish to not give this info
- Name (obligatory):
- Surname (obligatory):
- Company
- Sector
- ...

( ) I wish to receive the name company newsletter / e-mails customized to my profile / information and I therefore give permission to process my data and e-mails automatically.

( ) I give my permission to transfer my data to third commercial partners, which were carefully selected by company, in order to receive additional information, based on my interests.

Send/confirm/subscribe [button]

You can unsubscribe from these e-mails or modify your preferences at any time.

We respect your privacy and do not disclose your data to third parties. For more information, please find our Privacy Policy in this link [insert link].

And the footer of your emails can, for example, look like this:
3. **Time for action** [pop-up window]

Use our [template privacy policy](#) to draft your internal and public privacy policies.

Once you have drafted your privacy policies, you can verify their completeness via our tool SMOOTEXT.

### Consent and children’s data

The GDPR explicitly recognises that children deserve specific protection of their personal data, and introduces additional rights and safeguards for children. SMOOK will share some best practices for companies that process – or might process – children’s personal data.

If you provide information society services (e.g. web shops, video-sharing platforms, social networking sites, search engines etc.) to a child **while relying on consent** as the legal basis for the processing, you need to undertake reasonable efforts to obtain and verify **parental consent** when it concerns users below the age of 16. Reasonable effort should be determined by taking into account existing technology and the circumstances such as resources and level of risk. Depending on the Member State where you operate, a different age limit may apply as Member States are allowed to lower the age limit for parental consent down to 13 years old.

Take note that this rule only applies if the services are offered **directly** to the child, meaning that they either exclusively address children or explicitly focus on them.
Also, it does not mean that you always have to obtain parental consent for users under the chosen age limit. Only if you make your service available to children, and you rely on consent as your lawful basis (e.g. for any non-core processing, cookies or similar technologies or processing of special category data).

**To do:** in case you offer information society services directly to children, go check out your national post-GDPR law to find out up until which age parental consent should be obtained.

**National age limits for parental consent:**

![Diagram showing national age limits for parental consent](https://www.betterinternetforkids.eu/nl/web/portal/practice/awareness/detail?articleId=3017751)

When you do not directly offer content to children, but rather offer services that are likely to be accessed by children (<18 y/o), you will have to take additional measures to protect their best interest.

**Useful link:**

ICO has issued a code on Age appropriate design: a code of practice for online services, which provides practical guidance on how to ensure your online services appropriately safeguard children’s personal data. Following this code will assist you to process children’s data fairly.

The role of the ePrivacy Regulation

1. **In a nutshell**

When processing personal data, two major EU legislative instruments are of potential relevance to your operations: the GDPR and the ePrivacy Directive (currently under revision). As it is important to know which instrument to turn to under which circumstances, you need to be able to distinguish them and their scopes of application.

The goal of the GDPR is to protect fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and to ensure the free movement of personal data within the Union. The goal of the ePrivacy Directive is also to protect fundamental rights and freedoms of the public, but in particular the right to privacy and confidentiality specifically with respect to processing personal data in light of the use of electronic communication networks. Finally, the ePrivacy Directive also aims to ensure the free movement of such data and of electronic communication equipment and services in the Union.

! In other words, the ePrivacy Directive particularises and complements the GDPR regarding the processing of personal data in the electronic communication sector!

2. **More information**

In the event of processing personal data, there are three possible scenarios regarding the (lack of) interplay between both instruments: [Read more]

| The GDPR does not apply, but the ePrivacy Directive potentially does | - When the data that is being processed is not personal data (e.g. company emails that do not hold the name of natural persons or phone numbers of automated customer services of legal persons etc.) |
| - When it concerns processing activities mentioned in the list of article 2(2) and (3) of the GDPR |
| - When the processing activities do not fall under the territorial scope of the GDPR |

| The ePrivacy Directive does | - In general, the ePrivacy directive does not apply, unless: |


| not apply, but the GDPR potentially does | * it concerns an electronic communications service  
* which is offered over an electronic communications network  
* the service and network are publicly available (so not corporate networks that are only accessible to employees for professional purposes)  
* and are offered in the EU  
- Website operators or other businesses do not fall under the scope of the Directive (except when it concerns articles 5(3) (cookie rules) and 13 (direct marketing rules)) |
|---|---|
| The GDPR and the ePrivacy Directive both apply | It is possible for processing activities to fall within the material scope of both legal instruments:  
- In case of the use of cookies which collect personal data  
- In case of direct marketing practices  
- In case providers of electronic communications services process personal data of natural persons using their services and additionally specific rules – e.g. on subscriber directories, itemised billing, calling line identification – apply  
- In case traffic or location data are generated by electronic communications services in case personal data is involved |

For situations in which both legal instruments apply, the GDPR acknowledges that the **ePrivacy Directive should prevail** and that it does not impose additional obligations on natural or legal persons in relation to processing in light of the provision of publicly available electronic communications services in public communication networks in the EU. This is only for situations in which specific obligations exist within the ePrivacy Directive. In other cases, where it does not specify anything, the more general rules of the GDPR will govern the situation.

**What about enforcement?**

National data protection authorities are competent to enforce the GDPR ([Link](#)). The sole fact that part of a processing operation falls within the scope of the ePrivacy directive, does not affect the competence of data protection authorities under the GDPR. However, data protection authorities are not automatically competent in light of ePrivacy. The latter depends on whether the national law of your country designates the data protection authority as competent authority under the ePrivacy Directive. It is only then that the data protection authority has the competence to directly enforce national ePrivacy rules in addition to the GDPR.

3. **Time for action** [pop-up window]
In case you are processing data within the context of providing publicly available electronic communications services in EU public communication networks, do not forget to check first whether you, and how to, comply with the ePrivacy Directive.
WHAT IS SMOOK?

SMOOK is an online interactive handbook for micro-enterprises, providing detailed guidance to help them understand:

- How the General Data Protection Regulation (GDPR) affects their enterprises;
- What actions they must undertake in order to become GDPR-compliant;
- How to navigate through the GDPR regulation.

WHO IS SMOOK FOR?

SMOOK is especially designed for micro-enterprises. Although the content is tailor-made for them, any enterprise can extract GDPR information from this handbook.

Link - SMEs & the GDPR

My Data Protection Authority [pop-up window]

For any questions or advices on your processing activities, you need to turn to the competent data protection authority. This is also the case if you want to request an audit or to file a complaint.

If a data protection impact assessment indicates that your enterprise is engaging in high risk processing, you are obliged to consult the data protection authority prior to the processing of any data.

You will find the name and contact details of all the Data Protection Authorities in the EU and EEA [here].
GDPR compliance toolbox

This section will serve as the central database for all the tools provided throughout the Handbook: Checklists, questionnaires, templates etc.

It will also provide guidance and documents originating from national data protection authorities and the European Data Protection Board. E.g. both the UK’s Information Commissioner’s Office and the Belgian Data Protection Authority have provided models for registering data processing activities, the Commission Nationale de l’Informatique et des Libertés - the data protection authority of France - has provided templates for DPIAs and PIAs, etc.

This makes it easy for readers particularly searching for these tools.
<table>
<thead>
<tr>
<th><strong>GDPR Glossary</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cookies</strong></td>
</tr>
<tr>
<td><strong>Cookie banner</strong></td>
</tr>
<tr>
<td><strong>Cookie notice</strong></td>
</tr>
<tr>
<td><strong>Customers or clients</strong></td>
</tr>
<tr>
<td><strong>Data breach</strong></td>
</tr>
<tr>
<td><strong>Data controller</strong></td>
</tr>
<tr>
<td><strong>Data processor</strong></td>
</tr>
<tr>
<td><strong>Data protection authorities (DPA)</strong></td>
</tr>
<tr>
<td><strong>Data protection impact assessment (DPIA)</strong></td>
</tr>
<tr>
<td><strong>SMOOTH</strong></td>
</tr>
<tr>
<td><strong>Deliverable 2.4</strong></td>
</tr>
<tr>
<td><strong>Handbook and Requirements</strong></td>
</tr>
<tr>
<td><strong>Assessment (final version)</strong></td>
</tr>
</tbody>
</table>

| **Data protection officer (DPO)** | A position within an enterprise where the primary task is to ensure that [personal data](#) of staff, customers, providers or any other individuals is processed in compliance with the GDPR. |
| **Data retention policy** | A policy in which you define how long you will keep each type of data and the length of retention is being justified. |
| **Information society service** | Any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of a service (e.g. commercial websites, social media). |
| **Legal/Lawful basis** | Article 6 of the GDPR exhaustively lists the grounds based on which the processing of personal data could be justified (consent, necessary for a contract or the performance thereof, legal obligation, to protect someone’s vital interests, task in the public interest, legitimate interest). |
| **Legitimate interest assessment** | An assessment of the necessity of your processing, its impact on individuals’ rights and interests and whether the rights and freedoms of individuals override your company's legitimate interests. |
| **Micro-enterprise** | Companies with less than 10 employees and an annual turnover of no more than €2 million. |
| **Personal data** | Any information relating to an identified or identifiable natural person. (An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, |
| Processing | Any operation or set of operations performed on (sets of) personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| Recordkeeping | The obligation to keep records of data processing activities to ensure that enterprises dealing with personal data can be held accountable for keeping personal data safe. |
| Special categories of data | Personal data that needs more protection because it is sensitive (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data and data concerning health, sex life and sexual orientation). |
Test your GDPR and ePrivacy knowledge

1. **What is the main aim of the GDPR?**
   a) Giving citizens back control over their personal data by and to “harmonize” the different national data protection laws across the EU to facilitate the free movement of personal data
   b) To make sure the police cannot process your data without your consent
   c) To restrict online advertising

   **Answer:** a)
   In an increasingly digitized society, the GDPR aims to give citizens back the control over their personal data by providing them with greater protection and rights, as well as to harmonize the 28 different data protection laws across Europe, in order to facilitate the free traffic of personal data in the EU.

