Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Datenschutz durch Technik:

Sicherheit der Verarbeitung durch technisch-organisatorische Maßnahmen

Timo Göth
Bereich Technik

Ein Jahr Datenschutz-Grundverordnung - Erfahrungsaustausch und weiteres Vorgehen

Paritätischer Wohlfahrtsverband Landesverband Rheinland-Pfalz/Saarland e. V.

Bisherige Rechtsgrundlage

§ 9 LDSG, bzw. Anlage zu § 9 Satz 1 BDSG („10 Gebote“)

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übermittlungskontrolle
- Eingabekontrolle
- Auftragskontrolle
- Transportkontrolle
- Organisationskontrolle

Bild: https://pixabay.com/de/illustrations/gesetz-symbol-recht-paragraf-447487/

Seit 25. Mai 2018 → Datenschutz-Grundverordnung

Risikobasierter Ansatz

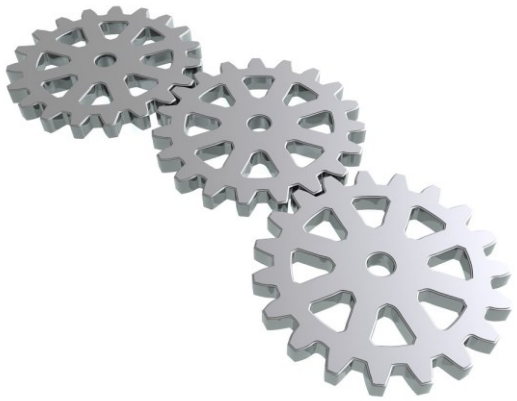
Ausrichtung der erforderlichen Maßnahmen an der Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken.

Dabei sind insbesondere folgende Risiken in den Blick zu nehmen:

- unbefugte Offenlegung,
- unbefugter Zugang zu personenbezogenen Daten.
- unbeabsichtigte/unrechtmäßige Vernichtung und Veränderung,
- unbeabsichtigter/unrechtmäßiger Verlust

Bild: https://pixabay.com/de/illustrations/gesetz-symbol-recht-paragraf-447487/

Technisch-Organisatorische Maßnahmen (TOM)



Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art und Zwecke der Verarbeitung sind geeignete technisch-organisatorische Maßnahmen zu treffen, die Folgendes einschließen:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen nach einem Zwischenfall rasch wiederherzustellen.

Bild: https://pixabay.com/de/illustrations/zahnr%C3%A4der-metall-industrie-zahnrad-686316/

Welche Anforderungen stellt die Datenschutz-Grundverordnung an die Sicherheit der Verarbeitung ?

Art. 5 Grundsätze
Art. 24 Verantwortung
Art. 25 Datenschutz durch Technikgestaltung
Art. 32 Sicherheit der Verarbeitung

Art. 5 Grundsätze

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Pers

b) für festgelegte, eindeutige und legitime Zwecke erhoben

c) Zw („D

e) in einer Form gespeichert werden, die die Identifizierung der betroffene Zwecke, fu personenb soweit die Durchführ Maßnahm und Freihe ausschließ

wecken nicht zu

ß

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („**Rechenschaftspflicht**“).

Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität und Vertraulichkeit**“);

Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („**Speicherbegrenzung**“);

Art. 24 Verantwortung

(1) Der Verantwortliche setzt unter Berücksichtigung der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke** der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der **Risiken** für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen** um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

(2) Diese Maßnahmen werden **erforderlichenfalls überprüft** und **aktualisiert**.

Art. 25 Technikgestaltung/Voreinstellungen

(1) Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke** der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen **Risiken** für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung **geeignete technische und organisatorische Maßnahmen** – wie z. B. **Pseudonymisierung** –, 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. 25 Technikgestaltung/Voreinstellungen

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch **Voreinstellung** nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck **erforderlich** ist, verarbeitet werden. [2]Diese Verpflichtung gilt für die **Menge** der erhobenen personenbezogenen Daten, den **Umfang ihrer Verarbeitung**, ihre **Speicherfrist** und ihre **Zugänglichkeit**. [3]Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Art. 32 Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke** der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere 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:

Art. 32

a) die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;

b) die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Was sind technische, bzw. organisatorische Maßnahmen?

