PRIVACY COMPANY

Data Protection by Design Framework

Governance:
Consists of privacy awareness within the organisation, internal policies, accountability measures, transparency to data subjects, cooperation with third parties and data processors (including data processing agreements)

Subjects **Actions**	**Anonymisation**	**1. Data minimisation** (art. 5(1)c)	**2. Pseudonymization** (art. 4(5))	**3. Encryption** (art. 6(4)e, 32(1)a)	**4. Access control** (art. 32(1), 5(1)f)	**5. Data protection by default** (art. 25(2))	**6. Deletion / retention terms** (art. 5(1)e)	**7. Facilitate rights of data subject** (art. 12-22)
Technical	Anonymise and aggregate (e.g. differential privacy)	Gather only data that is strictly necessary. Delete unnecessary data immediately.	Removal of all directly identifying elements, hashing, polymorphic pseudo-id.	e.g. public key encryption, disk encryption.	Digital data vault, physical access controls, logical access controls, authentication and authorisation.	Privacy friendly settings as default setting, transparent user interface, permission management.	Automated deletion, ‘flagging’ of data after end of retention term, sticky policies, data fading.	Privacy dashboard, communication / support. (art. 5(1)a)
Supportive Documents	No extra measures needed, no personal data involved	Description of purpose of data processing and list of necessary data.	Policy for separation of identifying data and other data or agreements.	Information security standards (art. 32(1)) and policies.	Authorisation matrix and logging, based on need to know and need to access.	Registration opt-in / opt-out and permissions.	Policy and overview of retention terms, management of e-waste (old documents and devices).	Privacy statement, policy for access requests, correction and deletion of personal data.
Alternative	If data is not anonymised follow the scheme	When possible anonymise / aggregate part of the data set, data fading.	Other security measures.	Other security measures (e.g. stand-alone server).	Access logs, with checks.	No alternative, just comply.	Anonymise and aggregate (archive if permitted).	No alternative, legal obligation.

Privacy Audit

A data protection impact assessment can test the requirements and illustrate what actions need to be taken (art. 35 GDPR).

Version 2.0 November 2017. The mentioned article numbers refer to the articles of the General Data Protection Regulation (Regulation 2016/679 (GDPR)). Data Protection by Design is required under the GDPR in article 25. In practice, Data Protection by Design is often referred to as Privacy by Design. Document has been compiled with care, but errors are possible. No rights can be derived from this publication. Always use the full text and / or consult a privacy expert. The most recent version of the Data Protection by Design Framework is available on www.privacycompany.eu.

Data Protection by Design Framework

Why this framework?

In the General Data Protection Regulation, Data Protection by Design is an explicit requirement for the processing of personal data (art. 25 GDPR). Data Protection by Design means that organisations pay attention to the protection of personal data when developing (new) products and services. The implementation of privacy enhancing measures in the early stages of development saves costs because it prevents more expensive interventions later on and it facilitates compliance earlier on. In practice, however, it is often unclear how compliance with the requirement of Data Protection by Design can be accomplished.

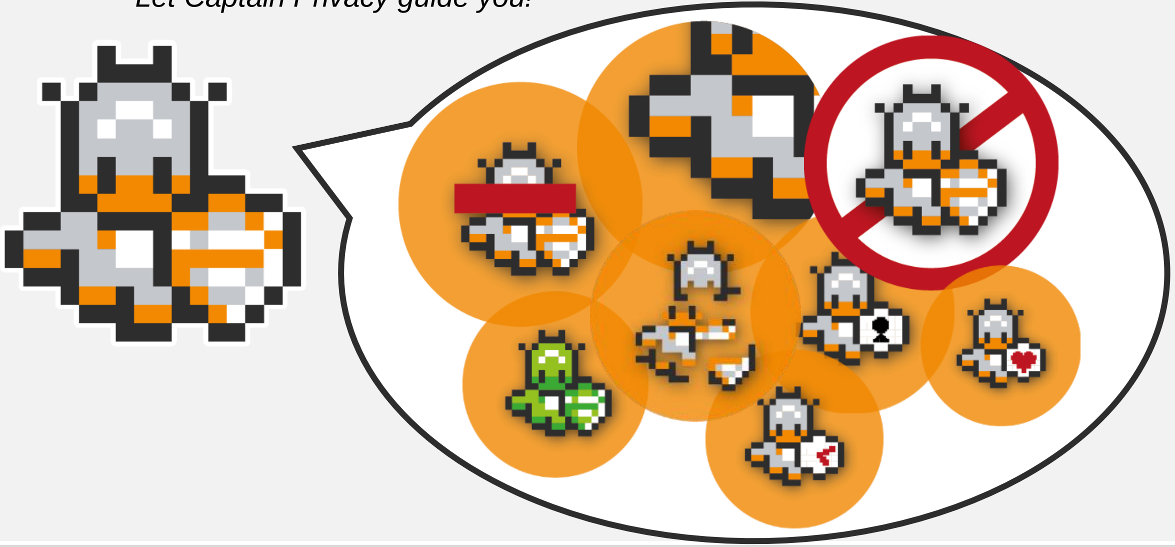
How to use this framework?

This framework provides a practical guide to Data Protection by Design based on several requirements that are spread over the General Data Protection Regulation.

Whenever possible, anonymised data should be used. If that is not an option, the other columns of the framework can be followed. In all cases there will be a technical/organisational component with supporting documentation or organisational measures. By using the framework and administering which aspects have been taken into account, an overview of the way your organisation complies with Data Protection by Design emerges.

Since there might be situations where not all technical aspects can be met, some alternative safeguards are suggested.

Let Captain Privacy guide you!



Incorporate this framework into your organisation

The framework can be used within an organisation as a part of the overall privacy and data governance. To safeguard compliance we suggest regular audits based on the framework. In addition, a data protection impact assessment can help make clear which measures are needed when new products or services are developed or new personal data processing activities are started.

Version 2.0 November 2017. The mentioned article numbers refer to the articles of the General Data Protection Regulation (Regulation 2016/679 (GDPR)). Data Protection by Design is required under the GDPR in article 25. In practice, Data Protection by Design is often referred to as Privacy by Design. Document has been compiled with care, but errors are possible. No rights can be derived from this publication. Always use the full text and / or consult a privacy expert. The most recent version of the Data Protection by Design Framework is available on www.privacycompany.eu.