   Click here for more information on the reasons behind the GDPR.

2. **Which companies have to comply with the GDPR?**
   a) Only companies who have an establishment in the EU
   b) Companies who are established in the EU and companies who target EU citizens
   c) All companies worldwide

   **Answer:** b)
   Both, companies who are established in the EU and companies who target EU citizens, have to respect the rules in the GDPR.

   Click here for more information on when the GDPR applies.

3. **An American business traveler in Spain orders a product from an online store which is also based in Spain. This traveler is...**
   a) not protected under the GDPR
   b) protected under the GDPR

   **Answer:** b)
   The processing of the traveler’s personal data is undertaken by an enterprise established in the EU,
hence the processing is regulated by the GDPR, regardless if he might have the product delivered in the US.

Click here for more information on when the GDPR applies.

4. **Is data collected before May 2018 subject to the GDPR?**

a) Yes
b) No

Answer: a) Yes, any personal data that you currently are processing is subject to the GDPR, regardless of when they were initially collected.

5. **Which of the following data are not personal data?** (more than one answer is possible)

a) Statistics of the number of visits to a website, tracked via cookies
b) License plates
c) IP addresses
d) The purchase history of a specific customer

Answer: a) Cookies tracking the number of visits to a website (statistics) are not personal data. License plates and IP addresses are personal data because personal data is all data that makes it possible to designate a person uniquely, even if you are not the person who can. Data that relates to an identifiable person is also personal data, hence a purchase history is personal data as long as it is possible to find out who it relates to.

Click here for more information on what is personal data and what is not.

6. **When does an EU company need to comply with the GDPR?**

a) When they are processing personal data
b) Only when they are storing personal data
c) Both
The main criterion triggering GDPR applicability is whether or not a company processes personal data. The term processing is very broad and covers any operation involving personal data: storage, collection, recording, structuring, consulting, usage, transmission...

Click here for more information on what constitutes processing of personal data under the GDPR.

7. When processing personal data...

a) The GDPR requires enterprises to always obtain consent of the person who’s personal data are being processed

b) Consent is only one out of an exhaustive list of lawful bases on which enterprises can rely to justify their processing activities and, hence, is not always necessary

c) Consent is never necessary under the GDPR

Answer: b)

Consent is only one out of an exhaustive list of lawful bases on which enterprises can rely to justify their processing activities (see articles 6 and 9 GDPR) and, hence, is not always necessary. For each processing activity you should always choose a legal basis for processing, depending on which basis is most suitable for the situation.

Click here for more information on how to choose a legal basis.

8. By embedding a Facebook “like button” – a social plug-in – on your website, you become a controller of the data that is being processed?

a) No

b) Yes, you become the only controller

c) Yes, you become a joint controller together with Facebook

Answer: c)

You become a joint controller to the extent you jointly determined the purposes and means for which data was collected by the “like button”.

Click here for more information on the data protection consequences of using social media to promote your business.
9. Under the GDPR, consumers have the right to be informed by companies who are processing their personal data. What does this mean?

a) Companies need to provide a web page with a list of all the personal data they hold about each customer to which customers can navigate to find information

b) Companies need to provide access to their systems by providing data subject with a user ID and password

c) Companies need to provide their data subjects with the information on what data they are collecting, what they are going to do with it, how long they are going to keep it and who will have access to it.

Answer: c)
Companies need to provide their data subjects with the information on what data they are collecting, what they are going to do with it, how long they are going to keep it and who will have access to it.

Click here for more information on individuals’ rights you need to take into account.

10. What information should you give individuals before processing their data for marketing purposes

a) Why their data are being processed

b) The name and contact details of your enterprise

c) How long the data will be stored

d) All of the above

Answer: d)
Article 13 of the GDPR provides a long list of information that should be provided to the individuals concerned before you as an enterprise can start processing their personal data.

Click here for more information on the data protection consequences for direct marketing.

11. In the event of an access request by an individual concerned, what kind of information should you give access to (if requested)?

a) The reason behind the processing

b) who else has access to the data
c) Where the data is stored
d) All of the above

Answer: d)
You should be able to provide the individual concerned with all this information, and this needs to happen without undue delay or in any case within one month of receipt of the request.

Click here for more information on the rights you should grant to individuals whose data you want to process.

12. Can companies informally engage a processor?
a) Yes, because in any case the controller will be the responsible actor under the GDPR
b) No, there always needs to be a contractual agreement between the controller and the processor

Answer: b)
There always needs to be a data processing agreement when engaging a processor.

Click here for more information on how to draft a data processing agreement.

Results & messages:
<7/12: Oops! It seems that you are still struggling with the GDPR...but no need to worry! You can always have a look at the content in this handbook, which is tailor-made to guide micro-enterprises towards GDPR compliance.

7-9/12: Not bad! However, it seems that you are still struggling with a number of GDPR aspects. If you want to learn more about these issues, go check out SMOOK!

10-11/12: Good job! You already seem to be fairly GDPR-literate. For those GDPR aspects that remain unclear, go check out SMOOK! The content of this handbook allows you to quickly navigate to topics of your interest.

12/12: Congratulations! You seem to have mastered the GDPR. If you still have questions, go check out SMOOK, where you can also find examples and templates.
The developers behind SMOOK

SMOOK has been developed under the SMOOTH-project.

The consortium of the SMOOTH-project is made up of technology partners, data protection authorities, innovation and research institutions, associations representing European SME’s and a standardization body organisation.

In total, it consists of 12 organisations, coming from 5 different EU countries (Spain, Belgium, Poland, Latvia and France) and the United Kingdom, which have joint effort and expertise to create tools to help small companies to adopt the GDPR.

The aim of the SMOOTH project is twofold:

1. **To create awareness** regarding the importance of being compliant with the GDPR, as many micro-enterprises may disregard their obligations in this respect.
2. **To assist micro-enterprises** in effectively adopting the GDPR.

A SMOOTH cloud platform will be set up and will use machine learning, text and data mining, and advance online auditing methods to automatically generate a bespoke GDPR compliance report for the most critical aspects for micro-enterprises.

Likewise, SMOOTH will provide useful materials for solving those identified GDPR aspects that are not properly covered. All this will positively contribute to reinforcing citizens’ rights, while avoiding potential fines for the micro-enterprises.
Annex III – SMOOK Mobile App – screenshots and demonstration videos

Eight videos demonstrating the functionality and the design of the SMOOK Mobile App can be viewed here (as these are not final yet, login-credentials are not public and will be communicated separately):

https://eurecatcloud.sharepoint.com/sites/smooth_project/Shared%20Documents/Forms/AllItems.aspx?viewid=671949d8%2D6472%2D4574%2Da015%2D182d9b166f4c&id=%2Fsites%2Fsmtth%5Fproject%2FShared%20Documents%2FSMOOK%20%2D%20Handbook%2FSMOOK%5FInterim%5FVersion%2Fvideos

A few screenshots are also added on the next pages
"GPRD is the biggest legal change of the digital age"
- Mark Lomas, Cap Gemini

& we are ready to help you, step by step, become more compliant.

LEARN MORE
FACTS & NUMBERS

WHAT IS SMOOK?

SMOOK is an online interactive handbook for micro-enterprises, providing detailed guidance to help them understand:

- How the General Data Protection Regulation (GDPR) affects their enterprises;
- What actions they must undertake in order to become GDPR-compliant;
- How to navigate through the GDPR regulation.

WHO IS SMOOK FOR?

SMOOK is especially designed for micro-enterprises. Although the content is tailor-made for them, any enterprise can extract GDPR information from this handbook.

SMEs & the GDPR

My Data Protection Authority

For any questions or advices on your processing activities, you need to turn to the competent data protection authority. This is also the case if you want to request an audit or to file a complaint.

If a data protection impact assessment indicates that your enterprise is engaging in high risk processing, you are obliged to consult the data protection authority prior.
Annex IV – SMOOK Website App – screenshots

What is the SMOOTH GDPR Handbook

SMOOK is an online interactive handbook for micro-enterprises, providing detailed guidance to help them understand:

- How the General Data Protection Regulation
Although the content is tailor-made for them, any enterprise can extract GDPR information from this handbook.

My Data Protection Authority (DPA)

For any questions or advices on your processing activities, you need to turn to the competent data protection authority.

This is also the case if you want to request an audit or to file a complaint.

