DIN EN 17529:2022-08 (E)

Data protection and p rivacy by design and by default

Contents

Page

European foreword 4

Introduction 5

1 Scope 6

2 Normative references 6

3 Terms, definitions and abbreviations 6
3.1 Terms and definitions 6
3.2 Abbreviated terms 7

4 General 7
4.1 Preparing the grounds for data protection and privacy by design and by default 7
4.2 Structure for disassembling product and service into applicable categories 8
4.2.1 Introduction 8
4.2.2 Product perspectives 9
4.2.3 Service elements 9
4.3 Self-declaration and levels of achievement 10

5 Privacy-aware development of products and services 12
5.1 Leadership and market intelligence 12
5.2 Preparation 13
5.3 Design 13
5.3.1 Determination of DPPbDD requirements 13
5.3.2 Development 14
5.3.3 Production and service provision 15
5.3.4 Release of products and services 15
5.4 Performance evaluation 15
5.5 Improvement 15

6 Data protection capability requirements on the design of products and services 15
6.1 Access 15
6.1.1 Access to data 15
6.1.2 Copy of data 16
6.2 Accountability 16
6.3 Accuracy 17
6.4 Data de-identification 18
6.5 Data minimization 19
6.6 Data portability 20
6.7 Confidentiality 21
6.8 Erasure 23
6.9 Consent and Children 24
6.9.1 Determination of user age 24
6.9.2 Configurable children age threshold 24
6.10 Information security 25
6.10.1 Unauthorized or unlawful processing 25
6.10.2 Data loss 28
6.10.3 Information protection targets 29
6.10.4 Restore 29
6.11 Lawfulness 30

6.11.1 Data disclosure **30**
6.11.2 Consent **30**
6.12 Objection to processing **31**
6.13 Automated decision making **32**
6.14 Restriction of processing **32**
6.15 Storage limitation **33**
6.16 Transparency **34**
6.16.1 Information **34**
6.16.2 Record of processing activities **37**

7 Requirements to the self-declaration of privacy-aware design **38**
7.1 Process requirements **38**
7.1.1 Preparation based on the product perspective and service element requirements **38**
7.1.2 Additional considerations related to DPIAs **38**
7.1.3 Determination of the level of achievement **38**
7.2 Self-declaration statement **39**

Annex A (informative) **Applicability mapping between Clause 6 requirements and perspectives or elements** **41**

Annex B (informative) **Approach for a specification** **53**

Annex C (informative) **Guidelines related to EN ISO 9001** **55**

Annex ZA (informative) **Relationship between this European Standard and the data protection by design and by default requirements of Regulation EU 2016/679 aimed to be covered** **60**

Bibliography **62**