

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