If a data protection impact assessment indicates that your enterprise is engaging in high risk processing, you are obliged to consult the data protection authority prior to the processing of any data.

You will find the name and contact details of all the Data Protection Authorities in the EU and EEA [here].
GDPR Principles & Rights

Is my enterprise a data controller or data processor?

Every time you process personal data, you will do so either as a data controller or as a data processor. It is very important to know in which of these roles you are operating for each and every data processing activity you undertake. This is because the legal obligations you will bear, differ according to this qualification.

This section aims to clarify when your company will qualify as a data controller, or rather a processor.

When am I a data controller or a data processor?

[video]

Am I a controller or processor?
Answer yes or no to each one of the following questions:

- Did you take the initiative to start collecting or processing in any other way personal data?
- Did you decide the purpose of the processing?
- Did you decide which types of personal data to process?

Am I a joint controller?
Answer yes or no to each one of the following questions:

- Do you have a common objective and purpose with other parties regarding the processing?
- Are you using the same set of personal data for this processing as another controller?
- Do you share the decision-making in relation to the processing of the data?
Additional obligations when relying on "direct marketing":

Essential here is that, through the accountability principle, the GDPR requires you to be able to demonstrate that you have obtained consent for direct marketing. This means that you must keep evidence of who, when, how, and what you told people in the context of requesting consent. Also, very important in this regard is that the individuals concerned have the right to withdraw their consent at any time. Moreover, you need to make sure they can withdraw consent equally as easy compared to the granting of consent.

When is no consent needed?

Important to know is that under certain conditions you are still allowed to process contact details for direct marketing purposes when you did not obtain consent, however, only in cases where the exemption to the 'opt-in consent rule' – referred to as the 'soft opt-in' – is applicable. The exemption exists when three conditions are met:

1. Contact details must have been obtained in the context of a sale of a product or a service, or through pre-contractual negotiations.
   - Safely knowing a company’s website does not matter. By the other hand, acquiring a company to enter into a contract product or service to a basket would be enough to trigger the application of the exemption. It is up to you as a controller to justify direct marketing in this context. 

2. Data collected in this way can only be used for direct marketing of your own similar products or services.
   - This implies that you can only benefit from the exemption if you are the company that initially collected the contact data, and thus have a basis for marketing this way. In this case, you should not be able to collect additional reasonable information.

3. Finally, the targeted individuals should be clearly and distinctly given the opportunity to opt-out, easy and free of charge, to this kind of use of their contact details.
   - The option to object must be presented at the time of the collection of the contact details, and at every time you send them in marketing communications. Generally, this happens through some of the links of the newsletter, and in any case, you must include both an opt-out for general marketing communications and an option for marketing communications falling under the “soft opt-in.”

While the ePrivacy legislation provides an exemption to the necessity for direct marketing, it does not relieve you from the obligation to around your processing on one of the legal bases listed in
Annex V – Human assessment of a case assessed by the SMOOTH Platform

This Annex contains the following documents:

Annex V.1: The entry questionnaire of Lawfrin
Annex V.2: The data file related to the clients of Lawfrin
Annex V.3: The compliance report, generated by the SMOOTH Platform
Annex V.4: The Human Assessment
Annex V.1: The entry questionnaire of Lawfrin

**Block 1: General Business Information**

1. Where does your company operate?
   Answer 1:
   A: Within the EU (or both within the EU and outside the EU)

2. In which country or countries does your company operate?
   Answer 1:
   Belgium

3. Is your company a micro-enterprise?
   Answer 1:
   A: Yes

4. In which sector does your company operate?
   Answer 1:
   E: Law firm

5. What file formats do you use to store personal data?
   Answer 1:
   A: Paper records
   Answer 2:
   B: Electronic copy of paper records (e.g. pdf files or similar)
   Answer 3:
   C: Excel

**Block 2: Processing Customer Personal Data**

1. Does your company collect, store or process in any way personal data from (potential) customers?
   Answer 1:
   A: Yes,
   Upload file name: staff.xlsx

2. Which types of personal data does your company collect from (potential) customers or clients?
   Answer 1:
   A: Contact information (name, (email)address, tel nr., etc.)
3. Where did your company get the personal data from?
   Answer 1:
   A: Directly from the individuals

4. Why does your company process that personal data?
   Answer 1:
   A: To conclude or perform a contract (e.g. for negotiating, for delivering goods, for invoicing...)
   Answer 2:
   B: To comply with a legal obligation

Block 3: Processing Employee Personal Data

1. Does your company collect, store or process in any way personal data of its employees or job applicants?
   Answer 1:
   A: Yes,

2. What type of personal data does your company collect of its employees or job applicants?
   Answer 1:
   A: Contact information (name, (email)address, tel nr., etc.)

3. Where did your company get the personal data from?
   Answer 1:
   A: Directly from the individuals

4. Why does your company need this data?
   Answer 1:
   A: For the performance of a contract (including payment)
   Answer 2:
   B: To comply with a legal obligation (e.g. report salary data of employees to social security or tax authorities)

Block 4: Processing Supplier Personal Data

1. Does your company process personal data of suppliers or any other third-party contractor (e.g. consultants, external IT service providers...)?
   Answer 1:
   B: No

Block 5: Website and Mobile App

1. Do you have a company website and/or mobile application related to your business?
2. Please provide the URL to your website

Answer 1:

URL: www.dvp-law.com

3. Does your website use cookies or other identifiers?

Answer 1:

A: Yes

4. Do you make website visitors aware of the use of cookies or other identifiers by using a cookie banner?

Answer 1:

A: Yes

5. Do you have a cookie policy in place?

Answer 1:

A: Yes

6. Please provide us with your cookie policy and indicate which language the document is written in.

Answer 1:

Upload file name: Law-Cookie policy_en.docx
Language: en

10. Please upload the android package (apk) file

Answer 1:

Upload file name: _con.netspark.mobile.apk
Apk demo user: user
Apk demo password: password

11. Does your mobile app collect, store or process in any other way personal data of its users?

Answer 1:

B: No

Block 6: Transparency

1. Does your company have a privacy policy in place?

Answer 1:

A: Yes
2. Please upload your privacy policy in '.txt' or '.docx' and indicate the language the document is written in

Answer 1:
Upload file name: Law-Privacy policy_en.docx
Language: en

Block 7: Data Minimisation, Accuracy, Storage

1. Does your company only collect the personal data it actually needs to reach its processing purpose(s)?

Answer 1:
A: Yes

2. Do you periodically review the data you hold and delete/anonymise the data you no longer need?

Answer 1:
B: No

3. Do you have appropriate processes in place to check and maintain the accuracy of the data you collect (such as asking individuals to confirm the correctness of their email addresses, by clicking on a link they receive by email or requiring the concerned persons to review their details every X years?)?

Answer 1:
B: No

4. Does your company know what personal data it holds and does it have an appropriate data retention policy in place?

Answer 1:
A: No

Block 8: ICT Security

1. Can every person who works in your company access most of the ICT environment?

Answer 1:
A: Most files and software are accessible by most employees.

2. Are your devices (computers, laptops, smart devices, routers, printers, etc) and ICT environment password protected and do you have a 'password policy' in place?

Answer 1:
B: We do use password protection for all/most devices, but we do not (yet) have a password policy in place.

3. Do you have internal security policies and data policies that you communicate to your employees to ensure that they treat your ICT environment and personal data in a secure way?
Answer 1:
B: Yes, there are some policies in place but my employees are not really aware of these and/or they are not really applied in practice

4. Are your devices (computers, laptops, smart devices, etc.) and portable storage devices encrypted?
Answer 1:
B: Some are, some are not

5. Do you log access to your ICT environment and to personal data?
Answer 1:
B: To a certain extent

6. Is access to your offices secured by an entry system do you keep track (in any way) of who is present in the building and who is not?
Answer 1:
C: No

7. Do you back-up your systems in any way (including in the cloud)?
Answer 1:
B: To a certain extent

8. Do you store your back-ups at a different location (which may be in the cloud) that cannot be directly affected if your main ICT environment gets infected or hacked or if it would be physically damaged?
Answer 1:
B: To a certain extent

Block 9: Data Subject's rights

1. Under the GDPR, companies are obliged to grant individuals certain rights regarding the processing of their personal data. Which of the following requests do you know how to recognise and to correctly respond to?
Answer 1:
B: Request for the right to rectification of inaccurate data

2. Is your company able to address data subject's requests (in principle) free of charge and within the one-month deadline provided in the GDPR (unless an extended deadline is justified)?
Answer 1:
B: No

3. When carrying out a request, are you able to filter out information concerning other persons to ensure you do not disclose information that breaches the right to data protection or any other rights of other individuals?
Block 10: Other GDPR Requirements

1. Do you keep evidence/documents of all the steps you take to comply with the GDPR?
   Answer 1:
   B: No

2. Do you have a register of your processing activities?
   Answer 1:
   B: No

3. Does your company rely on people or organisations (data processor) outside of the company for (certain) data processing activities?
   Answer 1:
   B: No

4. Do you have processes in place to immediately identify personal data breaches and to notify your data protection supervisory authority?
   Answer 1:
Annex V.2: the data file related to the clients of Lawfrin

The uploaded data file contains the following entries:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
<th>Street Address</th>
<th>Postcode</th>
<th>City</th>
<th>Country</th>
<th>Contact Person</th>
<th>Address</th>
<th>Payment Details</th>
</tr>
</thead>
</table>
Annex V.3: the compliance report, generated by the SMOOTH Platform
The main aim of the SMOOTH Platform is to guide micro-entities on the road to GDPR compliance. The results of the compliance report generated by the SMOOTH Platform are for general informational purposes and guidance only. More specifically, based on the information provided to us, it envisages to provide an indication on how well your company is dealing with the GDPR at the moment, and which steps your company should take in light of GDPR compliance. The compliance report is provided in good faith and based on the consortium’s extensive experience with, and knowledge about, the GDPR and its implementation in micro-enterprises. We do not, however, warrant or guarantee that the report will reflect your entire situation, nor can we guarantee that complying with all proposed steps will make you fully GDPR-compliant.

