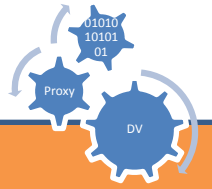
Datenschutz in der digitalen Welt



Welche Anforderungen stellt der technisch organisatorische Datenschutz an die Verantwortlichen und wo steht das?

Art. 32 DSGVO -> Sicherheit der Verarbeitung

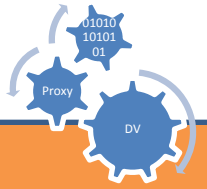
- **Passende Erwägungsgründe**
  (**75**) Risiken für die Rechte und Freiheiten natürlicher Personen
  (**76**) Risikobewertung
  (**77**) Leitlinien zur Risikobewertung
  (**78**) Geeignete technische und organisatorische Maßnahmen
  (**79**) Zuteilung der Verantwortlichkeit
  (**83**) Sicherheit der Verarbeitung

§ 9 BDSG vs § 64 DSAnpUG-EU
(Datenschutz-Anpassungs- und -Umsetzungsgesetz EU)

Zuwachs bei den technischen und organisatorischen Maßnahmen

Zuwachs bei den technischen und organisatorischen Maßnahmen

§ 9 BDSG -> Anlage zu § 9	§ 64 DSAnpUG-EU
Zutrittskontrolle	Zugangskontrolle
Zugangskontrolle	Zugriffskontrolle
Zugriffskontrolle	Übertragungskontrolle
Weitergabekontrolle	Eingabekontrolle
Eingabekontrolle	Wiederherstellbarkeit
Verfügbarkeitskontrolle	Verfügbarkeitskontrolle
Auftragskontrolle	Auftragskontrolle
Trennungsgebot	Trennbarkeit
	Datenträgerkontrolle (+)
	Speicherkontrolle (+)
	Benutzerkontrolle (+)
	Transportkontrolle (+)
	Zuverlässigkeit (+)
	Datenintegrität (+)



Die Anforderungen im Detail

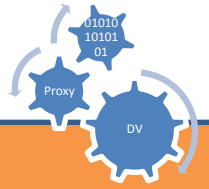
Zugangskontrolle incl. der Zutrittskontrolle aus dem BDSG § 9

Zu der erweiterten Kontrolle 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:

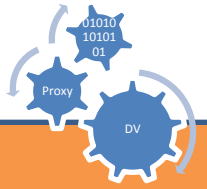
- Passwortrichtlinien
- Zwei-Faktor-Benutzeranmeldung
- Firewalls, Proxy
- digitale Zertifikate, Verschlüsselung
- Schutz vor Schadsoftware (Virenschutz)
- Bildschirmsperre und aktuelle Nutzerverwaltung (Benutzerrollen)



Datenträgerkontrolle (+)

Zu der Datenträgerkontrolle gehören somit Maßnahmen wie:

- Kopier- Faxgeräte mit einbeziehen,
- Verwaltung der Datenträger,
- Datenträger in verschließbaren Behältnissen lagern,
- Datenarchiv einrichten,
- Festlegung der Aufbewahrungsfristen,
- Überwachung des Fremdpersonals,
- Datenübermittlung nach Schutzwürdigkeit auch per Bote,
- Entsorgung der Datenträger regeln ...



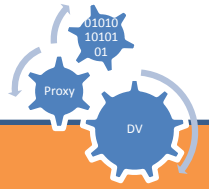
Speicherkontrolle (+)

Zu der Speicherkontrolle gehören somit Maßnahmen wie:

- regeln und festlegen von Befugnissen,
- installieren von Zugriffschutzsystemen für zentrale und dezentrale Rechner.

