BB-ONE net
Internet-Partner der Wirtschaft

Vitamine für Ihr Business

BB-ONE net

Agenda

- Begriffs-Bestimmungen

- Vertraulichkeit
- Integrität
- Verfügbarkeit & Belastbarkeit

Präambel

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten.

Die Maßnahmen sollen in einem angemessenen Verhältnis zwischen Aufwand und dem angestrebten Schutzzweck stehen.

Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Trennungskontrolle
- Pseudonymisierung

Zutrittskontrolle

- Maßnahmen, die verhindern, dass unbefugte Personen den physikalischen Zutritt zu Datenverarbeitungsanlagen erhalten.
  - Empfang mit Personenkontrolle
    sowie das Tragen von Firmen-/ Besucherausweisen
  - Verschlossene Türen
  - Alarmanlage
  - Videoüberwachung und Wachdienst
  - Schlüssel- und Chipkartenregelung sowie biometrische Einlass-Systeme
  - Einbruchhemmende Fenster

Zugangskontrolle

- Die Zugangskontrolle verhindert die Nutzung der Datenverarbeitungsanlagen durch Unbefugte.
  - Bildschirmschoner mit Passwortschutz
  - Passwortrichtlinie
  - Magnet- und Chipkarte
  - Benutzername und Passwort
  - PIN-Verfahren
  - Einsatz von Spamfilter und Virenscanner
  - Biometrische Verfahren

Zugriffskontrolle

- Die Zugriffskontrolle stellt sicher, dass ausschließlich befugte Personen Zugriff auf personenbezogene Daten, Programme, und Dokumente erhalten.
  - Erstellen eines Berechtigungskonzepts
  - Einrichten von Administratorenrechten
  - Verschlüsselung der Datenträger
  - Regelungen für den Gebrauch von mobilen Datenträgern und Endgeräten
  - Verschlüsselung des WLAN
  - Löschung wiederbeschreibbarer Datenträger und deren datenschutzkonforme Vernichtung

BB-ONE net

Trennungskontrolle

- Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
  - Trennung von Produktiv- und Testsystemen
  - Berechtigungkonzept
  - Mandantenfähigkeit

Pseudonymisierung

- Daten sollen ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.
  - Datentrennung
  - Entsprechende Anweisungen

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
- Eingabekontrolle

Integrität

- Maßnahmen, die gewährleisten, dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
  - Verschlüsselung von eMail und anderer Datenübertragung
  - Einsatz von VPN
  - Signaturverfahren

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle
- Belastbarkeitskontrolle

Verfügbarkeit und Belastbarkeit

- Maßnahmen, die gewährleisten, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
  - USV
  - Backup & Recovery
  - Serverraum klimatisiert, Branderkennung, Feuerlöschsystem
  - Plattenspiegelung, getrennte Partitionen
  - Notfallplan

BB-ONE net

Umsetzung der DS-GVO
muss zum Unternehmen passen

Literatur

- magazin.bb-one.net
- ebusiness-lotse.de
-
- https://dsgvo-gesetz.de
- https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/datenschutzgrundverordnung.pdf?__blob=publicationFile&v=14