Law | GDPR:Obligations

O.21 Security of Processing

Authors: David Gabel

Last update: 2021-06-25 11:11:48 | By: David Gabel

Created at: 2021-05-27 21:55:58

[Translation coming soon]

Die DS-GVO verpflichtet den Verantwortlichen (und den Auftragsverarbeiter) zur Gewährleistung der "Sicherheit der Daten" bzw. der "Sicherheit der Verarbeitung". An zentraler Stelle - in Art. 32 DS-GVO - wurde der im Datenschutzrecht bisher gebräuchliche Begriff "Datensicherheit" durch den Begriff "Sicherheit der Verarbeitung" abgelöst (*Jandt*, in: **Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 1. Aufl. 2020, 17.30**).

Datensicherheit hat das technische Ziel, Daten in ausreichendem Maße gegen Verlust, Manipulation und andere Bedrohungen zu sichern. Seine konkrete Ausgestaltung findet die Datensicherheit in der DS-GVO in zwei Normen. Beide verpflichten zur Umsetzung von technischen Maßnahmen zur Gewährleistung der Anforderungen der DS-GVO.

> ***Art. 25 I (Datenschutz durch Technikgestaltung):*** *"Unter Berücksichtigung [...] der [...] Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche [...] geeignete technische und organisatorische Maßnahmen [...], die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.*

> ***Art. 32 (Sicherheit der Verarbeitung):*** "Unter Berücksichtigung [...] des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein: [...]"

Ganz konsequent ist die DS-GVO bei der Ablösung von "Datensicherheit" durch "Sicherheit der

Verarbeitung" nicht. Der Begriff "Datensicherheit" findet noch verschiedentlich Erwähnung:

Art. 5 I f: *"Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet [...]."*

Überschrift von Kapitel IV, Abschnitt 2: *"Sicherheit personenbezogener Daten".*

Art. 47 II d: *Als Mindestinhalt verbindlicher interner Datenschutzvorschriften werden dort "Maßnahmen zur Sicherstellung der Datensicherheit" aufgeführt.*

EG 39 S. 12: *"*Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist [...]."

EG 83 S. 3: *"Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden [...]."*

Die "Sicherheit der Verarbeitung" findet Erwähnung in:

Art. 4 Nr. 12: *"Verletzung des Schutzes personenbezogener Daten" wird definiert als "eine Verletzung der Sicherheit, die [...] zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt [...]"*

Art. 32 Sicherheit der Verarbeitung

Art. 32 I d: *"*ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung"

Art. 35 IX: *"Sicherheit der Verarbeitungsvorgänge"*

Art. 40 II h: *"*die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32"

EG 81 S. 1: *"Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter [...] vorzunehmende Verarbeitung eingehalten werden, sollte ein Verantwortlicher [...] nur Auftragsverarbeiter heranziehen, die [...] hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die* ***Sicherheit der Verarbeitung*** *– getroffen werden [...].*

EG 83 S. 1: *"Zur Aufrechterhaltung der* ***Sicherheit*** *und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen."*

Auch **§ 22 II Nr. 9 BDSG** spricht von "Sicherheit der Verarbeitung". Von Sicherheitsvorkehrungen, Sicherheitsvorschriften bzw. Sicherheitsfunktionen sprechen Art. 34 III a, 35 VII d, 45 II a und EG 78 S. 3, 88 S. 1, 94 S. 1 DS-GVO.

Als allgemeine Schutzziele der Sicherheit in der Informationstechnik sind anerkannt (vgl. **§ 2 II BSIG**):

? *Vertraulichkeit der Daten* ***[Kachel B.15]***

? *Integrität der Daten* ***[Kachel B.17]***

? *Verfügbarkeit der Daten* ***[Kachel B.18]***

? *Als zusätzliches Schutzziel nennt die DS-GVO noch die Belastbarkeit der Systeme und Dienste* ***[Kachel P.25]***