**Warning message:** Do you process personal data on behalf (/on instruction) of your clients? That means you’re also acting as a data processor. Please read more on your obligations as a data processor in the SMOOTH GDPR Handbook.

### D1. General business info

Based on the business sector you are operating in, you are most likely involved in high-risk processing. The SMOOTH Platform was built for enterprises involved in low- or mid-risk processing, therefore it could be that our Platform is not entirely suitable to assess your GDPR compliance. High-risk processing requires extra safeguards to be taken. For more information on what constitutes high risk processing and the consequences thereof, check out the GDPR Handbook (https://www.gdphandbook.eu).

The format in which you store personal data (paper records or electronic copy of paper records) is unfortunately not supported to be analyzed.

### D2. Processing customer personal data

You have indicated that you process personal data of your customers/clients.

One of the most important GDPR principles is ‘data minimisation’, which means that:
- You can only collect personal data you actually need for your specified purposes

- You need to have sufficient personal data to properly fulfil those purposes. You periodically review the data you hold in order to delete the data that is no longer necessary.

It is important to assess whether the processing of your (potential) clients'/customers’ personal data complies with these requirements.

If you would like to know more on the data minimisation principle, check out the GDPR Handbook (https://www.gdprhandbook.eu).

When obtaining personal data, it is important to inform the individuals concerned upon the collection of the data. Mostly, this is done through a privacy policy. At least the following information should be provided:

- Your business’ identity and contact details
- The contact details of your data protection officer (only if you have one)

The purpose(s) for which you process personal data and the legal basis justifying this processing

- The legal basis for the processing (i.e. is the processing based on conclusion or execution of a contract, consent, a legal obligation, legitimate interest(s) etc.)
- The legitimate interest(s) which is/are pursued by your processing operations (only if some of your processing is based on legitimate interest)
- The (categories) of third parties who will have access or will receive the personal data (including your processors)
- Whether you transfer/process personal data outside of the European Economic Area, and the safeguards that are in place

The retention periods for the personal data, or if that is not possible, the criteria used to determine that period

- The rights the individuals have under the GDPR
- The existence of the individuals’ right to withdraw consent at any time
- The individuals’ right to lodge a complaint with a supervisory authority
- The possible consequences if the personal data is not provided
- The existence of automated decision-making, including profiling, and more information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

For each different processing activity you need to identify the concrete purpose(s) thereof. You need to inform the individuals concerned about these purposes (usually through your privacy policy) and record these purposes as part of your documentation obligation.
If, later, you would like to use the personal data for another purpose than the purpose that was originally identified, you can only do so if the new purpose is compatible with the original purpose of data collection, if you get consent or if you have a clear legal obligation or function.

To assess the compatibility of purposes, following elements should be taken into consideration:

a) the link between your original and new purpose
b) the context in which the personal data were originally collected (including your relationship with the individual and individual’s reasonable expectations) c) the nature of the personal data (Sensitive data? Data on children or criminal offences?)

d) potential consequences of the new processing
e) Which safeguards are/will be put in place?

You process personal data to conclude or perform a contract. In order to validly rely on the legitimate basis of ‘contract’ it is very important that you only process data which are necessary for the contract’s conclusion or performance. Processing personal data which are not necessary is not allowed.

The SMOOTH-Platform has identified the following types of customer data. If you do not really need this customer data in light of the purpose of your processing activities, make sure to delete this data and to no longer collect such data in the future. If you do need this customer data to reach the purpose of your processing activities, make sure to inform the individuals’ concerned beforehand.

1. religiousBeliefs
2. race
3. postalAddress
4. phoneNumber

We notice that you are processing personal data that are to be considered as special categories of data or sensitive data under the GDPR. More specifically the following data type(s) mentioned above are to be considered as such: race, religious Beliefs. Such data can only be processed under specific circumstances. To understand what you are allowed to do with such data, please check our GDPR Handbook (https://www.gdprhandbook.eu/justification-grounds), in the last section ‘Special categories of personal data’. Please note that we may not discover every type of (sensitive) personal data that you’re processing, especially if they are mentioned in other languages than the language you have chosen to perform this assessment. Please check our GDPR Handbook (https://www.gdprhandbook.eu/justification-grounds) to make sure that you are not illicitly processing sensitive data.

From analyzing your data files we found that there are personal data categories that you have also indicated in the questionnaire. These categories are also mentioned in your privacy policy. No need for further action. The categories found in your data file are the following.

1. email
D3. Processing employee personal data

You have indicated that you process personal data of your employees. One of the most important GDPR principles is ‘data minimisation’, which means that: - You can only collect personal data you actually need for your specified purposes

- You need to have sufficient personal data to properly fulfil those purposes- You periodically review the data you hold in order to delete the data that is no longer necessary

To do: assess whether the processing of your employees’ or job applicants’ personal data complies with these requirements.

If you would like to know more on the data minimisation principle, check out the GDPR Handbook (https://www.gdprhandbook.eu).

When obtaining personal data, it is important to inform the individuals concerned upon the collection of the data. Mostly, this is done through a privacy policy. At least the following information should be provided:

- Your business’ identity and contact details
- The contact details of your data protection officer (only if you have one)

The purpose(s) for which you process personal data and the legal basis justifying this processing

- The legal basis for the processing (i.e. is the processing based on conclusion or execution of a contract, consent, a legal obligation, legitimate interest(s) etc.)
- The legitimate interest(s) which is/are pursued by your processing operations (only if some of your processing is based on legitimate interest)

- The (categories) of third parties who will have access or will receive the personal data (including your processors)
- Whether you transfer/process personal data outside of the European Economic Area, and the safeguards that are in place

- Retention periods for the personal data, or if that is not possible, the criteria used to determine that period
- The rights the individuals have under the GDPR
- The existence of the individuals’ right to withdraw consent at any time
- The individuals’ right to lodge a complaint with a supervisory authority
- The possible consequences if the personal data is not provided
- The existence of automated decision-making, including profiling, and more information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.
You process job applicants’/employees’ personal data to conclude or perform a contract. In order to validly rely on the legitimate basis of ‘contract’ it is very important that you only process data which are necessary for the contract’s conclusion or performance. Processing personal data which are not necessary is not allowed.

For more information on when it is allowed to process personal data based on contractual necessity, check out GDPR Handbook (https://www.gdprhandbook.eu).

D5. Website and mobile app

The SMOOTH Platform has identified third party organisations on your website.

- One of the key principles underlying the GDPR is the information obligation.

As part of this information obligation, it is important to inform the individuals concerned about who else might receive their personal data.

To do: Make sure this information on third party receivers of personal data is contained in your privacy policy and/or cookie policy.

Analyzing your mobile app we have found third parties / companies that are also mentioned in your cookie policy. No need for further action.

The following companies have been found in your website and are not in the policy.

1. googletagmanager.com google llc alphabet
2. fontawesome.com fonticons inc redacted for privacy purposes
3. addtoany.com \cloudflare inc.\ data redacted
4. gstatic.com google llc
5. typekit.net adobe inc. adobe

D6. Transparency

We have analyzed your privacy policy and it seems that most of the paragraphs are not very easy to understand requiring an education level of College sophomore. You might want to revise it using simpler sentences. According to our analysis, the hardest to understand paragraphs are the following:

1-13 [REMOVED TO AVOID RECOGNITION OF THE ASSESSED COMPANY]

D7. Data minimisation, accuracy, storage

Regularly reviewing the personal data you hold in order to delete or anonymise the data you no longer need, is a necessary practice to comply with the GDPR’s data minimisation principle. To assess which data are no longer necessary, you need to take into account the purpose(s) of your processing activities. In general, the personal data you hold should not include irrelevant details, nor should it be collected on the off-chance that it could be useful in the future. (E.g. a job
application form asking for the applicant’s photo, religion or sexual orientation, when this is not relevant in light of the job).

The GDPR requires you to ensure the accuracy of the data you collect/have collected. You should take all reasonable steps to guarantee that the personal data you hold is correct. This implies that you may need to keep the personal data updated. In case personal data turns out to be incorrect or misleading, you are expected to take necessary, reasonable steps to correct or erase the data without any delay.

