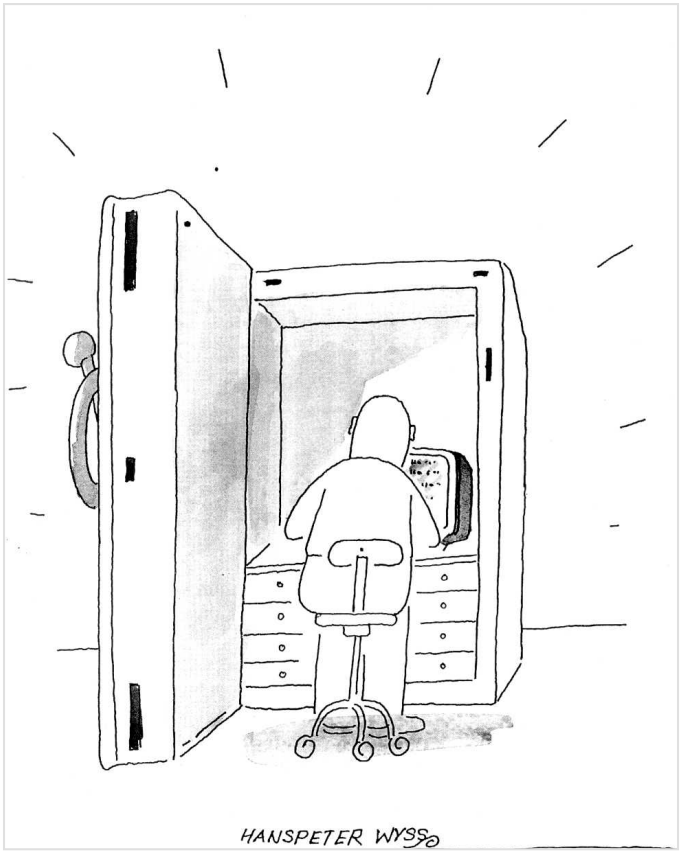


UpDate!
Datenschutz by Esturias

Hamburg, 16.5.2017

Anforderungen an die Sicherheit der Verarbeitung nach der Europäischen Datenschutzgrundverordnung

Datenschutzfolgeabschätzung

Verfahren bei Datenpannen

Agenda

- Sicherheit der Verarbeitung / Technikregelungen
- Datenschutzfolgeabschätzung (Vorabkontrolle)
- Verfahrensverzeichnis
- Verfahren bei Datenpannen

- Sicherheit der Verarbeitung / Technikregelungen

IT-Entwicklung – Der Wandel

- Location Based Services
- Ubiquitous Computing
- Smart Home/Car/Metering ...
- RFID, VR, …
- Big Data
- Autonome Systeme
- ...

Individuelle Datenverarbeitung

Individuelle Datenverarb
+ Internet

mobile Date

mobile Datenverarbeitung
+ Internet

Cloud
Computing

IT-Entwicklung – Kontinuität

§ 9 BDSG (Anlage)

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Zweckbindungskontrolle

Individuelle Datenverarbeitung

Individuelle Datenverarb
+ Internet

mobile Datenve

mobile Datenverarbeitung
+ Internet

Cloud
Computing

§ 9 BDSG (Anlage)

- Zutrittskontrolle ?
- Zugangskontrolle
- Zugriffskontrolle ?
- Weitergabekontrolle
- Eingabekontrolle ?
- Auftragskontrolle ?
- Verfügbarkeitskontrolle
- Zweckbindungskontrolle

mobile Datenverarbeitung

Cloud Computing

Datenschutz in IT-Verfahren - Kontinuität

Einzelne IT-Trends wiederholen sich auf einem höheren technischen Niveau, z.B.:

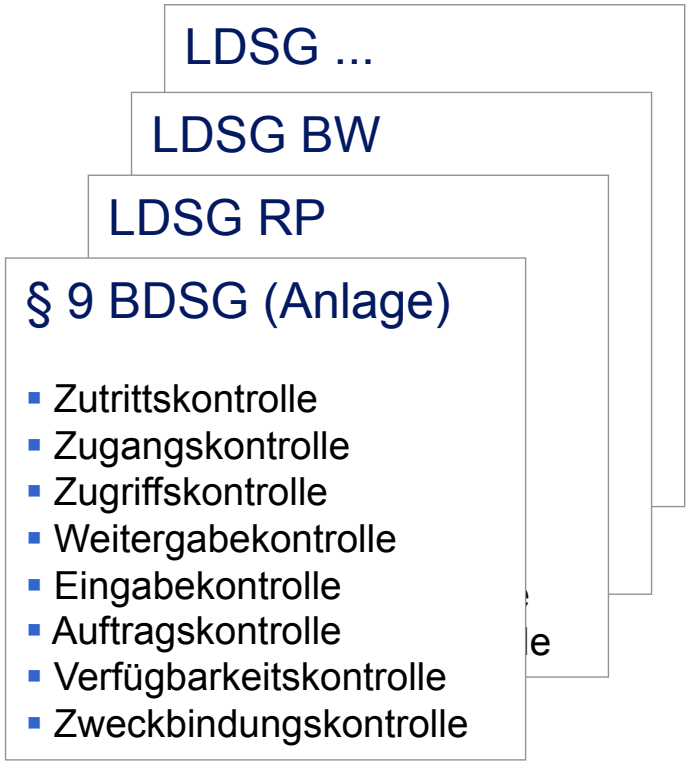
- **Vernetzung**
- **Zentralisierung**

Grundlegende Konzepte des technischen Datenschutzes haben dabei Bestand:

- **Benutzerverwaltung**
- **Berechtigungskonzept**
- **Löschkonzept**
- **Protokollierung**

Situation bisher ...

