COFACE

Appendix 06

Privacy by Design, Privacy by Default and Data Protection Impact Assessment Procedure

Privacy by design, Privacy by Default and Data Protection Impact Assessment Procedure

Table of Content

1. Objectives and Scope of Application

1.1 Objectives

Privacy by design

Privacy by design is an approach that seeks to ensure protection for the privacy of individuals by integrating considerations of privacy issues from the very beginning of the development of products, services, business practices, and physical infrastructures.

Privacy by Default

Privacy by Default principle aims toward the implementation of appropriate technical and organisation measures for ensuring that, by default,

- only personal data which are necessary for each specific purpose of the processing are processed;
- the storage period is limited to fulfil the specific purpose;
- access to personal data is limited to fulfil the specific purpose;
- personal data is processed with the highest privacy protection available;
- all data protection-relevant settings, which can later be changed by the data subject itself, are initially deactivated or set to "no / less data processing" when they first go into operation.

This principle refers to the choices made by Coface Entities regarding any pre-existing configuration value or processing option that is assigned in a software application, computer program or device.

The Data Protection Impact Assessment

The Data Protection Impact Assessment is ruled in Art. 35 GDPR and based on the principles and checks formerly elaborated by the Article 29 Data Protection Working Party (WP29) in their Guideline WP 248 from 4 April 2017. The DPIA will be used to assess the impact on privacy of a project, and can concern a single or several data processing operations.

Commitment to the principles Privacy by design, Privacy by Default and Data Protection Impact Assessment

Coface acknowledges the principles Privacy by design, Privacy by Default and Data Protection Impact Assessment in order to

- be compliant with the law, as these principles and instruments are enforced by law in Art. 25 and Art. 35 GDPR ;
- respect the rights and freedom of natural person with regard to their personal data;

- reduce costs, as it is an empirical fact that the data processing that has passed the Privacy by Design, Privacy by Default and Data Protection Impact Assessment procedures have significantly lower running costs than those without.

Risks

Coface is aware of the risks that can arise without the application of Privacy by Design, Privacy by Default and, if indicated, Data Protection Impact Assessment, in particular:

- Lack of ability to demonstrate compliance and resilience of a data protection organization to authorities and to data subjects (as required by Art. 24 GDPR)
- Improper handling of data subject rights with subsequent complaints, involving authorities
- Increased number of data breaches
- Negative brand value
- Significantly increased costs for retroactive feature implementations.

1.2 Scope of Application

The policy applies to all Coface Project Managers, Application Owners, Product Owners, Process Owners and Sponsors of projects who are responsible for planning or modifying (new) applications, processes or products for processing personal data.

2. Procedure

The framework of Privacy by Design, Privacy by Default and Data Protection Impact Assessment consists in two key phases.

2.1. Privacy Screening and Application of Privacy by Design and Privacy by Default

(1) Privacy Screening

- The responsible project or application manager must complete a "Privacy Screening" scoring checklist (as currently available) that assigns risk points depending on the categories of data planned for processing, the presence of high-risk indicators, and the presence of particular technical environments that may lead to higher risks.

(2) Result check by GDPO and the application of Privacy by Design and Privacy by Default

- The GDPO checks the result for comprehensibility and consistency, taking into account the specific project. If necessary, the scoring is adjusted in consultation with the project manager.
- Based on the final score, the GDPO will determine if a DPIA must be conducted, and two conditions must be met:
    - The final score is 10 or higher, and
    - At least one of the high-risk indicators must be positive.
- If two high risk indicators are positive (which already leads to a final score of 10 or higher), a Data Protection Impact Assessment is mandatory.
- If there is no need to conduct a DPIA, the GDPO shall add a mandatory recommendation note on Privacy by Design and Privacy by Default to the project documents. This recommendation must address all or specific items in the “Privacy by Design and by default Repository” (as currently available) and indicate which Privacy by Design and Privacy by Default patterns need to be considered based on the nature of the project.

2.2 Data Protection Impact Assessment

Mandatory checks

If a project must be subjected to a data protection impact assessment, this must include the checks listed in Annex 1.

Stakeholders

The Data Protection Impact Assessment should be carried out by all stakeholders involved in the project:

- **The Project manager**, in charge of project implementation, remains the first point of contact regarding all technical requirements, stated by Privacy by Design and Privacy by Default
- **The Sponsor** reviews as a first level of defense the graduated risk assessment process. He will also present the project's progress to the Board.
- **The Data Protection Officer** (**GDPO**) is in charge of identifying high risk data privacy within the country/entity and confirming to the sponsor and the project manager whether a mandatory prior consultation to the supervisory authority is needed.
- **The Chief Information Security Officer** (**CISO**) will provide his expertise on IT Security topics and his knowledge of the IT Group architecture.
- **The Legal and Compliance departments** main responsibility is to support and to advise the project manager on particular topics where their expertise is required.

Application of Privacy by Design and by default

In all technical aspects of the project and in the mandatory Annex 1 reviews, the document "Privacy by Design and by default Repository" must again be considered as a mandatory primary source.

Depending on a project's risks to data subjects, the GDPO will decide whether the content of the Privacy by Design and by default Repository provides adequate protection or whether other privacy protection or enhancement measures need to be sought.

Documentation

All mandatory checks of appendix 1 and their results and considerations, including the final opinion of the GDPO, must be documented in

- the project documentation;
- the record of processing activities, maintained by the GDPO.

3. Appendix 1 – Data Protection Impact Assessment Mandatory Checks

Data Protection Impact Assessment – Mandatory checks (Articles of GDPR)

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
  - ☐ a functional description of the processing operation is provided; o the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
  - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));
- ☐ necessity and proportionality are assessed (Article 35(7)(b)):
  - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:

- ☐ measures contributing to the proportionality and the necessity of the processing on the basis of:
  - ☐ specified, explicit and legitimate purpose(s) (Article 5(1)(b));
  - ☐ lawfulness of processing (Article 6);
  - ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
  - ☐ limited storage duration (Article 5(1)(e));
- ☐ measures contributing to the rights of the data subjects:
  - ☐ information provided to the data subject (Articles 12, 13 and 14);
  - ☐ right of access and to data portability (Articles 15 and 20);
  - ☐ right to rectification and to erasure (Articles 16, 17 and 19);
  - ☐ right to object and to restriction of processing (Article 18, 19 and 21);
  - ☐ relationships with processors (Article 28);
  - ☐ safeguards surrounding international transfer(s) (Chapter V);
  - ☐ prior consultation (Article 36).

☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):

- ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
  - ☐ risks sources are taken into account (recital 90);
  - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
  - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
  - ☐ likelihood and severity are estimated (recital 90);
- ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);

☐ interested parties are involved:

- ☐ the advice of the GDPO is sought (Article 35(2));
- ☐ the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).