D8. ICT Security

Getting there! The SMOOTH Platform indicates that you have already undertaken some important steps with benefitting your ICT security, but you are not quite there yet. A key GDPR principle is that personal data needs to be processed securely by means of appropriate technical and organisational measures. If you do not have one yet, you should start by establishing an ICT security policy, corresponding to the risk level of your enterprise’s activities. To see what other technical or organisational measures you could take, check out ICO’s checklist here https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-dataprotection-regulation-gdpr/security/

D9. Data subject’s rights

Not only should you take the necessary technical and organisational measures to be able to grant the data subjects’ rights, in general, when an individual exercises his or her rights, you should be able to respond to this request within a time period of one month. However, there are exceptions in which this time period can be extended.

In principle, you cannot charge a fee for satisfying the individual’s request If an individual submits manifestly unfounded or excessive requests you can either charge a reasonable fee or refuse to act on a request. It will be up to you to be able to prove that a request was manifestly unfounded or excessive.

It is important to implement technical and organizational measures so that, when granting a request, you can filter out information concerning other persons to ensure that the rights and freedoms of those other persons are not affected.

D10. Other GDPR requirements

The legislator does not only require you to comply with the GDPR, additionally you should also be able to demonstrate your compliance. You should keep evidence of the technical and organisational measures, as well as other activities, that you have undertaken in order to be GDPR compliant.

There is no list of specific measures to prove GDPR compliance, but some examples are:

- drafting and implementing a data protection policy
- keeping records about data processing activities
- documenting how, when and how consent was obtained
- implementing security measures
- recording (and reporting) data breaches
- appointing a DPO
- conducting a DPIA for processing personal data that are likely to result in high risk to individuals’ rights and interests.

For more information on the accountability principle, check out the GDPR Handbook (https://www.gdprhandbook.eu).

You have indicated that you do not have a register of your processing activities. However, the GDPR requires you to document your processing activities. Such a register should contain at least the following information:
- Name and contact details of your organisation (and where applicable, of other controllers, your representative and your data protection officer)
- The purposes underlying your processing activities
- The categories of individuals and categories of personal data
- The categories of recipients of personal data
- If applicable, details on transfers to third countries
- Retention policy (how long is the data stored?)
- Your technical and organisational security measures

These records need to be checked periodically, and if necessary, should be updated. This is important because you may be required to make these records available to the data protection authority of your country.

The GDPR takes SMEs into account by including an exemption on recordkeeping for companies with less than 250 employees. If you have less than 250 employees, you only need to document processing activities that:
- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data.

For an example of such a documentation template, click here

Annex V.4: the Human Assessment

GDPR assessment of the lawfirm ‘Lawfrin’

Please find below the performed assessment. In order to be able to easily compare this report with the automated report, the Human Assessment follows the same structure as the automated assessment. The titles below are the titles used in both the entry questionnaire and the compliance report.

Context

Lawfrin is a Belgian lawfirm, mainly active on the Belgian market. It is a business law firm, focussing on tax, white collar crime, wealth planning, corporate and general private law issues, delivering services to both enterprises and individuals.

The assessment below is to be considered as a general and accessible advice. Note that this kind of advice can be made form very short to very long, depending on the details that are dived into. The current depth of the analysis is based on the type of report and assessment that the Smooth Platform provides and also takes into account that a general advice addressed at a Micro-SME must be short, hands-on and cost-efficient.

Lawfrin’s GDPR compliance will be assessed based on:

- The completed entry questionnaire
- The uploaded privacy policy and cookie policy
- The uploaded data file
- Their website
- An android APK-file, relating to the MEnts mobile application

1. General business information

1.1. The entry questionnaire (the ‘EQ’)

Block 1: General Business Information

1. Where does your company operate?

Answer 1:
1.2. Analysis

As a lawfirm, Lawfrin operates in a regulated environment in which it will necessary engage in high-risk processing.

Extra care is therefore recommended. A more in-depth analysis may be required, beyond the scope of the type assessment the Platform (and this assessment) are providing.

Lawfrin should already take into account that it should take adequate measures to avoid that the personal data it processes that are stored in paper records and electronic files cannot be easily accessed or divulged by anyone. Furthermore, it is likely that Lawfrin also stores personal data in databases, including those that are part of the applications it uses (such as their e-mail client, accounting software, billing software, etc.).

1.3. The conclusion of the compliance report

Based on the business sector you are operating in, you are most likely involved in high-risk processing. The SMOOTH Platform was built for enterprises involved in low- or mid-risk processing, therefore it could be that our Platform is not entirely suitable to assess your GDPR compliance. High-
risk processing requires extra safeguards to be taken. For more information on what constitutes high risk processing and the consequences thereof, check out the GDPR Handbook (https://www.gdprhandbook.eu).

The format in which you store personal data (paper records or electronic copy of paper records) is unfortunately not supported to be analyzed.

1.4. Conclusion

The conclusions of both the Human Assessment and the automated assessment are similar. The Human Assessment is a little more tailored to the type of activities of Lawfrin, but it is logic that the Platform doesn’t do this as 1) its conclusions have to be generally applicable en 2) Lawfrin is not the primary audience of the Smooth Platform. Important here is that the Platform provides a clear disclaimer to Lawfrin, indicating that it will normally be involved into high-risk processing and therefore should seek additional information or guidance, while providing a link to the GDPR Handbook where additional information can be retrieved.

2. Processing customer personal data

2.1. The EQ

<table>
<thead>
<tr>
<th>Block 2: Processing Customer Personal Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does your company collect, store or process in any way personal data from (potential) customers?</td>
</tr>
<tr>
<td>Answer 1:</td>
</tr>
<tr>
<td>A: Yes,</td>
</tr>
<tr>
<td>Upload file name: staff.xlsx</td>
</tr>
<tr>
<td>2. Which types of personal data does your company collect from (potential) customers or clients?</td>
</tr>
<tr>
<td>Answer 1:</td>
</tr>
<tr>
<td>A: Contact information (name, (email)address, tel nr., etc.)</td>
</tr>
<tr>
<td>3. Where did your company get the personal data from?</td>
</tr>
<tr>
<td>Answer 1:</td>
</tr>
<tr>
<td>A: Directly from the individuals</td>
</tr>
<tr>
<td>4. Why does your company process that personal data?</td>
</tr>
</tbody>
</table>

---

*This comment is also applicable to the next blocks, but will not be repeated under each block.*
Answer 1:
A: To conclude or perform a contract (e.g. for negotiating, for delivering goods, for invoicing...)

Answer 2:
B: To comply with a legal obligation

The uploaded data file contains the following information of 9 persons:

- Internal identification number
- Name
- E-mail
- Phone number
- Bank account number
- Address
- Monthly income
- Date of birth
- Username
- Password
- Racial origin
- Religious belief

2.2. Human Assessment

2.2.1. The processed personal data

a. Data minimisation

Personal data can only be processed (and stored) if the processing thereof is required for a legitimate purpose and if, among other things, processing is based on a legitimate basis.

(Types of) personal data of which processing is not required (anymore) for such purpose, cannot (or no longer) be processed. The purpose of this obligation is to reduce the volume and types of processed data as much as possible.

b. Missing types of (sensitive) personal data

Lawfrin clearly indicated (much) too few personal data categories it is processing. The data categories present in the data file are broader than those in the EQ, but still don’t seem to be complete.

As a lawfirm, Lawfrin will normally/probably process many other (sensitive) categories, such as ID card number, (electronic) signature, social security number, nationality, marital status, trade union membership, images, information about health, diploma, information
about criminal offences or convictions or certificate of good conduct, data related to children, etc.

c. Not enough data subjects are covered by the data file

Furthermore, the uploaded list of processed personal data only refers to 9 data subjects, so it is clearly incomplete from that perspective too, which means that other data types may be missing too.

d. Categories of sensitive data that shouldn’t be processed

The data file contains sensitive information related to racial origin and religious belief. These types of personal data cannot be processed, except in specific and very exceptional circumstances and if actually required for a legitimate purpose (for example in a legal case about discrimination).

e. Other categories of sensitive data

Different special categories of more general sensitive data are processed, such as bank account number and income. These categories are also to be considered as having a more sensitive nature and should only be processed under specific circumstances and with due care.

2.2.2. The source of the personal data

Lawfin indicates that it obtains all customer personal data directly from the individuals. Normally Lawfin will also obtain personal data from third parties, such as the employer, the national register, other databases or counterparties.

2.2.3. Legitimate processing

To legitimitaly process personal data, it is required to apply the principles of data minimisation, lawfulness, fairness and transparency, purpose limitation, accuracy, storage limitation, integrity and confidentiality and accountability.

A little more information on some of these concepts (in very short):

- Data minimisation (see above)
- Lawfullness: Lawfin can only process personal data if this processing is based on one of the 6 lawfull processing bases described in the GDPR. The most relevant lawfull processing bases for an enterprise are: contract (when Lawfin needs to process personal data of a client as part of a contract with the client), legal obligation (when the law imposes the processing, for example a VAT number because it has to be mentioned on an invoice), consent (if the client consents to specific processing) and legitimate interest (if Lawfin has a legitimate interest to process personal and this interest overrides the client concerned’s interest not to have his data processed).
  - Lawfin indicates that personal data is only processed for the performance of a contract. First of all, only personal data that is strictly necessary for the
performance of a contract can be processed under this legal basis. Second, parts of the processing will normally also be based on legal obligation (for example the VAT number and anti-money laundering information), on legitimate interest and on consent.