Situation Anfang der 90er Jahre



Richtlinie 95/46/EG
Art. 16, 17

- Schutz vor unberechtiger Zerstörung, Verlust
- Vertraulichkeit
- Schutz vor unberechtigter Änderung

Systematik der IT-Sicherheit / IT-Grundschutz

Bundesamt
für Sicherheit in der
Informationstechnik

- Verfügbarkeit
- Vertraulichkeit
- Integrität

Technikregelungen der Datenschutzgesetze - Nordrhein-Westfalen

(2) Dabei sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

*1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (**Vertraulichkeit**),*

*2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (**Integrität**),*

*3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (**Verfügbarkeit**),*

*4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (**Authentizität**),*

*5.festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (**Revisionsfähigkeit**),*

*6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (**Transparenz**).*

*(3) Die zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines zu dokumentierenden **Sicherheitskonzepts** zu ermitteln*

Technikregelungen der Datenschutzgesetze – Schleswig-Holstein

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz […] ist durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind.

Sie müssen gewährleisten, dass

*1. Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (**Verfügbarkeit**),*

*2. Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (**Integrität**),*

*3. nur befugt auf Verfahren und Daten zugegriffen werden kann (**Vertraulichkeit**),*

*4. die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann (**Transparenz**),*

*5. personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (**Nicht-Verkettbarkei**) und*

*6. Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte […] wirksam ermöglichen (**Intervenierbarkeit**).*


Datenschutz
IT-Grundschutz-Kataloge
B 1.5 Datenschutz
Beschreibung
technisch-organisatorische Maßnahmen
IT-Grundschutz-Kataloge
Standardwerk zur IT-Sicherheit
IT-Sicherheit

IT-Grundschutz

B 1.5 Datenschutz

Gefährdungslage

Gefährdungen im Umfeld des Datenschutzes können vielfältiger Natur sein. Stellvertretend für diese Vielzahl der Gefährdungen werden in diesem Baustein die folgenden typischen Gefährdungen betrachtet:

Organisatorische Mängel

G 2.162	Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten
G 2.163	Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten
G 2.164	Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten
G 2.165	Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten
G 2.166	Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten
G 2.167	Fehlende oder nicht ausreichende Vorabkontrolle

IT-Grundschutz

B 1.5 Datenschutz

Maßnahmenempfehlungen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen eines Datenschutzmanagements müssen die rechtlichen Rahmenbedingungen beachtet und geeignete technische und organisatorische Maßnahmen getroffen werden, um den Datenschutz sicher zu stellen. Dazu gehören Maßnahmen in der Planungs- und Konzeptionsphase, im Zuge der Umsetzung, sowie beim Betrieb von IT-Systemen und -Verfahren.

Nachfolgend wird das ergänzende Maßnahmenbündel für den Bereich Datenschutz vorgestellt, das für alle IT-Systeme und IT-Verfahren anzuwenden ist, mit deren Hilfe personenbezogene Daten verarbeitet werden:

Planung und Konzeption

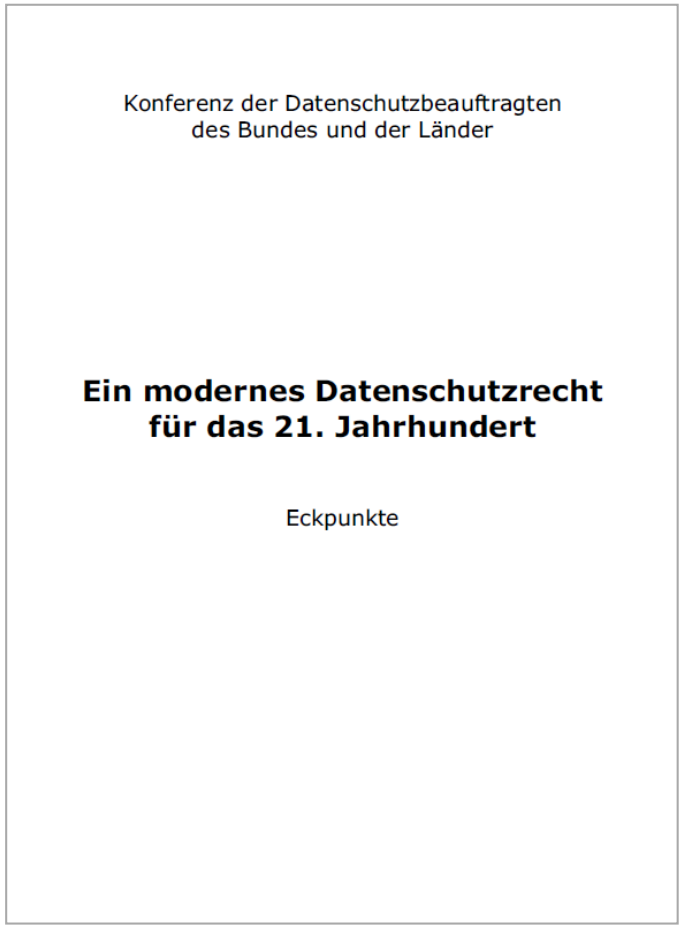
M 2.501	(C)	Datenschutzmanagement

Umsetzung

M 2.502		
M 2.503		
M 2.504		
M 2.505		
M 2.506	(A)	Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten
M 2.507		
M 2.508		
M 2.509		
M 2.510		
M 2.511		
M 2.512		