Technische Maßnahmen:

Beziehen sich auf die eigentliche Datenverarbeitung, also auf Maßnahmen die sich **physisch, bzw. in Software** umsetzen lassen, etwa:

- Türschlösser
- Alarmanlagen
- Benutzerkonten
- Zugriffsberechtigungen
- Passwortvorgaben
- Datensicherung
- Schutzsoftware
- SPAM-Filter
- usw.

Organisatorische Maßnahmen:

Beziehen sich auf die Rahmenbedingungen der Datenverarbeitung und werden in der Regel als **Vorgaben/Handlungsanweisungen** an die Beschäftigten festgelegt, etwa:

- Besucherbuch/-ausweise
- Wegschließen von Akten
- Abschließen des Büros
- Sperren des Computers
- Regelung zur Erteilung von Auskünften
- Vorgaben und Werkzeuge zur Schwärzung
- Verpflichtung auf Vertraulichkeit/Datengeheimnis
- usw.
- Regelmäßige Sensibilisierung

TOM bei den Hintergrundsystemen (Server)

- Aktuelle Betriebssysteme/Software
- Aktuelle Schutzsoftware
- Rollen-/Berechtigungskonzept („Need to know“)
  - Verzeichnisse
  - Dokumente
  - Mailpostfächer
- Verschlüsselte Datenübertragung
- Verschlüsselte Datenhaltung
- Passwortvorgaben für Clients
  - Länge, Komplexität, Gültigkeitsdauer
- Datensicherung
- Protokollierung
- Anonymisierung/Pseudonymisierung
- Löschung/Sperrung
- Getrennte Datenhaltung

Bild: https://pixabay.com/de/illustrations/hinweistafeln-sonderzeichen-105193/

TOM am Computer (Client)

- Aktuelle Betriebssysteme/Software
- Aktuelle Schutzsoftware
- Zugangsschutz
  - Passwort
  - Geheimhaltung des Passworts
  - (automatische) Computersperre
- Zugriffsschutz
  - Berechtigung
  - Verschlüsselung von Datenträgern
  - Verschlüsselung von Mails

Bild: https://pixabay.com/de/photos/schild-diebstahl-hinweis-weinberg-2012357/

TOM am Arbeitsplatz (Raum)

- Zutrittsschutz
  - Türschloss
  - Türknauf
- Sichtschutz
  - Wände, Folien
- Wegschließen der Akten/Unterlagen
  - Schrank, abschließbarer Transportbehälter
- Fax-/Druckeraufstellung
  - Indirekte Ausdrucke (Box, Chip)
- Räumliche Ausgestaltung
  - Trennung
  - Wartebereich
  - Gesonderter Raum für sensible Gespräche
- Aktenvernichter

Bild: https://pixabay.com/de/illustrations/schl%C3%BCssel-werkzeug-offen-sperre-2114459/

Beispiel: Aktenvernichtung (DIN 66399)

Übersicht der Klasse „P": Informationsdarstellung *in Originalgröße* (Papier, Film, Druckformen, …)

