An Approach for (Small) Businesses Seeking to Achieve Compliance With the General Data Protection Regulation

Version 2.1 / March 6, 2018

Grandite
Quebec (Canada)
www.grandite.com
info@grandite.com

Notice to the reader

The approach introduced with this document has been conceived from the practice to the practice. As such, it is subject to continuous development and improvement based on our experience, but first and foremost based on feedback that we receive from our clients.

If you have questions or comments, we welcome your feedback at info@grandite.com. Please refer to the version and date mentioned on the front page.

Also, we invite you to keep in touch with us via info@grandite.com to make sure that you have continued access to the latest version of this document.

Legal disclaimer

Nothing in this document should be construed as legal advice. This document as well as our tools and services in general are meant to suggest actionable items and help frame questions for your discussion with your legal counsel.

Introduction

The General Data Protection Regulation (GDPR) has been conceived and approved by the European Union to "protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data". It imposes obligations on every organization (or business person) **worldwide** that for business reason processes[1] Personal Data[2] of individuals who are (temporarily or permanently) in the European Union. This regulation enters force on May 25, 2018. Considering massive fines of up to EUR 20 million (or 4% of an organization's annual turnover – whichever is greater) and no further grace period, ignoring the GDPR is not an option. (If you want to verify whether the GDPR applies to your organization, take the short and simple self-assessment in the chapter "Does the GDPR apply to your organization?")

To comply with the GDPR, almost every organization needs to adjust their processing of Personal Data. The corresponding measures are determined by a multitude of factors which depend on the industry, the scale and categories of processed Personal Data, the number of employees, but first and foremost on the current status of processes and processing of Personal Data in the organization.

This document introduces an approach that is meant to particularly help small organizations to minimize time and expenses related to GDPR compliance without forcing them to dive into the legal details of the regulation from the start.

[1] 'processing' means "any operation or set of operations which is performed on Personal Data or 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".

[2] 'Personal Data' means "any information relating to an identified or identifiable natural person ('data subject'); 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".

Does the GDPR apply to your organization?

If your business is established in the European Union, the GDPR applies to your organization!

If your business is **not** established in the European Union, think of all categories / roles of individuals who have a business relationship with your organization such as

- Client (e.g. customer, patient, guest, passenger, member) / Contact person at a client organization
- Employee / freelancer
- Contact person at a supplier (e.g. marketing agency, printery)
- Contact person at a professional advisor (e.g. tax advisor, lawyer)
- Contact person at a cooperation / sales partner
- Natural person in any other business role

and ask yourself:

(A) How many individuals with any of the above roles are (temporarily or permanently) in the European Union?

(B) If individuals with any of the above roles move to a place within the European Union (temporarily or permanently), will your organization continue to be in business contact with them?

If you have answered the above questions (A) with "Zero" **and** (B) with "No", the GDPR does not apply to your organization, and no further action in this regard will be necessary! In any other case, your organization needs to prepare itself for the journey to GDPR compliance.

Approach to achieve GDPR compliance

The purpose of the GDPR is the protection of individuals' Personal Data.

Therefore, the first step is to find out and document who in your organization (and/or in an organization working on its behalf) processes which Personal Data how, why, where and when.

In the annex, you will find a questionnaire that contains the core set of questions that any organization of any industry and any size will face, if they seek to achieve GDPR compliance. We have compiled this set of questions from the provisions of the GDPR to liberate your organization from the obligation to dive into the legal details before you can even start.

This been said, the questionnaire addresses itself particularly (but not only) to small businesses that need a simple and size-appropriate solution.

Small businesses (e.g. organizations where less than 10 employees from business departments process Personal Data) can document the data flow in their organization along the lines of the questionnaire in a free / tabular format using office applications. For other businesses, we strongly recommend to employ a professional data and process modeling tool under our guidance while following the questionnaire.