Betrieb

M 2.110	(A)	Datenschutzaspekte bei der Protokollierung
M 2.513	(Z)	Dokumentation der datenschutzrechtlichen Zulässigkeit
M 2.514	(A)	Aufrechterhaltung des Datenschutzes im laufenden Betrieb
M 2.515	(A)	Datenschutzgerechte Löschung/Vernichtung



** Eckpunkte der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ (18.3.2010)*

Technikregelungen der Datenschutzgesetze

„Kontrollarten“

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- zweckbezogene Verarbeitung

„technikoffene Schutzziele“ *

- **Verfügbarkeit**
- **Integrität**
- **Vertraulichkeit**
- Transparenz
- Authentizität
- Revisionsfähigkeit
- Nichtverkettbarkeit
- Intervenierbarkeit

- Systemdatenschutz
- Audit / Zertifizierung
- Selbstdatenschutz

** Eckpunkte der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ (18.3.2010)*

Das Standard-Datenschutzmodell (2016)

http://www.datenschutz.rlp.de/downloads/mat/SDM-Handbuch_V09a.pdf

Gewährleistungsziel Datensparsamkeit .....

Gewährleistungsziel Verfügbarkeit .....

Gewährleistungsziel Integrität .....

Gewährleistungsziel Vertraulichkeit .....

Gewährleistungsziel Nichtverkettbarkeit .....

Gewährleistungsziel Transparenz.....

Gewährleistungsziel Intervenierbarkeit .....

Die 92. Datenschutzkonferenz hat das SDM beraten und die Veröffentlichung der Version 1.0 als Erprobungsfassung beschlossen. Das SDM soll sowohl in der eigenen Kontroll- und Beratungspraxis als auch bei der Planung und beim Betrieb von Datenverarbeitungen durch verantwortliche Stellen im öffentlichen und nicht-öffentlichen Bereich erprobt werden. Das SDM wird von einer Arbeitsgremium der Konferenz laufend fortentwickelt.

Im Rahmen der Novellierung des Datenschutzes auf Europäischer Ebene soll das Standard-Datenschutzmodel als Prüfmaßstab bei der Umsetzung der Europäischen Datenschutz-Grundverordnung vorgeschlagen werden.

7.1 Gewährleistungsziel Datensparsamkeit

Das Gewährleistungsziel Datensparsamkeit kann erreicht werden durch:

- Informationelle Gewaltentrennung innerhalb und zwischen verantwortlichen Stellen,
- Reduzierung von erfassten Attributen der betroffenen Personen,
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten,
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten,
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen,
- Implementierung automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren,
- Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren.

7.2 Gewährleistungsziel Verfügbarkeit

Typische Maßnahmen zur Gewährleistung der Verfügbarkeit sind:

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts,
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt),
- Dokumentation von Syntax und Semantik der Daten,
- Redundanz von Hard- und Software sowie Infrastruktur,
- Umsetzung von Reparaturstrategien und Ausweichprozessen,
- Vertretungsregelungen für abwesende Mitarbeiter.

7.3 Gewährleistungsziel Integrität

Typische Maßnahmen zur Gewährleistung der Integrität sind:

- Einschränkung von Schreib- und Änderungsrechten,
- Einsatz von Prüfsummen, elektronische Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts,
- dokumentierte Zuweisung von Rechten und Rollen,
- Prozesse zur Aufrechterhaltung der Aktualität von Daten,
- Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen.

7.4 Gewährleistungsziel Vertraulichkeit

Typische Maßnahmen zur Gewährleistung der Vertraulichkeit sind:

- Festlegung eines Rechte-Rollen-Konzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens,
- Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen,
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle,
- spezifizierte, für das Verfahren ausgestattete Umgebungen (Gebäude, Räume)
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen etc.),
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept),
- Schutz vor äußeren Einflüssen (Spionage).

7.5 Gewährleistungsziel Nichtverkettbarkeit

Typische Maßnahmen zur Gewährleistung der Nichtverkettbarkeit sind:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten,
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten,
- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung,
- Trennung nach Organisations-/Abteilungsgrenzen,

- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens,
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle,
- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten,
- geregelte Zweckänderungsverfahren.

7.6 Gewährleistungsziel Transparenz

Typische Maßnahmen zur Gewährleistung der Transparenz sind:

- Dokumentation von Verfahren mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Zusammenspiel mit anderen Verfahren,
- Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren,
- Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen,
- Dokumentation von Einwilligungen und Widersprüchen,
- Protokollierung von Zugriffen und Änderungen,
- Nachweis der Quellen von Daten (Authentizität),
- Versionierung,
- Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts.