- Transparency: Lawfrin must make sure that the persons concerned know that Lawfrin is processing their data, what data it is processing, that they understand the purpose of the processing, etc. This information is normally provided via privacy notices combined with your privacy policy. Lawfrin’s privacy policy has to provide specific types of information, as prescribed by law (see below).

2.3. Platform assessment (compliance report)

You have indicated that you process personal data of your customers/clients.

One of the most important GDPR principles is ‘data minimisation’, which means that:

- You can only collect personal data you actually need for your specified purposes
- You need to have sufficient personal data to properly fulfil those purposes- You periodically review the data you hold in order to delete the data that is no longer necessary

It is important to assess whether the processing of your (potential) clients’/customers’ personal data complies with these requirements.

If you would like to know more on the data minimisation principle, check out the GDPR Handbook (https://www.gdprhandbook.eu).

When obtaining personal data, it is important to inform the individuals concerned upon the collection of the data. Mostly, this is done through a privacy policy. At least the following information should be provided:

- Your business’ identity and contact details
- The contact details of your data protection officer (only if you have one)
- The purpose(s) for which you process personal data and the legal basis justifying this processing
- The legal basis for the processing (i.e. is the processing based on conclusion or execution of a contract, consent, a legal obligation, legitimate interest(s) etc.)
- The legitimate interest(s) which is/are pursued by your processing operations(only if some of your processing is based on legitimate interest)
- The (categories) of third parties who will have access or will receive the personal data (including your processors)
- Whether you transfer/process personal data outside of the European Economic Area, and the safeguards that are in place
- Retention periods for the personal data, or if that is not possible, the criteria used to determine that period

- The rights the individuals have under the GDPR

- The existence of the individuals’ right to withdraw consent at any time

- The individuals’ right to lodge a complaint with a supervisory authority

- The possible consequences if the personal data is not provided

- The existence of automated decision-making, including profiling, and more information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

For each different processing activity you need to identify the concrete purpose(s) thereof. You need to inform the individuals concerned about these purposes (usually through your privacy policy) and record these purposes as part of your documentation obligation.

If, later, you would like to use the personal data for another purpose than the purpose that was originally identified, you can only do so if the new purpose is compatible with the original purpose of data collection, if you get consent or if you have a clear legal obligation or function.

To assess the compatibility of purposes, following elements should be taken into consideration:

a) the link between your original and new purpose

b) the context in which the personal data were originally collected (including your relationship with the individual and individual’s reasonable expectations)

c) the nature of the personal data (Sensitive data? Data on children or criminal offences?)

d) potential consequences of the new processing

d) Which safeguards are/will be put in place?

You process personal data to conclude or perform a contract. In order to validly rely on the legitimate basis of ‘contract’ it is very important that you only process data which are necessary for the contract’s conclusion or performance. Processing personal data which are not necessary is not allowed.

The SMOOTH-Platform has identified the following types of customer data. If you do not really need this customer data in light of the purpose of your processing activities, make sure to delete this data and to no longer collect such data in the future. If you do need this customer data to reach the purpose of your processing activities, make sure to inform the individuals’ concerned beforehand.

- religiousBeliefs
- race
- postalAddress
- phoneNumber

We notice that you are processing personal data that are to be considered as special categories of data or sensitive data under the GDPR. More specifically the following data type(s)
mentioned above are to be considered as such: race, religious Beliefs. Such data can only be processed under specific circumstances. To understand what you are allowed to do with such data, please check our GDPR Handbook (https://www.gdprhandbook.eu/justification-grounds), in the last section ‘Special categories of personal data’. Please note that we may not discover every type of (sensitive) personal data that you’re processing, especially if they are mentioned in other languages than the language you have chosen to perform this assessment. Please check our GDPR Handbook (https://www.gdprhandbook.eu/justification-grounds) to make sure that you are not illicitly processing sensitive data.

From analyzing your data files we found that there are personal data categories that you have also indicated in the questionnaire. These categories are also mentioned in your privacy policy. No need for further action. The categories found in your data file are the following.

- email
- name

2.4. Conclusion

In general, both conclusions are similar, whereas the Platform Assessment provides more information on general aspects than the Human Assessment. Here we can see that the combo of the GDPR Handbook with the Platform is a strong one, because it allows for the Platform to briefly touch upon a subject and refer the MEnt to the GDPR Handbook for further information.

Both the Platform and the Human Assessment recognize a few sensitive types of data and provide adequate warnings. The Platform did however not recognize all types of (sensitive) data that were part of the uploaded file. This is due to the technical limitations (described elsewhere in D2.4, see above) and is consequently in line with what is to be expected. Furthermore, warning of these limitations was provided to make sure that the MEnt is aware of these.

In the case the data file was very small, both the Platform and the Human Assessment can rather easily identify the data categories that were part of it. However, as soon as these files are larger and contain personal data, it is to be expected that the Platform will outperform a human (subject to the limitations described above however).

Finally, here also, the Human Assessment who works on a case by case basis, is able to provide more tailored advice and notices that several categories of personal data are missing and also that the data sources appear to be inconsistent, whereas this is much more difficult to do for an automated system, especially in a case like this which involves a MEnt active in high risk processing.

3. Processing employee personal data

3.1. The EQ
Block 3: Processing Employee Personal Data

1. Does your company collect, store or process in any way personal data of its employees or job applicants?

   Answer 1:
   A: Yes,

2. What type of personal data does your company collect of its employees or job applicants?

   Answer 1:
   A: Contact information (name, (email)address, tel nr., etc.)

3. Where did your company get the personal data from?

   Answer 1:
   A: Directly from the individuals

4. Why does your company need this data?

   Answer 1:
   A: For the performance of a contract (including payment)
   Answer 2:
   B: To comply with a legal obligation (e.g. report salary data of employees to social security or tax authorities)

3.2. Human Assessment analysis

3.2.1. The processed personal data

Missing types of (sensitive) personal data

Lawfrin indicated that it only processes contact information of its employees. No data file has been uploaded.

Here also, it appears, that Lawfrin only identifies a few of the many types of the employee personal data it processes.

Any employer will process other (sensitive) personal data of its employees such as ID card number, (electronic) signature, social security number, nationality, marital status, trade union membership, images, information about health, diploma, etc.
3.2.2. The source of the personal data

Lawfrin indicates that it obtains all employee personal data directly from the employees. Normally Lawfin will also obtain personal employee data via other ways, for example from third parties, such as the social security service, and via indirect means, such as via a registered access system to its buildings, through monitoring of its network and through security cameras.

3.2.3. Legitimate processing

The principles described above (under 2.2.2) are also applicable to the processing of employee personal data.

Specifically when processing employee data, it has to be taken into account that the employer is in a hierarchic position and therefore it is very difficult for an employee to provide ‘free’ consent. Consequently, consent can only be used to process personal employee data in very limited circumstance for accessory processing activities under which there can not exist any doubt that the employee was really entitled to refuse consent and that the employee would not suffer any negative consequence when refusing or withdrawing consent.

Lawfrin indicates that it only processes personal data to perform its contractual obligations towards the employee and to comply with its legal obligations. Most likely, Lawfrin will also process personal data based on the legal ground ‘legitimate interest’ and possibly also based on ‘consent’.

3.3. The conclusion of the compliance report

You have indicated that you process personal data of your employees. One of the most important GDPR principles is ‘data minimisation’, which means that: - You can only collect personal data you actually need for your specified purposes

- You need to have sufficient personal data to properly fulfil those purposes- You periodically review the data you hold in order to delete the data that is no longer necessary

To do: assess whether the processing of your employees’ or job applicants’ personal data complies with these requirements.

If you would like to know more on the data minimisation principle, check out the GDPR Handbook (https://www.gdprhandbook.eu).

When obtaining personal data, it is important to inform the individuals concerned upon the collection of the data. Mostly, this is done through a privacy policy. At least the following information should be provided:

- Your business’ identity and contact details

- The contact details of your data protection officer (only if you have one)
- The purpose(s) for which you process personal data and the legal basis justifying this processing

- The legal basis for the processing (i.e. is the processing based on conclusion or execution of a contract, consent, a legal obligation, legitimate interest(s) etc.)

- The legitimate interest(s) which is/are pursued by your processing operations (only if some of your processing is based on legitimate interest)

- The (categories) of third parties who will have access or will receive the personal data (including your processors)

- Whether you transfer/process personal data outside of the European Economic Area, and the safeguards that are in place

- Retention periods for the personal data, or if that is not possible, the criteria used to determine that period

- The rights the individuals have under the GDPR

- The existence of the individuals’ right to withdraw consent at any time

- The individuals’ right to lodge a complaint with a supervisory authority

- The possible consequences if the personal data is not provided

- The existence of automated decision-making, including profiling, and more information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

You process job applicants’/employees’ personal data to conclude or perform a contract. In order to validly rely on the legitimate basis of ‘contract’ it is very important that you only process data which are necessary for the contract’s conclusion or performance. Processing personal data which are not necessary is not allowed.