Subsequent steps

Once you have completed the first step of documenting your organization's data flow based on the questionnaire, we offer you our professional services in

- Step 2: Analyze your documentation and clarify potentially additional questions with you
- Step 3: Assess existing risks / potential violations of the law
- Step 4: Derive measures to mitigate risks and to achieve GDPR compliance.

If you like to explore options how we can help you on your journey to GDPR compliance, please do not hesitate to contact us for further information at info@grandite.com .

Annex

Questionnaire to help you document the processing of Personal Data

Grandite

1. Individuals in the European Union

Approximately, how many individuals who have a business relationship with your organization are (temporarily or permanently) in the European Union?

Think of individuals in any of the following roles:

- Client (e.g. patient, guest, passenger, member, contact person at a client organization)
- Employee / freelancer
- Contact person at a supplier (e.g. marketing agency, printery)
- Contact person at a professional advisor (e.g. tax advisor, lawyer)
- Contact person at a cooperation partner
- Natural person in any other business role

2. Categories of Personal Data

Which (categories of) Personal Data are processed by your organization (and/or by an organization working on its behalf)?

List all categories and attributes of Personal Data that describe individuals and their roles (as of 1.). (The following categories and enumerations are examples and not necessarily exhaustive for your business! Check all that applies and add other!)

- Basic Personal Data

☐ name	☐ first name	☐ title	☐ street	☐ civic number
☐ postal code	☐ city	☐ country	☐ date of birth	☐ gender
☐ citizenship	☐ profession	☐ marital status	☐ eye color	☐ size
☐ weight	☐ …			

- Absolutely identifying Personal Data (i.e. data that can identify an individual worldwide)

☐ phone no.	☐ email address	☐ Skype ID	☐ Twitter handle	☐ Instagram handle
☐ Facebook page	☐ credit card no.	☐ IP address	☐ car license plate	☐ driver's license ID
☐ passport ID	☐ soc. security no.	☐ tax ID	☐ photo	☐ …

[continues on next page]

2. [continued] Which (categories of) Personal Data are processed by your organization (and/or by an organization working on its behalf)?

- Organization-related identifying Personal Data (i.e. data that can identify an individual in your organization or in any other business-related organization)

  ☐ customer no. ☐ user ID ☐ employee no.
  ☐ …

- (Other) sensitive Personal Data (that the GDPR explicitly mentions as such)

  ☐ user password ☐ racial or ethnic origin ☐ political opinions
  ☐ religious or philosophical beliefs ☐ trade union membership ☐ genetic data
  ☐ biometric data to uniquely identify a natural person ☐ health data
  ☐ data about sex life or sexual orientation
  ☐ data about criminal convictions and offences

3. Business Purposes

Which business purposes does your organization pursue?

Think of business purposes as a group of commercial processes e.g. such as

- Communicating
- Offering products / services
- Fulfilling contracts
- Performing marketing campaigns
- Conducting market research
- Administrating employees

If your organization offers a diverse range of unrelated products / services (e.g. selling food and car tires), the business purposes ought to be more specific and distinguished accordingly, e.g.

- Offering *food*
- Conducting marketing research *for tires*

4. Responsible Parties

4.1 Functional Units in Your Organization

Which functional units in your organization fulfill the business purposes (see 3.) with regard to individuals and their roles (as of 1.)?

List internal departments, positions and/or services that contribute to fulfilling the business purposes and process Personal Data; functional units such as

- Marketing
- Sales
- Customer Service
- Accounts Receivable
- Human Resources

For each functional unit, provide the following information:

- Name
- Country where related organisation is established

4.2 Data Processors on Your Organization's Behalf

Which external parties process Personal Data to help your organization fulfill its business purposes (see 3.)?

Think of all suppliers or services that your organization pays on a monthly or annual basis, e.g.

- Marketing agency
- SMTP service
- eMail & web server

For each external party, provide the following information:

- Name
- Country of establishment

Grandite

5. Business Processes

5.1 Business Data Stores

Which business stores for Personal Data exist in your organization (and/or an organization working on its behalf)?

