DIN SPEC 27557:2019-08 (D)

European Cloud Service Data Protection Controls Catalogue

Inhalt

Seite

Vorwort 4

1 Anwendungsbereich 5

2 Normative Verweisungen 5

3 Begriffe 5

4 Symbole und Abkürzungen 6

5 Elemente dieser DIN SPEC 7

6 Schutzklassen 7
6.1 Allgemeines 7
6.2 Das Schutzklassenkonzept 7
6.3 Die Schutzklassen 8

7 Nichtanwendbarkeit von Kriterien 14

8 Kriterien und Umsetzungsempfehlungen für die Auftragsverarbeitung 14
8.1 Rechtsverbindliche Vereinbarung zur Auftragsverarbeitung 14
8.1.1 Allgemeines 14
8.1.2 Wirksame und eindeutige Vereinbarung zwischen Cloud-Anbieter und Cloud-Nutzer (Art. 28 Abs. 3 DSGVO) 15
8.2 Rechte und Pflichten des Cloud-Anbieters 20
8.2.1 Sicherstellung der Datensicherheit durch geeignete TOM nach dem Stand der Technik 20
8.2.2 Sicherstellung der Weisungsbefolgung (Art. 28 Abs. 3 Satz 2 lit. a; 29 DSGVO) 33
8.2.3 Hinweispflicht des Cloud-Anbieters 34
8.2.4 Sicherstellung der Vertraulichkeit beim Personal (Art. 28 Abs. 3 Satz 2 lit. b DSGVO) 35
8.2.5 Unterstützung des Cloud-Nutzers bei der Wahrung der Betroffenenrechte 36
8.3 Datenschutz-Managementsystem des Cloud-Anbieters 41
8.3.1 Allgemeines 41
8.3.2 Datenschutz-Managementsystem 41
8.4 Datenschutz durch Systemgestaltung und datenschutzfreundliche Voreinstellungen 46
8.4.1 Datenschutz durch Systemgestaltung (Art. 25 Abs. 1 DSGVO i.V.m. Art. 5 Abs. 1 lit. f DSGVO) 46
8.4.2 Datenschutz durch Voreinstellungen (Art. 25 Abs. 2 DSGVO) 46
8.5 Subauftragsverarbeitung 47
8.5.1 Allgemeines 47
8.5.2 Subauftragsverhältnisse 47
8.6 Datenverarbeitung außerhalb der EU und des EWR 50
8.6.1 Datenübermittlung 50

9 Kriterien und Umsetzungshinweise für Verarbeitung als Verantwortlicher 51
9.1 Allgemeines 51
9.2 Der Cloud-Anbieter als Verantwortlicher 51
9.2.1 Sicherstellung der Datenschutzgrundsätze (Art. 5 Abs. 1 und 2 i.V.m. Art. 24 DSGVO) 51
9.2.2 Rechtsgrundlage für die Datenverarbeitung (Art. 6 Abs. 1 UAbs. 1 lit. b. sowie lit. c i.V.m. Abs. 2 DSGVO) 52
9.2.3 Gewährleistung der Datensicherheit durch geeignete TOM nach dem Stand der Technik 53
9.2.4 Wahrung von Betroffenenrechten 61
9.2.5 Verpflichtung zur Vertraulichkeit (Art. 5 Abs. 1 lit. a, Abs. 2 i.V.m. Art. 24 Abs. 1 DSGVO) 63
9.2.6 Meldung von Datenschutzverletzungen (Art. 33 Abs. 1, 3 und 5 DSGVO) 64

9.2.7 Benachrichtigung der betroffenen Person bei Datenschutzverletzungen (Art. 34 Abs. 1 und 2 DSGVO) 64
9.2.8 Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 1 DSGVO) 65
9.2.9 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen 65
9.2.10 Auftragsverarbeitung des Cloud-Anbieters 66

Literaturhinweise 70