DIN 32757	DIN 66399	Zuordnung der Datenträger nach DIN 66399 Datenträgervernichtung derart, …	Schutzklasse DIN 66399	Partikelgrößen nach DIN 66399		zulässige Toleranzen
1	P-1	…dass die Reproduktion der auf ihnen wiedergegebenen Daten ohne besondere Hilfsmittel und Fachkenntnisse, jedoch nicht ohne besonderen Zeitaufwand möglich ist Empfohlen z. B. für Datenträger mit allgemeinen Daten, die unlesbar gemacht werden sollen.	1	Materialteilchenfläche max. 2.000 mm² oder Streifenbreite max. 12,0 mm Streifenlänge nicht begrenzt		10% des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch max. 3.800 mm² groß sein
2	P-2	…dass die Reproduktion der auf ihnen wiedergegebenen Daten mit Hilfsmittel nur mit besonderem Aufwand möglich ist Empfohlen z. B. für Datenträger mit internen Daten, die unlesbar gemacht werden sollen.	1	Materialteilchenfläche max. 800 mm² oder Streifenbreite max. 6,0 mm Streifenlänge nicht begrenzt		10% des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch max. 2.000 mm² groß sein
3	P-3	…dass die Reproduktion der auf ihnen wiedergegebenen Daten nur unter erheblichem Aufwand (Personen, Hilfsmittel, Zeit) möglich ist Empfohlen z. B. für Datenträger mit sensiblen und vertraulichen Daten	1 + 2	Materialteilchenfläche max. 320 mm² oder Streifenbreite max. 2,0 mm Streifenlänge nicht begrenzt		10% des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch max. 800 mm² groß sein
–	NEU P-4	…dass die Reproduktion der auf ihnen wiedergegebenen Daten nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen möglich ist Empfohlen z. B. für Datenträger mit besonders sensiblen und vertraulichen Daten	2 + 3	Materialteilchenfläche max. 160 mm² und für regelmäßige Partikel: max. Streifenbreite 6,0 mm		10% des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch max. 480 mm² groß sein
4	P-5	…dass die Reproduktion der auf ihnen wiedergegebenen Daten nach dem Stand der Technik unwahrscheinlich ist Empfohlen z. B. für Datenträger mit geheim zu haltenden Daten	2 + 3	Materialteilchenfläche max. 30 mm² und für regelmäßige Partikel: max. Streifenbreite 2,0 mm		10% des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch max. 90 mm² groß sein
5	P-6	…dass die Reproduktion der auf ihnen wiedergegebenen Daten nach dem Stand der Technik unmöglich ist Empfohlen z. B. für Datenträger mit geheim zu haltenden Daten, wenn außergewöhnlich hohe Sicherheitsvorkehrungen einzuhalten sind.	3	Materialteilchenfläche max. 10 mm² und für regelmäßige Partikel: max. Streifenbreite 1,0 mm		10% des Materials dürfen die geforderte Materialteilchenfläche überschreiten, jedoch 30 mm² groß sein
–	NEU P-7	…dass die Reproduktion der auf ihnen wiedergegebenen Daten nach dem Stand von Wissenschaft und Technik unmöglich ist Empfohlen für Datenträger mit streng geheim zu haltenden Daten, wenn höchste Sicherheitsvorkehrungen einzuhalten sind.	3	Materialteilchenfläche max. 5 mm² und für regelmäßige Partikel: max. Streifenbreite 1,0 mm oder Auflösen mit Materialteilchenfläche max. 5 mm² oder Asche zerkleinert mit Materialteilchenfläche max. 5 mm²		keine Toleranzen zulässig

Quelle: https://www.fp-altmann.de/doks/intimus_Uebersicht-Schutzklassen.pdf

Beispiel: Aktenvernichtung

- DIN 33699 (Seit 2012)
- Umfasst auch Datenträger
- Medizinische Daten (Papier)

  → Schutzklasse III → Sicherheitsstufe P5
- Inanspruchnahme eines Dienstleisters

  → Auftragsverarbeitungsvertrag

Bild: https://pixabay.com/de/photos/papierschnitzel-aktenschnitzel-168650/

Beispiel: (Mail) Verschlüsselung

- Wahrung der **Vertraulichkeit** der übermittelten Daten
- E-Mail entspricht in Sachen Vertraulichkeit einer mit Bleistift geschriebenen Postkarte!

Was ist geboten, insofern sensible personenbezogene Informationen übermittelt werden sollen?

- Korrekte Empfangsadresse
- Inhaltsverschlüsselung
  - Neutraler Betreff
  - Sicheres Passwort
  - Passwort auf separatem Weg übermitteln
- Alternative Post oder Fax

https://www.datenschutz.rlp.de/de/themenfelder-themen/e-mail-inhalte-schuetzen/

Bild: https://pixabay.com/de/illustrations/globus-e-mail-kugel-ball-erde-107394/

Beispiel: Verschlüsselung (ZIP)

Es muss nicht immer kompliziert sein

Eine verschlüsselte ZIP-Datei ist eine einfache Möglichkeit

- Freie OpenSource Software (z.B. 7-Zip)
- Verschlüsselung nach dem Stand der Technik (AES 256)
- Geeignet vor allem für den Versand **mehrerer** Dateien

Beachten:

- Übermittlung des Passwortes auf anderem Weg (Telefonisch oder vorher festgelegt)
- Passwortkomplexität und Länge
- Dateiname (auch die der in der ZIP Datei enthaltenen Dateien)
- Betreff/Mailtext

https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/anleitung_7zip.pdf

Beispiel: Verschlüsselung (PDF)