7.7 Gewährleistungsziel Intervenierbarkeit

Typische Maßnahmen zur Gewährleistung der Intervenierbarkeit sind:

- differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten,
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen,
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes,
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem,
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen,
- Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte,

- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept,
- Einrichtung eines Single Point Of Contact (SPOC) für Betroffene,
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten,
- Einsichtsmöglichkeiten für die Datenschutzbeauftragten der verantwortlichen Stellen und die Datenschutz-Kontroll- und Aufsichtsbehörden.

Schutzbedarfskategorien nach dem Standard-Datenschutzmodell*

Schutzbedarfskategorie „normal"	
1. Unrechtmäßige Datenverarbeitung (Verstoß gegen Gesetze/Vorschriften/ Verträge)	Transparente unrechtmäßige Datenverarbeitung im anzunehmenden Interesse des Betroffenen, Interventionsmöglichkeit des Betroffenen vorhanden.
2. Beeinträchtigungen für informationelle Selbstbestimmung	Verarbeitung personenbezogener Daten des Betroffenen.
3. Beeinträchtigungen des Ansehens und der Reputation des/der Betroffenen	Eine geringe bzw. nur interne Ansehens- oder Reputationsbeeinträchtigung ist möglich, Interventionsmöglichkeiten für den Betroffenen sind vorhanden.
4. Beeinträchtigungen der persönlichen Unversehrtheit des/der Betroffenen	Eine Beeinträchtigung erscheint nicht möglich.
5. Finanzielle Auswirkungen für den/die Betroffenen	Der finanzielle Schaden bleibt für den Betroffenen tolerabel oder kann vom Verursacher oder Dritten restituiert werden.
6. Auswirkungen auf nicht unmittelbar Betroffene (Grundrechtsausübung)	Erhebliche negative gesellschaftliche Auswirkungen sind nicht ausgeschlossen.

* Handbuch Standard-Datenschutzmodell V 0.9a, Seite 32

Schutzbedarfskategorien nach dem Standard-Datenschutzmodell*

Schutzbedarfskategorie „hoch“	
1. Unrechtmäßige Datenverarbeitung (Verstoß gegen Gesetze/Vorschriften/Verträge)	Unrechtmäßige Datenverarbeitung, die erwartbar nicht im Interesse des Betroffenen liegt
2. Beeinträchtigungen für informationelle Selbstbestimmung	Verarbeitung personenbezogener Daten des Betroffenen, die einen weitreichenden Einblick in dessen Persönlichkeit oder dessen mögliches Verhalten und Handeln erlauben.
3. Beeinträchtigungen des Ansehens und der Reputation des/der Betroffenen	Eine Ansehens- oder Reputationsbeeinträchtigung ist zu erwarten, Interventionsmöglichkeiten für den Betroffenen sind beschränkt, bei der er auf externe Hilfe angewiesen ist.
4. Beeinträchtigungen der persönlichen Unversehrtheit des/der Betroffenen	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.
5. Finanzielle Auswirkungen für den/die Betroffenen	Der Schaden bewirkt beachtliche finanzielle Verluste für den Betroffenen, ist jedoch noch nicht existenzbedrohend.
6. Auswirkungen auf nicht unmittelbar Betroffene (Grundrechtsausübung)	Erhebliche negative gesellschaftliche Auswirkungen sind zu befürchten.

* Handbuch Standard-Datenschutzmodell V 0.9a, Seite 32

Schutzbedarfskategorien nach dem Standard-Datenschutzmodell*

Schutzbedarfskategorie „sehr hoch"	
1. Unrechtmäßige Datenverarbeitung (Verstoß gegen Gesetze/Vorschriften/Verträge)	Unrechtmäßige Datenverarbeitung, die dem Interesse des Betroffenen klar widerspricht und unmittelbare konkrete negative Folgen hat.
2. Beeinträchtigungen für informationelle Selbstbestimmung	Verarbeitung besonders schützenswerter personenbezogener Daten des Betroffenen, die dazu führen, dass ein Betroffener weitestgehend von den Aktivitäten einer Organisation gesteuert und davon abhängig wird.
3. Beeinträchtigungen des Ansehens und der Reputation des/der Betroffenen	Ein starke Ansehens- oder Reputationsbeeinträchtigung ohne Interventionsmöglichkeiten für den Betroffenen, eventuell sogar Existenz gefährdender Art, ist denkbar.
4. Beeinträchtigungen der persönlichen Unversehrtheit des/der Betroffenen	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich, mit Gefahr für Leib und Leben.
5. Finanzielle Auswirkungen für den/die Betroffenen	Der finanzielle Schaden ist für den Betroffenen existenzbedrohend.
6. Auswirkungen auf nicht unmittelbar Betroffene (Grundrechtsausübung)	Erhebliche negative gesellschaftliche Auswirkungen sind zu erwarten.