For more information on when it is allowed to process personal data based on contractual necessity, check out GDPR Handbook


3.4. Conclusion

The conclusion is more or less the same than the conclusion under ‘processing customer personal data’, i.e. that both come to similar results, that the Platform provides more information with links to the GDPR Handbook, but that it is more difficult for the Platform to spot missing information, related to specific types of MEnts.
4. Processing supplier personal data

4.1. The EQ

**Block 4: Processing Supplier Personal Data**

1. **Does your company process personal data of suppliers or any other third-party contractor (e.g. consultants, external IT service providers...)?**

   Answer 1:
   
   B: No

4.2. Human Assessment analysis

Lawfrin indicates that it doesn’t process any personal data of its suppliers.

This is very unlikely and the answer to this question should be re-assessed by Lawfrin.

4.3. Platform assessment (compliance report)

N/A (as it was indicated that Lawfrin doesn’t process supplier personal data, there is no conclusion for this block)

4.4. Conclusion

The Platform doesn’t provide any feedback.

Ideally, in a following update the compliance report can display a warning similar to the one above, when a MEnt indicates that it doesn’t process personal data of suppliers.

5. Website and mobile app

5.1. The EQ

**Block 5: Website and Mobile App**
1. Do you have a company website and/or mobile application related to your business?
Answer 1:
A: Yes, both

2. Please provide the URL to your website
Answer 1:
URL: [obfuscated]

3. Does your website use cookies or other identifiers?
Answer 1:
A: Yes

4. Do you make website visitors aware of the use of cookies or other identifiers by using a cookie banner?
Answer 1:
A: Yes

5. Do you have a cookie policy in place?
Answer 1:
A: Yes

6. Please provide us with your cookie policy and indicate which language the document is written in.
Answer 1:
Upload file name: Law-Cookie policy_en.docx
Language: en

10. Please upload the android package (apk) file
Answer 1:
Upload file name: _con.netspark.mobile.apk
Apk demo user: user
Apk demo password: password

11. Does your mobile app collect, store or process in any other way personal data of its users?
Answer 1:
B: No
5.2. Human Assessment analysis

5.2.1. Secure website and use of cookies

The website uses a secure (SSL) connection.

When visiting the website, a cookie banner pops up, asking for permission to install statistical and marketing cookies. Only functional cookies are pre-ticked (and cannot be unticked). Functional cookies are described as "Cookies that are necessary for the website to function normally". There is no separate mention of necessary cookies. Therefore, the category of functional cookies should be split in ‘necessary cookies’ and ‘functional cookies’ and ‘functional cookies’ should not be pre-ticked.

It is a good thing that marketing and statistical cookies are not pre-ticked, but, however, it appears that even before the cookies are accepted, several marketing and statistical cookies are installed on the computer of the website visitor (for example LinkedIn analytics and Google analytics). This is not allowed: these cookies may only be installed upon approval of the website visitor.

Finally, there is a cookie preference center where website visitors can review what cookies they have consented to and withdraw their consent, which is a good thing too.

5.2.2. Cookie policy

The cookie policy appears to be quite complete and quite readable and distinguishes between ‘necessary’ and ‘functional’ cookies (as opposed to the cookie banner, which describes functional cookies as necessary cookies). It appears that it needs to be updated though, as it refers to general solutions only to refuse cookies or withdraw earlier consent (such as the browser settings) and doesn’t refer to the (existing) cookie preference center. It doesn’t contain a link to the cookie preference center, but a link to this center can be found in the footer, next to a link to the privacy policy. Links to both and a few words of explanation should be inserted in the cookie policy itself.

The cookie policy mentions the cookies that are supposed to be used on the website, but some cookies mentioned here appear not to be used on the website (for example hotjar). On the other hand, some cookies that are used on the website, are not mentioned in the cookie policy (for example Adobe). This should also be updated.

5.2.3. The mobile app

It’s not possible for me the verify the apk-file.

5.3. Platform assessment (compliance report)

*The SMOOTH Platform has identified third party organisations on your website.*

- **One of the key principles underlying the GDPR is the information obligation.**

As part of this information obligation, it is important to inform the individuals concerned about who else might receive their personal data.
To do: Make sure this information on third party receivers of personal data is contained in your privacy policy and/or cookie policy.

Analyzing your mobile app we have found third parties / companies that are also mentioned in your cookie policy. No need for further action.

The following companies have been found in your website and are not in the policy.

- googletagmanager.com google llc alphabet
- fontawesome.com fonticons inc redacted for privacy purposes
- addtoany.com \cloudflare inc \ data redacted
- gstatic.com google llc
- typekit.net adobe inc. adobe

5.4. Conclusion

The Platform does a good job in identifying the used cookies and verifying if they are mentioned in the cookie policy. It is also able to check the APK-file, which the human could not.

The other topics of the human assessment are not part of the assessment performed by the Platform.

6. Transparency

6.1. The EQ

Block 6: Transparency

1. Does your company have a privacy policy in place?

Answer 1:

A: Yes

2. Please upload your privacy policy in '.txt' or '.docx' and indicate the language the document is written in

Answer 1:

Upload file name: Law-Privacy policy_en.docx

Language: en
6.2. Human Assessment analysis

Note: normally I would not ‘describe’ the assessment of a privacy policy in a separate document, but correct and modify the policy itself.

6.2.1. The privacy policy

The privacy policy formally mentions (almost) all the topics it has to mention. It is however too short and lacks clarity and sufficient information to allow the persons concerned (the website visitor, the client, the counterparty, the job applicant, etc.) to really understand how Lawfrin is processing (collecting, using, etc) their data, what their rights are, what safeguards are in place, how long the data is retained, etc.

In its current form, this privacy policy is insufficient. Additional and more practical information should be mentioned.

Also, it mentions that no data is processed outside of the EU, which is very unlikely taking into account the cookies that are used. Moreover, no mention of the use of cookies is made and a link to the cookie policy is missing.

Finally, ideally the format should be modified to make the privacy policy more intelligible and accessible. Next to using accessible and plain language, this can, for example, be done by using a layered privacy policy, adding a short resume of the important points at the beginning of the policy and/or formatting it in such a way that the most important information can be easily retrieved in the policy.

6.3. Platform assessment (compliance report)

We have analyzed your privacy policy and it seems that most of the paragraphs are not very easy to understand requiring an education level of College sophomore. You might want to revise it using simpler sentences. According to our analysis, the hardest to understand paragraphs are the following:

[13 PARAGRAPHS REMOVED TO AVOID RECOGNITION OF THE ASSESSED COMPANY]

6.4. Conclusion

In general, both assessments conclude that the privacy policy is insufficient and that it should be drafted in a more readable and clear way.

The Human Assessment provides more detail however on what parts are exactly missing or should be explained in more detail. This is due to the technical limitations of the Platform.
7. Data minimisation, accuracy and storage

7.1. The EQ

<table>
<thead>
<tr>
<th>Block 7: Data Minimisation, Accuracy, Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does your company only collect the personal data it actually needs to reach its processing purpose(s)?</td>
</tr>
<tr>
<td>Answer 1: A: Yes</td>
</tr>
<tr>
<td>2. Do you periodically review the data you hold and delete/anonymise the data you no longer need?</td>
</tr>
<tr>
<td>Answer 1: B: No</td>
</tr>
<tr>
<td>3. Do you have appropriate processes in place to check and maintain the accuracy of the data you collect (such as asking individuals to confirm the correctness of their email addresses, by clicking on a link they receive by email or requiring the concerned persons to review their details every X years)?</td>
</tr>
<tr>
<td>Answer 1: B: No</td>
</tr>
<tr>
<td>4. Does your company know what personal data it holds and does it have an appropriate data retention policy in place?</td>
</tr>
<tr>
<td>Answer 1: A: No</td>
</tr>
</tbody>
</table>

7.2. Human Assessment analysis

Personal data can only be processed if such processing is strictly necessary for the lawful processing purposes it was collected for. When this is no longer the case, such data should be destroyed or duly anonymized (duly anonymizing personal data is considered the same as destroying personal data from a data protection point-of-view). Therefore, Lawfrin should have a retention policy in place in which it defines the durations. It will store the different types of personal data it is processing and processes that ensure that the retention periods are applied in practice. These obligations relate to the ‘data minimisation’ and the ‘storage limitation’ principles.
Further, following the ‘accuracy’ principle, Lawfrin must also take care that the personal data it processed remains accurate and is kept up to date. It should put processes in place to maintain such accuracy, such as suggested in the question above.

7.3. Platform assessment (compliance report)

Regularly reviewing the personal data you hold in order to delete or anonymise the data you no longer need, is a necessary practice to comply with the GDPR’s data minimisation principle. To assess which data are no longer necessary, you need to take into account the purpose(s) of your processing activities. In general, the personal data you hold should not include irrelevant details, nor should it be collected on the off-chance that it could be useful in the future. (E.g. a job application form asking for the applicant’s photo, religion or sexual orientation, when this is not relevant in light of the job).

