Deloitte.

EU General Data Protection Regulation (GDPR)
Nordic Data Retention Guideline and Policy

Nordic Data Retention Guideline and Policy

This document provides guidance to support personnel's overall understanding of data retention related matters, such as what are the factors to be considered when defining how long personal data can be retained.

The following represents high-level guidance and policy. Please consult with your local privacy lead for further support if needed.

- Each national practice shall define their respective data retention times for different types and categories of data. The retention times cannot be defined on a general level as each controller shall make their own reasoned and documented decisions, which are to a great extent based on local legislation.

- In general, the main categories of data the national practices process is related to client data (e.g. clients, potential clients, marketing & analytics), HR data (e.g. employees, externals, recruitment, payroll, health information etc.) and business partner related data.

- Attached to this guideline is a data retention master excel template, which can be utilized and localized when documenting specific data categories, the defined retention times and grounds for choosing them. The template is not meant to be all-inclusive, but provides an example of different types and categories of personal data the national practice might collect.

General

According to the GDPR data processing principles,
personal data should not be processed longer than is necessary for the purposes for which it is processed (obtained).

Recital 39 further defines that the period for which the personal data are stored needs to be limited to a strict minimum. In order to ensure that personal data are not kept longer than necessary**, time limits should be established by the controller** for erasure or for a periodic review.

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.*

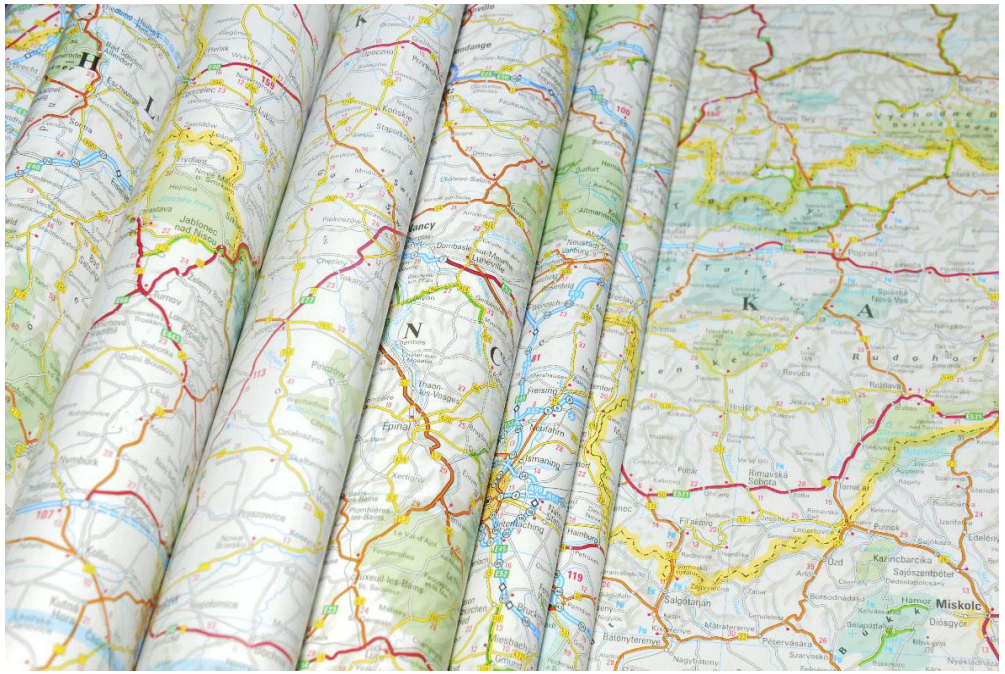
Processing *means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

Roles and responsibilities of Controller and Processor

As described in the previous slide, the time limits shall be established by the Controller.

In order to understand and determine, whether the personal data is processed as a Controller or as a Processor, it is necessary to understand the significant elements of both roles.

This guide comprises the parts *Definitions, Responsibilities* and *Operational* to help understand in which role the data is processed.



Controller: definition, responsibilities & operational

Definition

The Controller means the natural or legal person who determines the purposes and means of the processing of personal data.

