Änderungen zur neuen DSGVO-
Technischen & organisatorischen Maßnahmen (TOM)*

Durch das Datenschutz-Anpassungs- und Umsetzungsgesetz hat die EU die Vorgaben der Datenschutz-Grundverordnung (DSGVO / GDPR) zur Datensicherheit näher spezifiziert.

Einiges davon ist aus dem bestehenden BDSG bekannt. Andere technische und organisatorische Maßnahmen (TOMs) sind neu und bedürfen entsprechend der Vorbereitung und Umsetzung. Zu finden sind die aktuellen Anforderung in § 64 BDSG (neue Fassung).

Vorbereitung auf erweiterte Datenschutzkontrollen

Auf Basis einer Risikobewertung sind ab sofort Maßnahmen für die Datensicherheit zu ergreifen.

§ 64 BDSG n.F. gibt hinsichtlich der zu treffenden Maßnahmen (Kontrollen) einen Überblick:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte **(sog. Zugangskontrolle)**

Zu der erweiterten Zugangskontrolle gehören somit Maßnahmen wie

- Absicherung der Gebäude, Fenster und Türen,
- Sicherheitsglas,
- Bruch- und Öffnungsmelder,
- Videoüberwachungs-Anlagen,
- Alarmanlagen,
- Zutrittskontroll-Systeme mit Chipkarten-Leser und
- Besucher-Dokumentation

Aber auch Vorkehrungen wie

- Passwortrichtlinien,
- Zwei-Faktor-Benutzeranmeldung,

- Firewalls,
- digitale Zertifikate,
- Verschlüsselungen
- Schutz vor Schadsoftware,
- Bildschirmsperre und
- aktuelle Nutzerverwaltung.

2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle)

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)

4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle)

5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle)

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle)

7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle)

8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle)

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit)

10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit)

11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)

12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit)

Im Vergleich zur bekannten Anlage zu § 9 Satz 1 BDSG sind hier nun auch neue Datenschutzkontrollen genannt. Die anderen Datenschutzkontrollen bestanden auch bereits nach altem Recht, sodass hier unbedingt zu prüfen ist, inwieweit bereits schon diese Datenschutzkontrollen bisher im Unternehmen nicht eingehalten werden.

Was ist nun neu? Was sind die neuen Kontrollen?

Nach neuem BDSG + DS-GVO nun umzusetzen:

- Sie müssen gewährleisten, dass sie eingesetzte Systeme im Störungsfall wiederherstellen können (Wiederherstellbarkeit).
- Sie müssen gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit).
- Sie müssen gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)

In diesen Bereichen fehlen heute vielfach noch geeignete technisch-organisatorische Maßnahmen.

Wichtigkeit der Wiederherstellbarkeit

Vergangene Cyber-Angriff haben gezeigt, dass viele Unternehmen nach Attacken und Störungen nicht über geeignete Maßnahmen für die Wiederherstellbarkeit ihrer Daten verfügen.

Hier sollten unbedingt die geeigneten technischen und organisatorischen Maßnahmen getroffen werden –für die Umsetzung der DSGVO aber insbesondere auch im Eigeninteresse.**

* bei diesem Artikel handelt es sich lediglich um eine Kurzdarstellung der allgemeinen Problematik, welche dazu dienen kann, Ihnen einen ersten kurzen Überblick über die neue Rechtslage zu bieten. Dieser Überblick ersetzt jedoch in keinem Fall eine rechtliche Beratung hinsichtlich der auf Sie zutreffenden und dann ggf. bedarfsgerecht abzuändernden technischen und organisatorischen Maßnahmen. Aufgrund der empfindlichen Bußgelder empfehlen wir Ihnen unbedingt Ihr Unternehmen auf den neuesten Stand zu bringen. Hierzu bieten wir Ihnen eine rechtliche Beratung und unser Zusatzprodukt „Coaching + Schulungen im Datenschutzrecht“ an.

** diese Kurzübersicht bieten keinen Anspruch auf Vollständigkeit.