* *Handbuch Standard-Datenschutzmodell V 0.9a, Seite 32*

Zuordnung „Anforderungen BDSG / Gewährleistungsziele“

	Datenspar-samkeit	Verfügbar-keit	Integrität	Vertrau-lichkeit	Nichtver-kettbarkeit	Transpa-renz	Interve-nierbarkeit
§ 28, 28a	§ 28 Abs. 1 Satz 1 Nr. 1, Nr. 2, Abs. 2, Abs. 3 Satz 2, Abs. 6-9 § 28 a Abs. 1	§ 28 Abs. 3a Satz 1	§ 28 Abs. 3a Satz 1		§ 28 Abs. 1 Satz 1 Nr. 1, Nr. 2, Abs. 1 Satz 2, Abs. 2, § 28 Abs. 3 Satz 1, Satz 2, Satz 3, Satz 4, Satz 5, Satz 7, Abs. 5, Abs. 6-9 § 28a Abs. 1, Abs. 2, § 28a Abs. 2 Satz 4	§ 28 Abs. 3 Satz 4, Satz 5, § 28a Abs. 3 § 28a Abs. 2 Satz 2, Abs. 3	§ 28 Abs. 3a Satz 1, Abs. 4
§ 29					§ 29 Abs. 1, Abs. 2, Abs. 4	§ 29 Abs. 2 Satz 2, Satz 3, Satz 4, Abs. 7 Satz 1	§ 29 Abs. 3, Abs. 4
§ 30	§ 30 Abs. 1 § 30 a Abs. 3						
§ 31					§ 31		
§§ 33-35	§ 35					§§ 33, 34	§§ 33-35
§ 38						§ 38 Abs. 1 Satz 5	
§ 39					§ 39		
§ 40	§ 40				§ 40		
§ 42a						§ 42a	

Zuordnung „Anforderungen DSGVO / Gewährleistungsziele“

Tabelle 3: Zuordnung der Artikel der DS-GVO zu den Gewährleistungszielen.

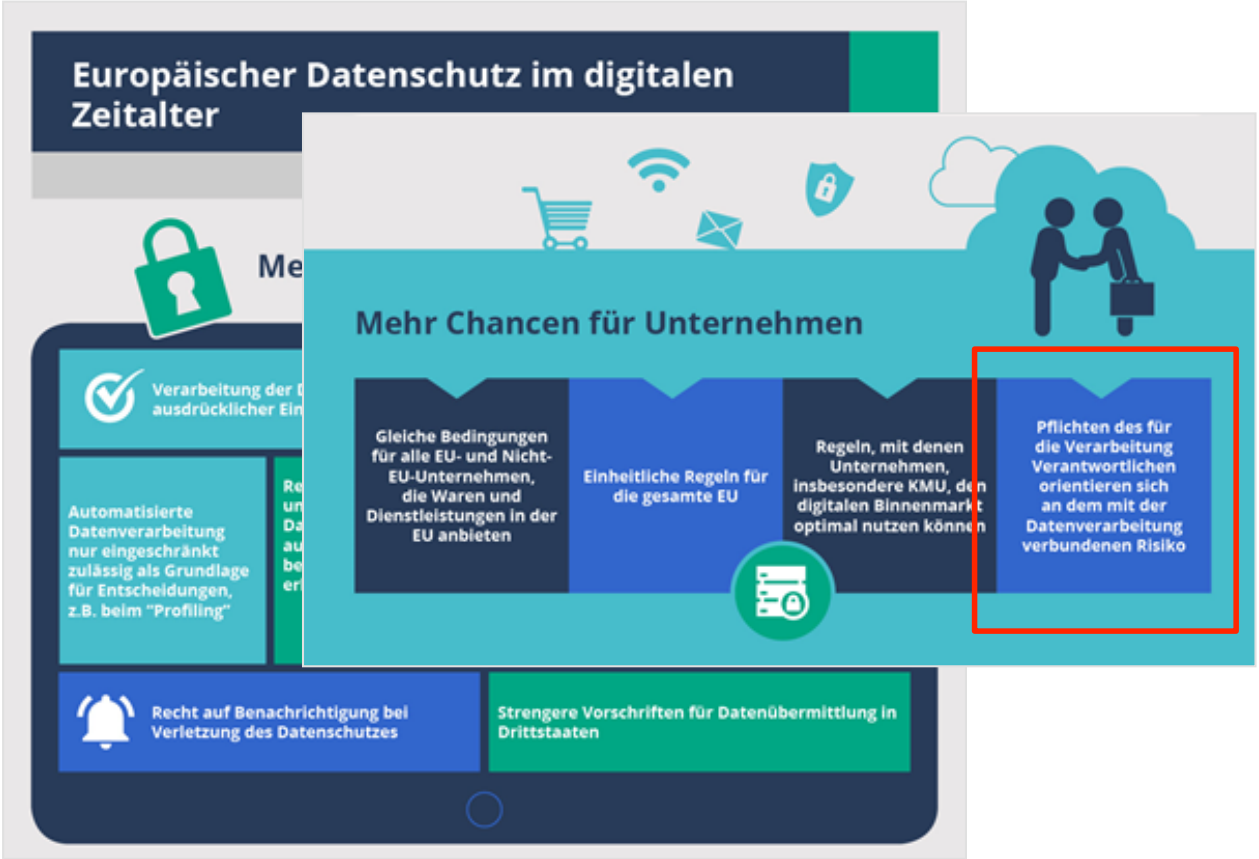
Datenminimierung	*Verfügbarkeit*	*Integrität*	*Vertraulichkeit*	*Nichtverkettung*	*Transparenz*	*Intervenierbarkeit*
5 I c), 5 I e), 25, 32	5 I e), 13, 15, 20, 25, 32	5 I f), 25, 32, 33	5 I f), 25, 28 III b), 29, 32	5 I c), 5 I e), 17, 22, 25, 40 II d)	5 I a), 13, 14, 15, 19, 25, 30, 32, 33, 40, 42	5 I d),5 I f), 13 II c), 14 II d), 15 I e), 16, 17, 18, 20, 21, 25, 32

Tabelle 4: Zuordnung der Erwägungsgründe der DS-GVO zu den Gewährleistungszielen.

