What are DPAs expecting from Controllers to comply with Article 25 GDPR?

Felix Bieker, Marit Hansen

IPEN Workshop
Frankfurt (Main), 9 September 2016

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ipen

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Overview

(1) Data Protection by Design

(2) Data Protection by Default

(3)

Data Protection	What?	Really new?	Will it work?	Remarks
... by Design				
... by Default				

(4) Conclusions

(1) Data protection by design

Article 25 Data protection by design and by default

(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Not a new concept, t+o measures already in Article 17 DPD, but not enforceable

(1) Data protection by design

Article 25 Data protection by design and by default

(1) Taking into account

the state of the art,

the cost of implementation and

the nature, scope, context and purposes of processing as well as

the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing,

Many limiting conditions – not to be used as shabby excuses

the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Limiting conditions “state of the art and the cost of implementation”?

Identical wording in Art. 32 “Security of processing”

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and processing as well as the risks of varying likelihood and severity for rights and processing, the controller shall, both at the time of the determination of the r processing itself, implement appropriate technical and organisational measu designed to implement data-protection principles, such as data minimisation, necessary safeguards into the processing in order to meet the requirements c data subjects.

2. The controller shall implement appropriate technical and organisation only personal data which are necessary for each specific purpose of the proce to the amount of personal data collected, the extent of their processing, the pe In particular, such measures shall ensure that by default personal data are n intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may compliance with the requirements set out in paragraphs 1 and 2 of this Articl

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context a of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural controller and the processor shall implement appropriate technical and organisational measures to ensu security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification m referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirem in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the aut

Limiting conditions "state of the art and the cost of implementation"?

Not contained in Art. 24 GDPR: responsibility

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

(2) Data protection by default

Article 25 Data protection by design and by default

Unclear, but at least "purpose limitation" (Article 5 GDPR)

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Social network clause

(2) Data protection by default – cases

Article 25 Data protection by design and by default

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Let's discuss a few cases:
- Choice of payment model
- Storage location
- Tracking on the Internet
- Conference participation

Some hints in Recital 78 (I)

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.
[…]

Documentation required

[DE]: Strategien
[FR]: règles internes

Some hints in Recital 78 (I)

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.
Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. […]

- Data minimisation
- Early pseudony-misation
- Transparency
- Monitoring of data processing by the data subject
- Expandable security
- ...

Some hints in Recital 78 (II)

[…] When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.
The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

Producers are key:
- Infrastructures
- Platforms

Good way to exercise influence

Data protection by design – controller's perspective in 2016

Minimum:

- Low-key interpretation of the legal rules
- Documentation of internal policies and measures
- Awaiting requirements of supervisory bodies
- Awareness of responsibility (CEO; at best supported by Data Protection Officer)

For "optimum" on top:

- Acting proactively
- Knowing and extending solution space
- Striving for certification
- Implementing a data protection management system for entire lifecycle
- Interacting with other actors and disciplines for improving technologies and workflows

Possible fines according to Art. 83

Article 83 General conditions for imposing administrative fines

(1) Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

[…]

(4) Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

Summary: Data Protection by …

Data Protection	What?	Really new?	Will it work?	Remarks
… by Design	Implement t+o measures & integrate safeguards to meet reqs from GDPR: at best built-in data protection	No, but hardly ever enforced before	+ powerful mechanism – requires much knowledge at controller & DPA – "fig leaf approach" possible: do minimum and show documentation	Producers not directly addressed. Infra-structures, platforms, crucial
… by Default				

Summary: Data Protection by …

Data Protection	What?	Really new?	Will it work?	Remarks
… by Design	Implement t+o measures & integrate safeguards to meet reqs from GDPR: at best built-in data protection	No, but hardly ever enforced before	+ powerful mechanism – requires much knowledge at controller & DPA – "fig leaf approach" possible: do minimum and show documentation	Producers not directly addressed. Infra-structures, platforms crucial
… by Default	Basically implemented purpose limitation	No, but hardly enforced before	+ powerful mechanism – can be circumvented (e.g. by combination with nice features)	Narrow definition in the GDPR

(3) Conclusions

- Data protection by design and by default
  - Demanded by the General Data Protection Regulation
  - Now enforceable
- Important part of data protection management system
  - Controllers / processors have to consider alternatives
  - Have to provide documentation
  - Easier implementation with DPIA
- Infrastructures, platforms are crucial, must be standardised in accordance with data protection principles

Thank you for your attention

Felix Bieker
fbieker@datenschutzzentrum.de

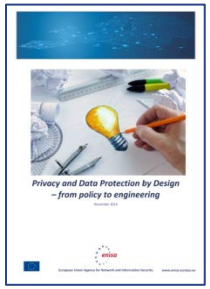
forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

iPen

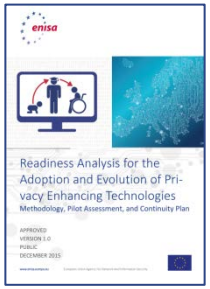
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

References

- https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design (2014)



- https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pets (2015)



- https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf (2015)[English translation in progress]

- Hansen/Jensen/Rost: Protection Goals for Privacy Engineering, Proc. 1st International Workshop on Privacy Engineering, IEEE (2015)

Funding Notice

Forum Privatheit
und selbstbestimmtes Leben
in der Digitalen Welt
(Privacy Forum)

partly funded by the
German Federal Ministry
of Education and Research

www.forum-privatheit.de