The Controller always defines the frame of the data management, especially retention period, unless required to do so by Union or Member State law of which the Processor is subject to.

Characteristic for the Controller is that it decides what to do and how to do it. The Controller is sovereign and independent in it's performance, it cannot take instructions of what measures to be taken in the processing of the personal data.

Responsibilities

The Controller is primarily responsible for compliance with the data protection rules, and applicable national law for data protection.

The Controller must ensure to fulfill the requirements of the rules so lawfulness is achieved, which here means to be transparent in the processing of personal data and to inform the data subject when collecting personal data of the purpose of collecting and the storing period, or if that's not possible, the criteria used to determine that period. The Controller must also have appropriate technical and organizational measures to demonstrate that processing is performed in accordance with data protection rules, which means to keep formalized record of processing describing the storing policy.

Operational

Data Controllers enjoy greater practical discretion over the use of personal data and will be able to determine the purposes for which it may process, disclose personal data it collects or receives as part of client engagements, and in particular - decide for how long the personal data needs to be stored.

Controller: defining retention time 1/2

It is the responsibility of a controller to define how long certain personal data is retained and to inform the data subjects of it.

If it’s not possible to define a specific retention time for certain personal data, then the controller needs to define the criteria used to determine the retention time (e.g. certain employment data needs to be retained for certain specific amount of years after termination of employment due to regulatory requirements and this is the criteria based on which the retention time is calculated as it is not possible to define a specific retention time without knowing when a certain employment will be terminated).

GDPR does not provide defined retention times for personal data, but gives principles and guidelines, which shall be applied when retention time is defined. Also, when personal data is processed in accordance with the defined retention time it helps in keeping the processed data accurate and up to date.

Controller: defining retention time 2/2

For controller to be able to define retention time, they shall **first define and document the purposes of the processing** and ensure there is a lawful basis (see Privacy Policy or GDPR art 6) for processing personal data for these defined purposes**.**

Firstly, personal data should not be stored longer than necessary for the purposes it is processed. Therefore, when defining the retention time, it needs to be considered how long it is necessary to keep the personal data for the specific purposes it is obtained for. For instance, it is necessary to keep client data as long as the client relationship lasts but it also needs to be considered and defined how long the data is needed after the client relationship ends (take into consideration business needs and regulatory requirements).

It also needs to be taken into consideration how the lawful basis on which the personal data is processed affects to the retention time. For instance, when personal data is processed based on consent, the data subject can withdraw their consent at any time.

In addition, regulatory requirements regarding data retention shall be reviewed as legislation may require that the data is kept longer than would be necessary solely based on the purposes of the processing (e.g. laws relating to taxation, employment, bookkeeping, crimes and violations, sectoral legislation such as health or finance related etc.). It however needs to be considered what specific data the law requires to be retained.

- When the data is no longer processed for the purposes it was obtained for, but has to be further retained due to regulatory requirements, the data needs to be stored, but the access rights to this data should be limited.

It is important to document the defined retention times with reasoning for identified cases. This supports transparency compliance and drafting of Information Notices (information provided to data subjects, GDPR art 13-14), as well as guides the process and IT requirements. You can utilize the data retention master excel template attached to this guideline when documenting the defined retention times and grounds for choosing them.

Controller: processing and removing/anonymizing personal data in accordance with the defined retention times

Processing the personal data in accordance with the defined retention times

- There needs to be **assigned roles and responsibilities** regarding defining, documenting and reviewing the retention times and ensuring that personal data is removed as required.
- It is advisable to
  - Create a process to **track the retention times.**
  - Periodically review whether the retention times are applied accordingly in practice and whether the data is still needed for the purposes it was obtained for. Document the review.
  - Review whether the data is removed or anonymized as instructed. Document the review.
- **If the controller uses a processor** for the personal data processing activities, the controller shall have a contract in place with the processor and provide written instructions regarding the processing prior the processing can take place. The contract shall include, inter alia, a statement on the duration of the processing and whether the processor shall delete or return all the personal data to the controller after the end of provision of services relating to processing.