Datenminimierung	*Verfügbarkeit*	*Integrität*	*Vertraulichkeit*	*Nichtverkettung*	*Transparenz*	*Intervenierbarkeit*
28, 29, 30, 39, 78, 156	49, 78, 83	39, 49, 78, 83	39, 49, 78, 83	31, 32, 33, 39, 50, 53, 71, 78	32, 39, 42, 58, 60, 61, 63, 74, 78, 84, 85, 86, 87, 90, 91, 100	39, 59, 65, 66, 67, 68, 69, 70, 78

Situation ab Mai 2018 ...

Die Datenschutz-Grundverordnung



„risk based approach“

http://www.consilium.europa.eu/de/policies/data-protection-reform/data-protection-regulation-infographics/

EU Datenschutz-Grundverordnung - **Instrumentarium**

- Sicherheit der Verarbeitung
  Erwägungsgründe 78, 83,84
  Artikel 5, 25, **32**

- Verhaltensregeln
  Erwägungsgründe 77, 81, 98, 99, 148
  Artikel 24, 28, 32, 35, **40**, 41

- Datenschutzfolgeabschätzung
  Erwägungsgründe 84, 89, 90-92, 94, 95
  Artikel **35**, 36, 39

EU Datenschutz-Grundverordnung – **Instrumentarium**

- Zertifizierung

  Erwägungsgründe 77, 81, 100, 166
  Artikel 24, 25,28, 32, **42**, **43**

- Datenschutzsiegel und –prüfzeichen

  Erwägungsgründe 100
  Artikel 42, **43**

EU DSGVO Erwägungsgrund 78

(78) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen

EU DSGVO Erwägungsgrund 83

(83) Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau – auch hinsichtlich der Vertraulichkeit – gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte.

?!

EU DSGVO Erwägungsgrund 84

(84) Damit diese Verordnung in Fällen, in denen die Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, besser eingehalten wird, sollte der Verantwortliche für die Durchführung einer Datenschutz-Folgenabschätzung, mit der insbesondere die Ursache, Art, Besonderheit und Schwere dieses Risikos evaluiert werden, verantwortlich sein. Die Ergebnisse der Abschätzung sollten berücksichtigt werden, wenn darüber entschieden wird, welche geeigneten Maßnahmen ergriffen werden müssen, um nachzuweisen, dass die Verarbeitung der personenbezogenen Daten mit dieser Verordnung in Einklang steht. Geht aus einer Datenschutz-Folgenabschätzung hervor, dass Verarbeitungsvorgänge ein hohes Risiko bergen, das der Verantwortliche nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann, so sollte die Aufsichtsbehörde vor der Verarbeitung konsultiert werden.

EU DSGVO Art. 5 – **Grundsatz: angemessene Sicherheit**

KAPITEL II

GRUNDSÄTZE

Artikel 5

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

[…]

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen ("Integrität und Vertraulichkeit");

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

EU DSGVO Art. 5 – **Grundsatz: angemessene Sicherheit**

Sicherheitskonzept
(internes) Audit

New!

KAPITEL II

GRUNDSÄTZE

Artikel 5

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

[…]

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen ("Integrität und Vertraulichkeit");

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

EU DSGVO Art. 25 – **Datenschutz durch Technik & Voreinstellung**

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche 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 – trifft, 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.

Risikoadäquanz

EU DSGVO Art. 25 – **Datenschutz durch Technik & Voreinstellung**

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

„Privacy by Default“:
- Datenumfang + Verarbeitung
- Speicher-/Löschfristen
- Zugriffsrechte

EU DSGVO Art. 32 – **Sicherheit der Verarbeitung**

ABSCHNITT 2

SICHERHEIT PERSONENBEZOGENER DATEN

Artikel 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 unter anderem Folgendes ein:

Risikoadäquanz
Risikoanalyse

Angemessene
TOM

EU DSGVO Art. 32 – **Sicherheit der Verarbeitung**

Vertraulichkeit

Integrität

Verfügbarkeit

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;

