

DIN 66398:2016-05 (E)

Guideline for development of a concept for data deletion with derivation of deletion periods for personal identifiable information

Contents

Page

Foreword	5
Introduction	6
1 Scope	9
2 Terms and definitions	9
3 Abbreviations	13
4 Basics of a deletion concept	13
4.1 General	13
4.2 Application of relevant legal requirements	15
4.3 What is the meaning of "deletion"?	16
4.4 One deletion rule for every type of PII	16
4.4.1 Types of PII	16
4.4.2 Deletion rules	16
4.4.3 Retention period and regular deletion period	17
4.4.4 Handling of non-productive pools of data: Archives and backup copies	19
4.4.5 Standard deletion periods, starting points, deletion rules and deletion classes	19
4.4.6 Deletion in special situations	20
4.5 Document structure in the deletion concept	20
5 Defining types of PII	21
5.1 Pools of data, purposes and types of PII	21
5.2 Systematic collection of types of PII	22
5.3 Design criteria for the definition of types of PII	22
5.3.1 Guidance from the practice	22
5.3.2 Orientation towards the legal provisions	22
5.3.3 Orientation towards the PII principals	22
5.3.4 Orientation towards purposes of data processing	23
5.3.5 Orientation towards the sensitivity of data	23
6 Specification of deletion periods	23
6.1 Using standard deletion periods	23
6.2 Period specifications	24
6.2.1 Procedure and standard deletion periods	24
6.2.2 Methods for the period derivation	26
6.2.3 Specification of a catalogue of standard deletion periods	27
6.3 Specifics for period specifications	27
6.3.1 Regular deletion periods and deviations	27
6.3.2 Period changes by compaction with alteration of the type of PII	27
6.3.3 Altering the type of PII for special cases with longer periods of use	28
6.3.4 Exceptions to regular processes: Suspension of the deletion	28
6.3.5 Deviations from standard deletion periods for backup copies	28
7 Deletion classes	29
7.1 Abstract starting points -- abstract deletion rules	29
7.2 Matrix of the deletion classes	30
7.3 Types of PII, deletion classes and deletion rules	30

8	Requirements for implementation of deletion rules	32
8.1	Structure and contents of the requirements for implementation	32
8.1.1	Relationship between the document "Deletion rules" and requirements for implementation	32
8.1.2	of requirements for implementation	33
8.2	Requirements for implementation for cross-sectional areas	34
8.3	Requirements for implementation for individual IT systems	36
8.4	Individual measures for the deletion of pools of data	38
8.4.1	General guidance for requirements for implementation for individual measures	38
8.4.2	Requirements for implementation for data objects in everyday business life	38
8.4.3	Requirements for implementation for pools of data in regular manual processes	39
8.4.4	Requirements for implementation for copies of personally identifiable information for special uses	40
8.4.5	Requirements for implementation for remainders in IT systems	41
8.4.6	Requirements for implementation for inadmissible pools of data containing PII	42
8.5	Requirements for implementation for service providers	43
9	Operational and organizational structure: Responsibility and processes for the deletion of personally identifiable information	44
9.1	Organizational embedding	44
9.2	Management of the organization	44
9.3	Role of the privacy authority of the organization	45
9.3.1	Responsibility for the document maintenance	45
9.3.2	Processes under the responsibility of the privacy authority of the organization	45
9.3.3	Release participations	45
9.4	Responsibility for requirements for implementation	46
9.4.1	Organizational units with responsibility for pools of data with personally identifiable information	46
9.4.2	Additional tasks in connection with requirements for implementation	47
9.4.3	Organizational unit change management	48
9.4.4	Organizational units with responsibility for the control of service providers	48
9.5	General reporting obligations	48
	Annex A (informative) Guidance for a project "Deletion concept"	49
	Annex B (informative) Guidance for the anonymization of personally identifiable information	52
	Annex C (informative) Guidance on provisions for the security of deletion mechanisms	54
	Annex D (informative) Guidance for restriction of processing for pools of data	56
	Bibliography	58
	Tables Table 1 -- Abbreviations used	13
	Figure 1 -- Example of period sections for an 'order' in the deletion concept	18
	Figure 2 -- Possible standard deletion periods of a telecommunications service provider	27
	Figure 3 -- Exemplary matrix of deletion classes for a telecommunications service provider	30
	Table 2 -- Recommendations for the maintenance responsibility and release rules of the document "Deletion rules"	31
	Figure 4 -- Relationship between the document "Deletion rules" and requirements for implementation	32
	Table 3 -- Recommendations with regard to the responsibility for maintenance and to the rules for releasing the "Requirements for implementation for cross-sectional areas"	36
	Table 4 -- Recommendations with regard to the responsibility for maintenance of the "Inventory of data storage media"	36

Table 5 -- Recommendations for the maintenance responsibility and release rules of the "Requirements for implementation for individual IT systems"	38
Table 6 -- Recommendations for the maintenance responsibility and release rules of the "Requirements for implementation for data objects in everyday business life"	39
Table 7 -- Recommendations for the maintenance responsibility and release rules of the "Requirements for implementation for pools of data in regular manual processes"	39
Table 8 -- Recommendations for the maintenance responsibility and release rules of the "Requirements for implementation for copies of personally identifiable information for special uses"	40
Table 9 -- Recommendations for the maintenance responsibility and release rules of the "Overview on exceptional rules"	41
Table 10 -- Recommendations for the maintenance responsibility and release rules of the "Requirements for implementation for remainders in IT systems"	42
Table 11 -- Recommendations for the maintenance responsibility and release rules of the "Requirements for implementation for inadmissible pools of data containing PII"	43
Table 12 -- Recommendations for the maintenance responsibility and release rules of the "Requirements for implementation for service providers"	44
Table 13 -- Recommendations for the maintenance responsibility of the "Overview on IT systems and other pools of data containing PII"	47
Table 14 -- Recommendations for the maintenance responsibility of the "Needs for action from requirements for implementation"	48
Figures Figure 1 -- Example of period sections for an `order' in the deletion concept	18
Figure 2 -- Possible standard deletion periods of a telecommunications service provider	27
Figure 3 -- Exemplary matrix of deletion classes for a telecommunications service provider	30
Figure 4 -- Relationship between the document "Deletion rules" and requirements for implementation	32
Figure A.1 -- Subdivision into project phases	50