Diese Systeme sollen folgende Grundforderungen erfüllen:

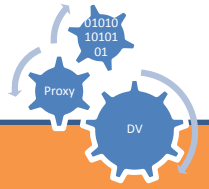
- Untergliederung von Verarbeitungsrechten,
- Anwender-Kennung (Userid), persönliches Passwort
- Zwang zum periodischen Passwortwechsel
- automatische und manuelle Dunkelschaltung des Bildschirms. Entriegelung nur über Passworteingabe,
- führen von Logdateien,
- maschinelles Auswerten dieser Logdateien nach bestimmten Kriterien,
- auswerten von Logdateien und Konsolprotokollen,
- nutzen der betriebssysteminternen Sicherheitsmechanismen.



Benutzerkontrolle (+)

Zu der Benutzerkontrolle gehören somit Maßnahmen wie:

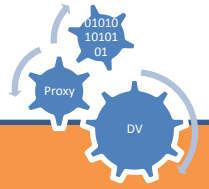
- Verschluss oder sogar Verplomben der Datenstationen,
- Verwendung von Benutzerkennungen und Passwörtern,
- Festlegungen zu Datenübertragungen bei Netzarbeit (Abschottung von anderen Netzen, Begrenzung der Netzverwaltung auf 1 oder 2 Nutzer, Festlegung, welche Daten sollen wie übertragen werden),
- revisionsfähige Dokumentation der Benutzerprofile,
- revisionsfähige Protokollierung,
- Einsatz von Sicherheitssoftware,
- Einsatz von Verschlüsselungsverfahren,
- Abweisung unberechtigter Benutzer.



Zugriffskontrolle

Zu der Zugriffskontrolle gehören somit Maßnahmen wie:

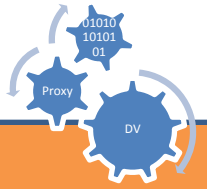
- Stellenbeschreibung
- differenzierte Berechtigungen
- regeln Benutzerrechte
- Auswertung von Logfiles
- Auswertungen der Löschungen
- Auswertungen der Veränderungen
- Domainenregelungen
- Einsatz von Anwendungssoftware mit “Rollenberechtigungskonzepten”
- Einsatz von Anwendungssoftware mit “differenzierbaren Rechten”
- ...



Übertragungskontrolle

Zu der Übertragungskontrolle gehören somit Maßnahmen wie:

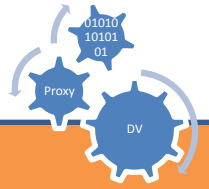
- Festlegung der zugelassenen Übertragungsberechtigten (Sender), Übermittlungsempfänger und Übermittlungswege,
- Überprüfung der Authentizität des Empfängers,
- Dokumentation der Empfänger,
- Festlegung einer ausreichenden Benutzeridentifizierung (Zeiten, Personen, Verfahren, Geräte, Programme, welche Daten),
- Festlegungen zur Auswertung der Protokolle (Periodizität, Umfang),
- Fernwartung nur bei Sicherstellung, dass personenbezogene Daten nicht eingesehen werden können,
- Protokollierung der Datenübermittlung,
- Einsatz von Verschlüsselungsverfahren,
- Einsatz von sicherheitsgeprüften Protokollen,
- Dokumentation der Abruf- und Übermittlungsprogramme,
- Netzwerkdokumentation,
- Dokumentation der Programmfreigabe von Übermittlungsprogrammen.



Eingabekontrolle

Zu der Eingabekontrolle gehören somit Maßnahmen wie:

- erweiterte Unterweisungen an diese Personen
- Stellenbeschreibung
- differenzierte Berechtigungen
- regeln Benutzerrechte
- Auswertung von Logfiles bezüglich “Zugang” und “Zugriff”
- Auswertungen der Logfiles, bezüglich Erfassen, Ändern und Löschen der Daten
- Einsatz von Anwendungssoftware mit “Rollenkonzepten”
- Einsatz von Anwendungssoftware mit “differenzierbaren Rechten”
- ...

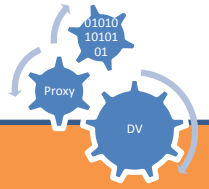


Transportkontrolle (+)

Zu der Transportkontrolle gehören somit Maßnahmen wie:

Übertragung:
- nur verschlüsselte Daten übermitteln,
- Schlüssel periodisch ändern,
- Übermittlungszeiten variieren.