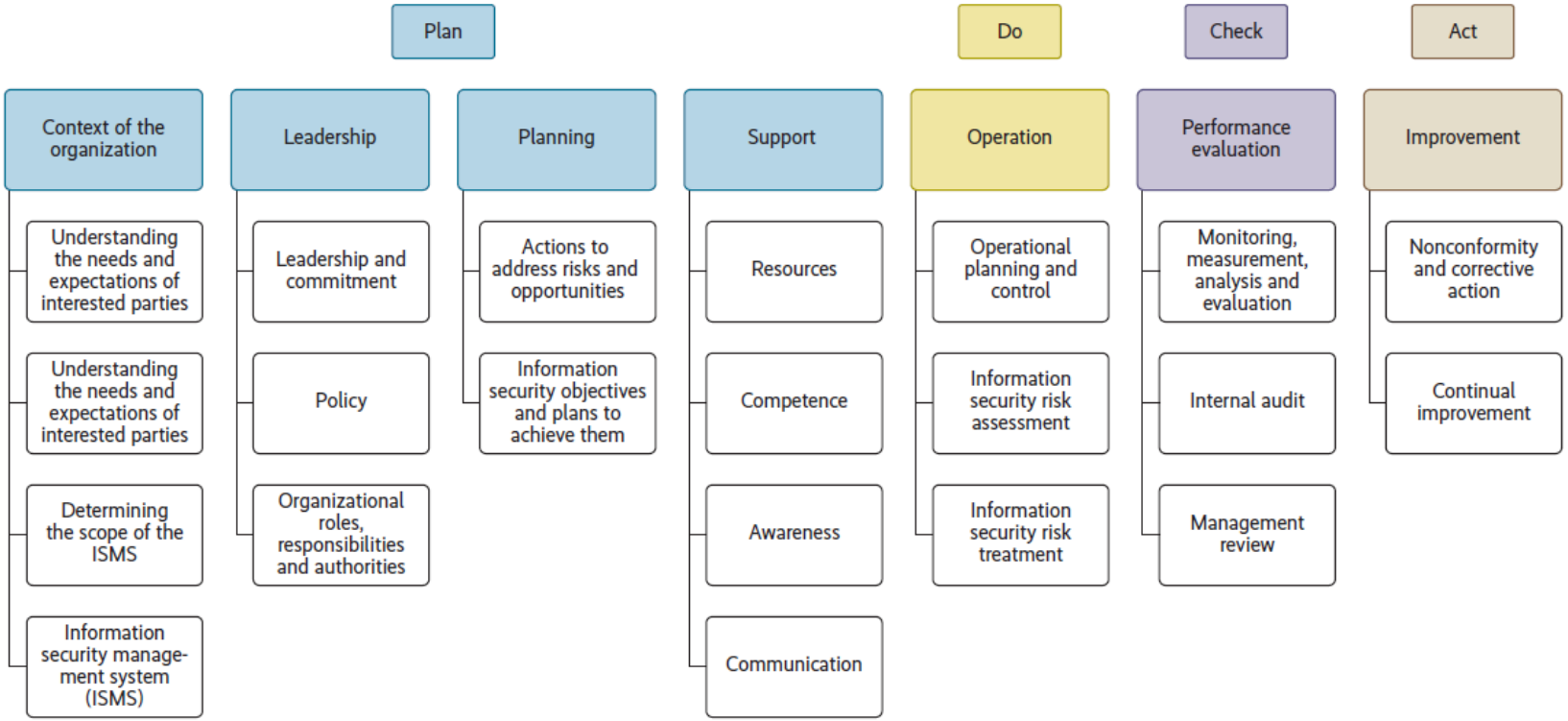
Sicherheits-management

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

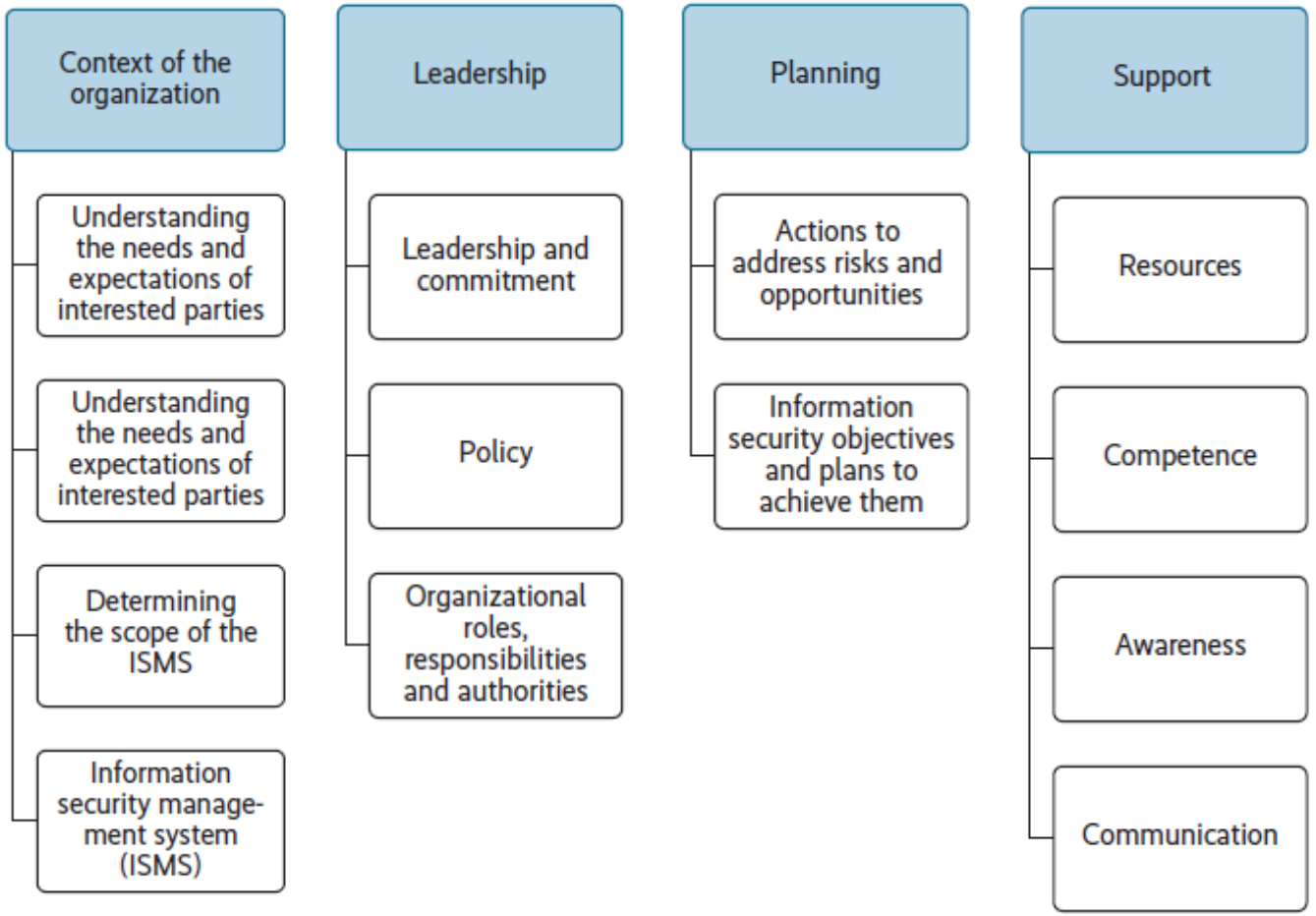
New!

