

DIN SPEC 4997:2020-04 (E)

Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English

Inhalt	Seite
Foreword	4
Introduction.....	6
1 Scope.....	7
2 Normative references	7
3 Terms and definitions.....	7
4 Symbols and abbreviations.....	12
5 Personal data	12
5.1 Personal data in general	12
5.2 Defining Personal data	12
5.3 Practical consideration about identifiability and identifiers	13
5.4 Identifying personal data in a blockchain context	15
5.5 Requirement of an Anonymity assessment	17
6 GDPR awareness.....	18
7 Principles of data protection and their risks from the perspective of Privacy by Design	21
7.1 General.....	21
7.2 Fundamental principles of data protection	22
7.3 Assessing the risk of processing personal data	24
7.3.1 General.....	24
7.3.2 Traditional risk assessment methodology.....	24
7.3.3 Risk assessment from the perspective of data protection law	26
7.4 Initial assessment of risks in a blockchain application	26
8 Mitigating the risk of processing and decreasing identifiability through technical measures.....	26
8.1 General.....	26
8.2 Technical measures	28
8.2.1 Categories of technical measures of data protection:.....	28
8.2.2 Techniques to improve data protection or mitigate risk of processing	29
8.3 Architectural blueprint for an IT system processing personal data utilizing a blockchain-based tamper-proof access log.....	31
8.3.1 General.....	31
8.3.2 DLT-based tamper-proof access log	33
8.3.3 Decentralized Personal Data Storage	34
8.3.4 Consent Management System.....	34
Annex A (normative) Recommendations for handling personal data in blockchain applications.....	35
Annex B (normative) GDPR awareness.....	36
B.1 General.....	36
B.2 Contollership and processors in a BC/DLT-system.....	36
B.3 Right to Erasure (art. 17 GDPR)	38
B.4 Justifications for immutability	38
B.5 Right to rectification.....	39
B.6 Data Portability (art. 20 GDPR)	40
B.7 Processing Agreements between Controllers and Processors	40

B.8	Household exemption	40
B.9	Identification requirements for controllers	41
B.10	Personal data vs Privacy enhancing technology (ISO/IEC 27018)	41
B.11	Automated decision making (art. 22 GDPR)	41
B.12	Staff training + obligation (art. 29 and art. 32(4) GDPR)	42
B.13	Data protection impact assessment (art. 35 GDPR)	42
B.14	Documentation + record of processing activities (art. 5(2) GDPR)	43
B.15	Right to information (art. 13, 14 GDPR)	43
B.16	Data minimization (Art. 5 (1) lit. c GDPR)	44
B.17	Data Protection Officer (Art. 37 (1) GDPR)	45
B.18	Privacy by Design & Default	45
B.19	Notification of data breach to authorities and data subjects (art. 33/34 GDPR)	45
B.20	Right of access by the data subject	46
B.21	Right to object (art. 21 GDPR)	47
B.22	Transfer to third countries	47
Annex C (normative) Questionnaire: Extent of the implementation of data protection principles in a DLT, in particular blockchain solution		49
Annex D (informative) Summary of applicable risk assessment methodologies		52
Annex E (informative) Additional Information on Technical Measures		53
Bibliography		54