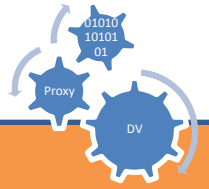
Transport:
- feste, verschließbare Metallbehälter verwenden,
- Datenträger als Wertsendung verschicken (Wert größer 1500€)
- keine Kennzeichnung der Behältnisse als Datenträger,
- abgleichen der Risiken zwischen Spediteur und Postdienste,
- bei hausinternem Transport die Versandmappen fest verschließen



Verfügbarkeitskontrolle/Wiederherstellbarkeit

Zu der Verfügbarkeitskontrolle/Wiederherstellbarkeit gehören somit Maßnahmen wie:

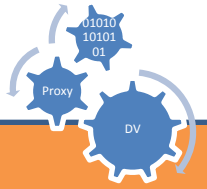
- Einstufen der Daten nach Vertraulichkeits-, Integritäts- und Verfügbarkeits-Anforderungen
- Firewall (eventuell auch direkt auf den einzelnen PCs)
- Virenschutz
- Notfallkonzept
- Regelungen zu Routern und Switches
- Internetverhaltensregelungen aufstellen
- Regelung “E-Mail“
- Backup-Konzept und danach erst
- geregelte Datensicherungen nach den Bedürfnissen der Stelle
- geübtes Restore der Datensicherungen (disaster recovery Konzept)
- ...



Zuverlässigkeit (+) / Datenintegrität

Zu der Zuverlässigkeitskontrolle gehören somit Maßnahmen wie:

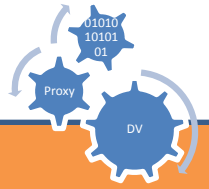
- Stand der Technik einhalten (Monitoring)
- Firewall (eventuell auch direkt auf den einzelnen PCs)
- Virenschutz
- Notfallkonzept
- Updatekonzept
- USV
- Überspannungsschutz
- Eigener Stromkreis
- Klimaanlage



Auftragskontrolle

Zu der Auftragskontrolle gehören somit Maßnahmen wie:

- Intern darstellen und begründen was Auftragsdatenverarbeitung für den Auftraggeber, also die Stelle, bedeutet und welche Gefährdungen und Haftungsfragen bei der Stelle verbleiben
- Unterweisung gerade des eigenen Personals zu diesem extrem sensiblen Datenschutzaspekt
- vertragliche Regelung der ADV
- immer gleiches und formalisiertes Vergabe-/Auswahlkriterium
- Kontrolle und Überwachung
- Ansprechpartner und Vertreter bestimmen
- Geheimhaltung und stellenbezogene Notwendigkeiten § 203 StGB
- Regeln der zeitlichen und umfänglichen Datenzugriffe des AN
- Regeln des Zugriffverfahrens (Technik. Wie, mit was)
- Auswertung von Logfiles bezüglich “Zugang” und “Zugriff”
- Einfordern von Nachweisen wie etwa Datenschutz- oder IT-Sicherheits-Zertifikat, bestellter DSB, Unterweisungsstand der AN-Mitarbeiter
- ...



Trennbarkeitskontrolle

Zu der Trennbarkeitskontrolle gehören somit Maßnahmen wie:

- Zweckbindung im Verfahrensverzeichnis genau formulieren und den Zugriffsberechtigten zur Kenntnis bringen
- Unterweisung der Mitarbeiter zu diesem Sachverhalt
- regeln Benutzerrechte
- regeln Backup dahingehend, dass beim Restore die Trennung erhalten bleibt
- Trennung Produktiv und Testdaten
- Trennung von Keys/IDs und Nutzdaten
- logische und/oder physikalische Trennung der Datenbestände/Datenbanken
- Funktionstrennung (Verantwortung/Ausführung)
- regeln der Datenübermittlung
- Mandantenfähigkeit der Anwendung nutzen
- ...