DIN EN 17529:2022-08 (D)

Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen; Deutsche Fassung EN 17529:2022

Inhalt

Seite

Europäisches Vorwort ... 5

Einleitung ... 6

1 Anwendungsbereich ... 7

2 Normative Verweisungen ... 7

3 Begriffe und Abkürzungen ... 7

4 Allgemeines ... 8
4.1 Grundlagen für den Datenschutz und den Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen ... 8
4.2 Struktur für die Zerlegung von Produkten und Diensten in anwendbare Kategorien ... 10
4.2.1 Einleitung ... 10
4.2.2 Produktperspektiven ... 10
4.2.3 Dienstelemente ... 11
4.3 Eigenerklärung und Zielerreichungsgrade ... 12

5 Datenschutzbewusste Entwicklung von Produkten und Diensten ... 14
5.1 Führung und Marktkenntnis ... 14
5.2 Vorbereitung ... 14
5.3 Gestaltung ... 15
5.3.1 Bestimmung der Anforderungen für DSTV ... 15
5.3.2 Entwicklung ... 16
5.3.3 Produktion und Diensterbringung ... 16
5.3.4 Freigabe von Produkten und Diensten ... 16
5.4 Leistungsbewertung ... 17
5.5 Verbesserung ... 17

6 Anforderungen an die Datenschutzfähigkeit bei der Gestaltung von Produkten und Diensten ... 17
6.1 Zugang ... 17
6.1.1 Zugang zu Daten ... 17
6.1.2 Kopie der Daten ... 18
6.2 Verantwortlichkeit ... 18
6.3 Genauigkeit ... 19
6.4 Entpersonalisierung von Daten ... 20
6.5 Datenminimierung ... 21
6.6 Datenübertragbarkeit ... 22
6.7 Vertraulichkeit ... 23
6.8 Löschung ... 25
6.9 Einwilligung und Kinder ... 26
6.9.1 Bestimmung des Benutzeralters ... 26
6.9.2 Konfigurierbare Altersgrenze für Kinder ... 27
6.10 Informationssicherheit ... 27
6.10.1 Unbefugte oder unrechtmäßige Verarbeitung ... 27
6.10.2 Datenverlust ... 30
6.10.3 Ziele des Informationsschutzes ... 31
6.10.4 Wiederherstellung ... 32
6.11 Rechtmäßigkeit ... 32
6.11.1 Datenoffenlegung ... 32

6.11.2 Einwilligung 33
6.12 Widerspruch gegen die Verarbeitung 33
6.13 Automatisierte Entscheidungsfindung 34
6.14 Einschränkung der Verarbeitung 34
6.15 Speicherbegrenzung 35
6.16 Transparenz 37
6.16.1 Informationen 37
6.16.2 Verzeichnis von Verarbeitungstätigkeiten 39

7 Anforderungen an die Eigenerklärung datenschutzbewusster Gestaltung 40
7.1 Prozessanforderungen 40
7.1.1 Vorbereitung basierend auf den Anforderungen der Produktperspektive und des Dienstelements 40
7.1.2 Zusätzliche Überlegungen im Zusammenhang mit DSFA 40
7.1.3 Bestimmung des Zielerreichungsgrads 41
7.2 Aussage zur Eigenerklärung 42

Anhang A (informativ) Zuordnung der Anwendbarkeit zwischen den Anforderungen und Perspektiven oder Elementen von Abschnitt 6 43
A.1 Allgemeines 43

Anhang B (informativ) Ansatz für a Spezifikation 55
B.1 Allgemeines 55
B.2 Datenschutz 55
B.3 Privatsphäre 55
B.4 Datenschutz und Privatsphäre durch Technikgestaltung 56
B.5 Datenschutz und Privatsphäre durch datenschutzfreundliche Voreinstellungen 56

Anhang C (informativ) Leitfaden in Bezug auf EN ISO 9001 57
C.1 Allgemeines 57
C.2 Kontext der Organisation 57
C.2.1 Verstehen der Organisation und ihres Kontextes 57
C.2.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien 57
C.2.3 Festlegen des Anwendungsbereichs des Qualitätsmanagementsystems 57
C.2.4 Qualitätsmanagementsystem und seine Prozesse 57
C.3 Führung 57
C.3.1 Führung und Verpflichtung 57
C.3.2 Politik 57
C.3.3 Organisatorische Rollen, Verantwortlichkeiten und Befugnisse 58
C.4 Planung 58
C.4.1 Maßnahmen zum Umgang mit Risiken und Chancen 58
C.4.2 Qualitätsziele und Planung zu deren Erreichung 58
C.4.3 Planung von Änderungen 58
C.5 Unterstützung 58
C.5.1 Ressourcen 58
C.5.2 Kompetenz 58
C.5.3 Bewusstsein 58
C.5.4 Kommunikation 58
C.5.5 Dokumentierte Informationen 58
C.6 Betrieb 59
C.6.1 Betriebliche Planung und Steuerung 59
C.6.2 Anforderungen an Produkte und Dienste 59
C.6.3 Gestaltung und Entwicklung von Produkten und Diensten 59
C.6.4 Steuerung von extern bereitgestellten Prozessen, Produkten und Diensten 59
C.6.5 Produktion und Diensterbringung 59
C.6.6 Freigabe von Produkten und Diensten 60
C.6.7 Steuerung fehlerhafter Ausgaben 60
C.7 Leistungsbewertung 60
C.7.1 Überwachung, Messung, Analyse und Bewertung 60
C.7.2 Internes Audit 60

C.7.3 Managementbewertung 60
C.8 Verbesserung 61
C.8.1 Allgemeines 61
C.8.2 Nichtkonformität und Korrekturmaßnahmen 61
C.8.3 Fortlaufende Verbesserung 61
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den Anforderungen der abzudeckenden Verordnung EU 2016/679 an den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen 62
Literaturhinweise 64