The GDPR requires you to ensure the accuracy of the data you collect/ have collected. You should take all reasonable steps to guarantee that the personal data you hold is correct. This implies that you may need to keep the personal data updated. In case personal data turns out to be incorrect or misleading, you are expected to take necessary, reasonable steps to correct or erase the data without any delay.

7.4. Conclusion

Both the Platform assessment and the Human Assessment come to more or less the same conclusions.

8. ICT Security

8.1. The EQ

Block 8: ICT Security

1. Can every person who works in your company access most of the ICT environment?

Answer 1:

A: Most files and software are accessible by most employees.

2. Are your devices (computers, laptops, smart devices, routers, printers, etc) and ICT environment password protected and do you have a 'password policy' in place?

Answer 1:
B: We do use password protection for all/most devices, but we do not (yet) have a password policy in place.

3. Do you have internal security policies and data policies that you communicate to your employees to ensure that they treat your ICT environment and personal data in a secure way?

Answer 1:

B: Yes, there are some policies in place but my employees are not really aware of these and/or they are not really applied in practice

4. Are your devices (computers, laptops, smart devices, etc.) and portable storage devices encrypted?

Answer 1:

B: Some are, some are not

5. Do you log access to your ICT environment and to personal data?

Answer 1:

B: To a certain extent

6. Is access to your offices secured by an entry system do you keep track (in any way) of who is present in the building and who is not?

Answer 1:

C: No

7. Do you back-up your systems in any way (including in the cloud)?

Answer 1:

B: To a certain extent

8. Do you store your back-ups at a different location (which may be in the cloud) that cannot be directly affected if your main ICT environment gets infected or hacked or if it would be physically damaged?

Answer 1:

B: To a certain extent

8.2. Human Assessment analysis

It appears that Lawfrin has already taken the most important steps, but that there are still a few steps to take. Lawfrin, as a lawfirm, should implement the measures suggested above in the questions should of the EQ. It should more in general take care that it has adequate technical and organisational measures in place to protect the data it is processing and, more in general, its ICT
environment. Also, it is important to draft the required policies, to enforce them where possible and to ensure that the employees are aware of this policies and their importance.

8.3. Platform assessment (compliance report)

*Getting there! The SMOOTH Platform indicates that you have already undertaken some important steps with benefitting your ICT security, but you are not quite there yet. A key GDPR principle is that personal data needs to be processed securely by means of appropriate technical and organisational measures. If you do not have one yet, you should start by establishing an ICT security policy, corresponding to the risk level of your enterprise’s activities. To see what other technical or organisational measures you could take, check out ICO’s checklist here https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protection-regulation-gdpr/security/*

8.4. Conclusion

Both the Platform and the Human Assessment come to more or less the same conclusions.

Here also, the Human Assessment is able to tailor the advice more to the specific MEnt, whereas the Platform is able to provide additional useful general information, referring to the GDPR Handbook for further information.

9. Data subject’s rights

9.1. The EQ

**Block 9: Data Subject’s rights**

1. Under the GDPR, companies are obliged to grant individuals certain rights regarding the processing of their personal data. Which of the following requests do you know how to recognise and to correctly respond to?

   Answer 1:

   B: Request for the right to rectification of inaccurate data

2. Is your company able to address data subject’s requests (in principle) free of charge and within the one-month deadline provided in the GDPR (unless an extended deadline is justified)?

   Answer 1:

   B: No

3. When carrying out a request, are you able to filter out information concerning other persons to ensure you do not disclose information that
breaches the right to data protection or any other rights of other individuals?

Answer 1:
B: No

9.2. Human Assessment analysis

Under the GDPR, data subjects have the following ‘data subjects’ rights’:

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object
- Right not to be subject to automated individual-decision making (including profiling)

In short, the first 5 of these rights allow the persons concerned, under the applicable conditions, to gain insights in and access their personal data Lawfrin is processing, to have such data corrected or deleted, to have Lawfrin stop processing the data without deleting it and to take such data to another service provider.

When Lawfrin obtains a request from a person who wishes to exercise such a right, it should react (and comply with the request) within one month as from the request. If this is objectively justified, this delay can be extended with 2 more months but the person concerned has to be informed hereof within the initial month.

This means that Lawfrin’s systems have to be able to comply with such requests and that it has to have processes on how to deal with such requests within the applicable delays. It must also make sure that its employees recognize such requests, because requests will not always be addressed to the right persons.

Also, when communicating personal data to a person concerned, such communication cannot infringe other’s data protection rights, so an evaluation of the data to be communicated may be required.

These requests have to be complied with free of charge, except in circumstances where the request are clearly abusive, in which case the request can be refused or a reasonable cost can be charged. It is in that case of course up to Lawfrin to demonstrate that the request was abusive.
9.3. Platform assessment (compliance report)

Not only should you take the necessary technical and organisational measures to be able to grant the data subjects’ rights, in general, when an individual exercises his or her rights, you should be able to respond to this request within a time period of one month. However, there are exceptions in which this time period can be extended.

In principle, you cannot charge a fee for satisfying the individual’s request. If an individual submits manifestly unfounded or excessive requests, you can either charge a reasonable fee or refuse to act on a request. It will be up to you to be able to prove that a request was manifestly unfounded or excessive.

It is important to implement technical and organizational measures so that, when granting a request, you can filter out information concerning other persons to ensure that the rights and freedoms of those other persons are not affected.

9.4. Conclusion

The conclusions of both assessments are similar.

10. Other GDPR requirements

10.1. The EQ

<table>
<thead>
<tr>
<th>Block 10: Other GDPR Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Do you keep evidence/documents of all the steps you take to comply with the GDPR?</td>
</tr>
<tr>
<td>Answer 1:</td>
</tr>
<tr>
<td>B: No</td>
</tr>
<tr>
<td>2. Do you have a register of your processing activities?</td>
</tr>
<tr>
<td>Answer 1:</td>
</tr>
<tr>
<td>B: No</td>
</tr>
<tr>
<td>3. Does your company rely on people or organisations (data processor) outside of the company for (certain) data processing activities?</td>
</tr>
<tr>
<td>Answer 1:</td>
</tr>
</tbody>
</table>
B: No

4. Do you have processes in place to immediately identify personal data breaches and to notify your data protection supervisory authority?

Answer 1:

10.2. Human Assessment

Lawfrin must not only comply with the GDPR, but it should also be able to demonstrate that it complies with the GDPR and the processing principles. This obligation is the ‘accountability’ principle. This means that it has to document the steps it takes to protect the personal data it processes, and it must be able to submit such documentation to the data protection authority to demonstrate its compliance. Such documentation should also contain the evaluations and trade-offs that were made when a specific way of processing was chosen or, for example, why certain security measures were considered to be sufficient in a specific context.

As a lawfirm, Lawfrin will most likely be required to maintain a record of processing activities and, if not, it is still strongly recommended. A record of processing activities must list the processing activities and mention specific information about these processing activities. It will be the go-to database for all information about processing and it will be one of the first documents a data protection authority would want to see in the case of an audit. An easy to complete template can be provided, which will help Lawfrin to complete the record.

Lawfrin indicates that it does not rely on data processors for the processing of its data. This is not credible. First of all, in Belgium, the lawyers working at Lawfrin are all independents and are all to be considered as data processors. Furthermore, Lawfrin will in almost any case use hosting providers, external ICT service providers, external accountants, external lawyers, etc. who will all to a certain extent process personal data on behalf of Lawfrin. With each of these processors, a data processing agreement must be signed. These data processing agreements have to meet the requirements as imposed by the GDPR. If Lawfrin would desires so, templates can be provided, or we can help them drafting these.

10.3. Platform assessment (compliance report)

The legislator does not only require you to comply with the GDPR, additionally you should also be able to demonstrate your compliance. You should keep evidence of the technical and organisational measures, as well as other activities, that you have undertaken in order to be GDPR compliant.

There is no list of specific measures to prove GDPR compliance, but some examples are:

- drafting and implementing a data protection policy
- keeping records about data processing activities
- documenting how, when and how consent was obtained
- implementing security measures
- recording (and reporting) data breaches
- appointing a DPO
- conducting a DPIA for processing personal data that are likely to result in high risk to individuals’ rights and interests.

For more information on the accountability principle, check out the GDPR Handbook (https://www.gdprhandbook.eu).

You have indicated that you do not have a register of your processing activities. However, the GDPR requires you to document your processing activities. Such a register should contain at least the following information:

- Name and contact details of your organisation (and where applicable, of other controllers, your representative and your data protection officer)
- The purposes underlying your processing activities
- The categories of individuals and categories of personal data.
- The categories of recipients of personal data
- If applicable, details on transfers to third countries
- Retention policy (how long is the data stored?)
- Your technical and organisational security measures

These records need to be checked periodically, and if necessary, should be updated. This is important because you may be required to make these records available to the data protection authority of your country.

The GDPR takes SMEs into account by including an exemption on recordkeeping for companies with less than 250 employees. If you have less than 250 employees, you only need to document processing activities that:

- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data.

For an example of such a documentation template, click here

10.4. Conclusion

The conclusions of both assessments are similar, but the Platform provides more details on the records of processing and documentation obligations (again combined with a link to the GDPR Handbook), whereas the Human Assessment provides a little more specific recommendations taking into account the business of Lawfirm.