Removal or anonymization of personal data

- When it is no longer necessary to process personal data for the prior defined purposes for which the data was obtained and there is no other legal requirement to retain the data, the data shall be **securely removed** in compliance with member firms **data destruction policy** or **made anonymous** in line with the member firm's **data anonymization policy**.
  - The data needs to be removed or anonymized regarding all locations, e.g. servers (own & third party), desktops and local files, emails, devices, paper files, backups etc. If it is not yet technically possible to remove or anonymize personal data from an existing system determine the risks to the data subject stemming from this situation and define alternative measures to remediate that risk (e.g. if backups cannot be destroyed simultaneously with other personal data, at least restrict access rights to backups to strict minimum). Always document the analysis and reasoning. The target however has to be that in the future personal data can be removed or anonymized as required by the GDPR and local legislation.
- Data subjects may also request their data to be removed. These requests need to be evaluated case by case to determine whether the data can be removed or not (e.g. there is a legal requirement to keep the data).
- As anonymized data no longer is personal data it can be used for further processing purposes, such as analytics.

Processor: definition, responsibilities & operational

Definition

The Processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Characteristic for the Processor is that the Processor has no reason or cause to process the personal data other than on behalf of the Controller. The Processor is a separate legal entity with respect to the Controller, and the processing of personal data is solely on the Controllers behalf. The processing activity may be limited to a very specific task or context or may be more general and extended.

Responsibilities

The Processor is primarily responsible for compliance with the Data Processor Agreement rules, and applicable national law for data protection.

The Processor must ensure to have appropriate technical and organizational measures to demonstrate that processing is performed in accordance with the instructions from the Controller.

Operational

Data Processors are to be instructed by the Controller of what to do (purposes) and how to do it (means). The Processor may not decide any purposes for processing, nor any means unless such means are a reasonable way to achieve the purpose and of subordinate character.

The Processor needs a Data Processing Agreement that defines the processing, the personal data to be processed and the technical and organizational measures it can use for this. The agreement needs to state the conditions and requirements that the Processor may operate within. The Processor may not itself store any personal data, unless the European data protection regulation or national law states otherwise.

Processor: data retention

When processing personal data on behalf of a controller, the responsibilities between the parties must be clearly defined and understood. Overstepping the role of a processor by using the measures reserved for the processor leads to data processor having the responsibilities of a data controller in relation to that specific personal data and evaluation on whether that personal data is processed without lawful basis. Overstepping the role would also mean breaching the contract with the controller.

Below is listed few key points to consider **in relation to data retention** when acting as a processor.

Prior receiving or collecting (processing) personal data, ensure that:

- There is a GDPR compliant data processing agreement made with the controller (art 28 of the GDPR). The agreement shall govern, inter alia, duration, nature and purpose of the processing. **Retention time is defined by the controller**.
- Adequate written instructions from the controller regarding the processing activities are received.

When processing personal data on behalf of a controller, ensure that:

- Personal data processed on behalf of the controller is only processed in accordance with the controller's written instructions, unless otherwise required by the Union or Member State law (in which case the controller must be informed prior processing, unless informing is prohibited by the Union or Member State law).
- Personal data is not processed to any other purposes than to the ones defined by the controller (for instance, the data cannot be used for marketing purposes by the processor unless otherwise is agreed with the controller).

Process at the end of the provision of services relating to processing:

- Personal data processed on behalf of the controller shall be, **at the choice of the controller, deleted or returned** to the controller after the end of the provision of services relating to processing.
- Also the **existing copies shall be deleted**, unless Union or Member State law requires storage of the personal data.

Appendix – Data retention master excel template

The master excel template can be utilized when locally documenting specific data types and categories, the defined retention times for these and grounds for choosing them.

The template is not meant to be all-inclusive, but provides an example of different types and categories of personal data the member firm might obtain and process. The template can be modified to the needs and wanted level of accuracy of the member firm.

Please notice that the template is divided to function/service line specific spreadsheets.

Deloitte.