Es muss nicht immer kompliziert sein

Auch eine verschlüsselte PDF-Datei ist eine einfache Möglichkeit

- Freie Software (z.B. PDF-XChange Viewer, PDF24 uvm.)
- Verschlüsselung nach dem Stand der Technik (AES 256)
- Geeignet vor allem für den Versand **einzelner** Dateien

Beachten:

- Übermittlung des Passwortes auf anderem Weg (Telefonisch oder vorher festgelegt)
- Passwortkomplexität und Länge
- AES 256 erst ab PDF V1.7 (Kompatibilität mit Acrobat X und höher)
- Dateiname
- Betreff/Mailtext

http://www.kswillisau.ch/mensamenu/digibag/Publishing/PDF-Bearbeitung/PDF-Bearbeitung.pdf

Beispiel: Verschlüsselung (Gpg4win)

Nach einmaliger (etwas komplexerer) Einrichtung die komfortabelste Methode

Setzt den Einsatz entsprechender Software auf beiden Seiten voraus

- Gpg4win (www.gpg4win.de, freie im Auftrag des BSI entwickelte Software)
- Verschlüsselung nach dem Stand der Technik
- Geeignet vor allem für die regelmäßige Kommunikation mit festen Kontakten
- Integration in Outlook, Thunderbird oder Browser (WebMailer) möglich
- Schlüssel öffentlich verfügbar, also kein Austausch über anderen Kanal notwendig
- Mailinhalt und auch Anhänge können automatisch verschlüsselt werden

Beachten:

- Korrekter öffentlicher Schlüssel und
- Passwortkomplexität und Länge
- Dateiname
- Betreff, ggf. Mailtext

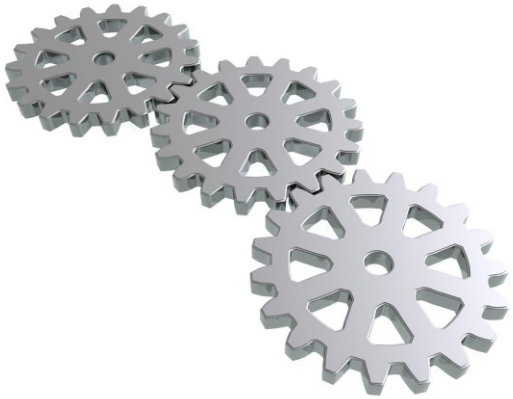
https://www.gpg4win.de/documentation-de.html

Beispiel: Beschäftigtensensibilisierung

- **Bewusstsein schaffen**
- **Informationen geben**
- **Fördern**

Bild: https://pixabay.com/de/illustrations/kette-stark-schutz-selbstbestimmung-1027864/

Beispiel: Beschäftigtensensibilisierung



- Mailversand
  - Korrekte Empfänger
  - BCC bei Massenmails
  - Verschlüsselung
- Phishing/Schadsoftware
  - Emotet (Gefälschte Mails von Kontakten)
  - Have I Been Pwned? / HPI Identity Leak Checker
- Regeln für Auskunft am Telefon
- Zweckbindung
- Löschung

https://haveibeenpwned.com/
https://sec.hpi.de/ilc
https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html
https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/merkmale-einer-phishingmail-6073

Bild: https://pixabay.com/de/illustrations/zahnr%C3%A4der-metall-industrie-zahnrad-686316/

Weitere Hinweise finden Sie unter:

https://www.datenschutz.rlp.de/de/themenfelder-themen/informationstechnikit-sicherheit/

https://www.datenschutz.rlp.de/de/themenfelder-themen/sicherheit-der-verarbeitung-nach-dsgvo/

https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-grundverordnung/datenschutz-folgenabschaetzung/

https://www.datenschutz.rlp.de/de/themenfelder-themen/vereine/

Danke! Fragen?

Bild: https://pixabay.com/de/illustrations/verkehrszeichen-achtung-vorfahrt-63983/

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Timo Göth

Referat Technik

beim Landesbeauftragten für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz

Postanschrift:	Postfach 30 40 55020 Mainz
Büroanschrift:	Hintere Bleiche 34 55116 Mainz
Telefon:	+49 (6131) 208-2578
Telefax:	+49 (6131) 208-2497
E-Mail:	poststelle@datenschutz.rlp.de
Web:	www.datenschutz.rlp.de