List the various data stores (e.g. eMails, Contacts, Orders, Invoices) that include Personal Data or relate to it. Check the list against data stores processed in fulfillment of the business purposes (as of 3.)

Consider data stores used in daily operations as well as for archive / backup purpose.

For each data store, provide the following information:

- Name
- Categories of stored Personal Data
- Retention period for records in data store
- Databases (tables / files / directories) used for storage
- Country where related organisation is established

5.2 Processes

Using the above data stores, which processes involving Personal Data does your organization (and/or an organization on its behalf) perform for which purpose?

For each process, provide the following information:

- Name
- Business purpose (see 3.)
- MANUAL or AUTOMATED
- (if AUTOMATED) application software (used to perform the process in part or in total)
- Responsible party (see 4.)
- Country of processing
- Category / role of affected individuals (see 1.)
- Categories of Personal Data (see 2.) used from which data store
- Categories of Personal Data (see 2.) produced into which data store
- (Categories of) recipients of Personal Data (e.g. marketing agency, printery, tax advisor) and each recipient's respective country of establishment

6. Application Systems

6.1 Databases

Based on the data stores (see 5.), create an inventory of all related databases (tables / files / directories (including backup databases)) in your organization that contain Personal Data.

For each database (table / file / directory), provide the following information:

- Name
- Storage device type type (e.g. mobile device , laptop, desktop, server, mainframe, USB stick)
- Protection of access to data
  - Who has access to the database on its storage device?
  - How do authorized parties authenticate themselves (e.g. employee-specific user / password, company password, no protection)?
  - Are the Personal Data encrypted or anonymized?

If you discover databases that contain Personal Data and are not related to the previously found data stores (see 5.1), repeat step 5 to describe the omitted data stores and processes.

6.2 Application Software / Services

Based on the list of business processes (see 5.2), create an inventory of applications (processing Personal Data) that your organization has installed on user devices or servers or that it uses as a 3rd-party service.

For each software system or service, provide the following information:

- Name
- Device type (e.g. laptop, smartphone, tablet, server, Cloud)
- Protection of access to application software or service
  - Who has access to the application software or service on its processing device?
  - How do authorized parties authenticate themselves?
- Categories of Personal Data used from which databases (see 6.1)
- Categories of Personal Data produced into which databases (see 6.1)
- Does the application software or service encrypt data for the transfer from/to databases when using wireless networks (especially in public)?

If you discover application software that processes Personal Data and is not related to the previously found business processes (see 5.2), repeat step 5 to describe the omitted data stores and processes.

7. Devices

7.1 Computer

Create an inventory of all computers (e.g. mobile device , laptop, desktop, server, mainframe) used in your organization to work with Personal Data.

For each device, provide the following information:

- Name
- Device type (e.g. mobile device , laptop, desktop, server, mainframe)
- Authorized user (group)
- Installed application software systems
- Device security
  - Who has access to the device's direct surroundings (building / room / pocket)?
  - Who has access to the device itself (i.e. if switched on or activated from sleep modus, does device prompt for authentication)?
- Does the computer encrypt Personal Data, if they are transferred to/from databases using wireless networks (particularly in public areas)?

If you discover computers that are used to work with Personal Data and are not related to the previously found software systems or services (see 6.2), repeat step 6 to describe the omitted application software or services.

7.2 Storage Devices

Create an inventory of all devices used in your organization to store Personal Data (including backup devices).

For each device, provide the following information:

- Name
- Device type (e.g. mobile device , laptop, desktop, server, mainframe)
- Authorized user (group)
- Device security
  - Who has access to the device's direct surroundings (building / room / pocket)?
  - Who has access to the device itself (i.e. if switched on or activated from sleep modus, does device prompt for authentication)?

If you discover storage devices that are used to store Personal Data and are not related to the previously found databases (see 6.1), repeat step 6 to describe the omitted databases.