EU-Datenschutz-Grundverordnung – Nr. 5 Datenschutz und Datensicherheit

Vorbemerkungen

Die EU-Datenschutz-Grundverordnung (DS-GVO) verknüpft Datenschutz und Datensicherheit eng miteinander. Schutz und Technik sind nicht nur bei den technisch-organisatorischen Maßnahmen miteinander verbunden, wie es bisher bei § 9 BDSG und seiner Anlage der Fall war. Die DS-GVO verlangt Datensicherheitsmaßnahmen, die geeignet sind, das Schutzniveau zu gewährleisten, das dem Risiko der Datenverarbeitung für die Rechte und Freiheiten des Betroffenen angemessen ist. Hierbei ist der Stand der Technik angemessen zu berücksichtigen. Es bedarf also einer stetigen Anpassung der Maßnahmen. Zu prüfen ist, ob ein IT-Sicherheitsmanagement notwendig ist.

Welche Schutzziele sind einzuhalten?

(Die Zuordnung erfolgt zur Konkretisierung unter Berücksichtigung der bisher in § 9 BDSG und seiner Anlage vorgenommenen Definitionen)

1. Vertraulichkeit durch
   - Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)

   - Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle)

   - Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle)

   - Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungsgebot).

2. Integrität durch
   - Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle)

- Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle/Verarbeitungskontrolle)

- Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können (Dokumentationskontrolle)

- Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

3. Verfügbarkeit und Belastbarkeit (Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten) durch
   - Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).

   - Maßnahmen die gewährleisten, dass technische Systeme, bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO).

Wie ist der Schutzbedarf festzustellen?

Hierfür werden üblicherweise die drei Schutzklassen „normal“, „hoch“ und „sehr hoch“ verwendet. Diese Zuweisung zu den Schutzklassen muss nicht nur für personenbezogene Daten gelten, sondern kann für alle unternehmensrelevanten Informationen verwendet werden.
Die Klassifizierung „normal“ gilt z. B. für alle internen Datenverarbeitungen bzw. für Daten, die aus allgemein zugänglichen Quellen stammen. Das Risiko für den Betroffenen ist tolerabel.
„Hoch“ ist ein Schutzbedarf für Daten, die einen gewissen Vertraulichkeitsgrad erfüllen müssen, weil eine – erhebliche - Beeinträchtigung der Rechte des Betroffenen möglich ist.
Ein „sehr hohes“ Schutzniveau ist zu gewährleisten, wenn eine besonders bedeutende Beeinträchtigung zu befürchten ist.

Die **Risikobewertung** muss also abwägen, wie wahrscheinlich ein Schadenseintritt ist und welchen Schaden er mit welchen Auswirkungen beim Betroffenen anrichten könnte.

Welche Maßnahmen müssen ergriffen werden?

Die technischen und organisatorischen Maßnahmen müssen im Verhältnis zum Risiko stehen. Hierbei sind folgende Punkte zu berücksichtigen:

- Geeignetheit der Maßnahmen
- Stand der Technik
- Kosten der Implementierung
- Aufwand

Nach der DS-GVO gibt es einige Maßnahmen wie:

- Pseudonymisierung
- Verschlüsselung
- Die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicherzustellen

- Die Verfügbarkeit und den Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall schnell wiederherzustellen
- Ein Verfahren einzurichten, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technisch-organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gewährleistet
- Sicherstellung, dass die Mitarbeiter, die personenbezogenen Daten verarbeiten, dies nur entsprechend ihrer Aufgabenerfüllung auf Anweisung des Verantwortlichen tun.

Im Rahmen der Rechenschaftspflicht nach Art 5 DS-GVO müssen die Risikobewertung und die daraufhin passend ergriffenen Maßnahmen dokumentiert werden.

Weitere technische Maßnahmen

Bereits im Vorfeld von Anwendungen zur Verarbeitung personenbezogener Daten müssen die Aspekte eines Datenschutzes durch Technikgestaltung (privacy by design) oder durch datenschutzfreundliche Voreinstellungen (privacy by default) berücksichtigt werden. Damit ist dem Grundsatz der Datenminimierung (Art. 5 DS-GVO) zu entsprechen. Schon bei der Beschaffung von IT-Lösungen muss geprüft werden, wie diese Anforderungen umgesetzt werden können. Anonymisierung, Pseudonymisierung, Einschränkung der Verarbeitung (Sperrung) oder Löschung von Daten können hier Maßnahmen sein.
Auch diese Überlegungen bzw. Maßnahmen sind zu dokumentieren.

Stand: Juni 2017

Mitgliedsunternehmen der IHK Bonn/Rhein-Sieg erteilt weitere Information:

Detlev Langer, Tel: 0228/2284 134, Fax: 0228/2284-222, Mail: langer@bonn.ihk.de
Tamara Engel, Tel: 0228/2284 208, Fax: 0228/2284-222, Mail: engel@bonn.ihk.de
Bonner Talweg 17, 53113 Bonn, www.ihk-bonn.de

Verantwortlich: Deutsche Industrie- und Handelskammertag DIHK, Breite Str. 29, 10178 Berlin, www.dihk.de