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

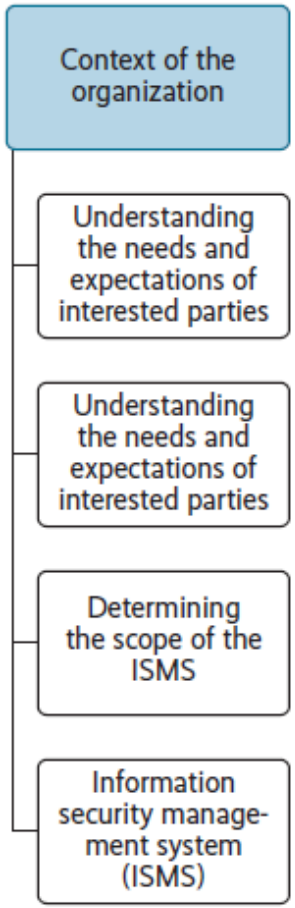
IT-Sicherheitsmanagment ISO 27001



ISO 27001


Context of the organization
Understanding the needs and expectations of interested parties
Understanding the needs and expectations of interested parties
Determining the scope of the ISMS
Information security manage-ment system (ISMS)
Leadership
Leadership and commitment
Policy
Organizational roles, responsibilities and authorities
Planning
Actions to address risks and opportunities
Information security objectives and plans to achieve them
Support
Resources
Competence
Awareness
Communication

ISO 27001

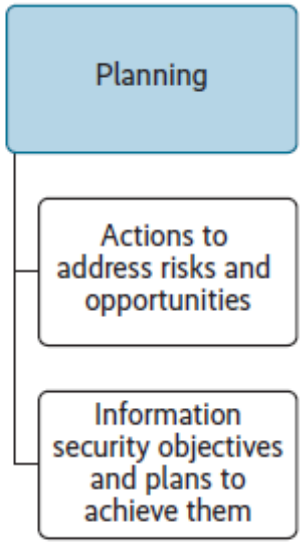


- Berücksichtigung von Unternehmensunfeld, inneren und äußeren Einflüssen (Kunden, Lieferanten, Behörden etc.)
- Ermittlung rechtlicher und vertraglicher Anforderungen (compliance)
- Fokus auf “primary assets” (Informationen, Prozesse) statt “supporting assets” (IT-Systeme)
- Kein Mindestmaß an IT-Sicherheit, sondern angepasstes Sicherheitsnivau (kein Security-Standard, sonderen MS-Standard)

ISO 27001

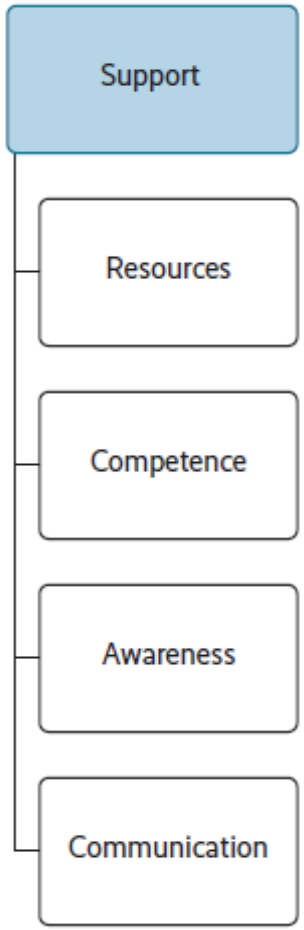
- Einbindung der Leitungsebene
- Festlegung von Sicherheitszielen
- Verabschiedung einer Sicherheitsleitlinie
- Integration ISMS in die Geschäftsprozesse
- Selbstverpflichtung zur Umsetzung
- Selbstverpflichtung zur kontinuierlichen Verbesserung

ISO 27001



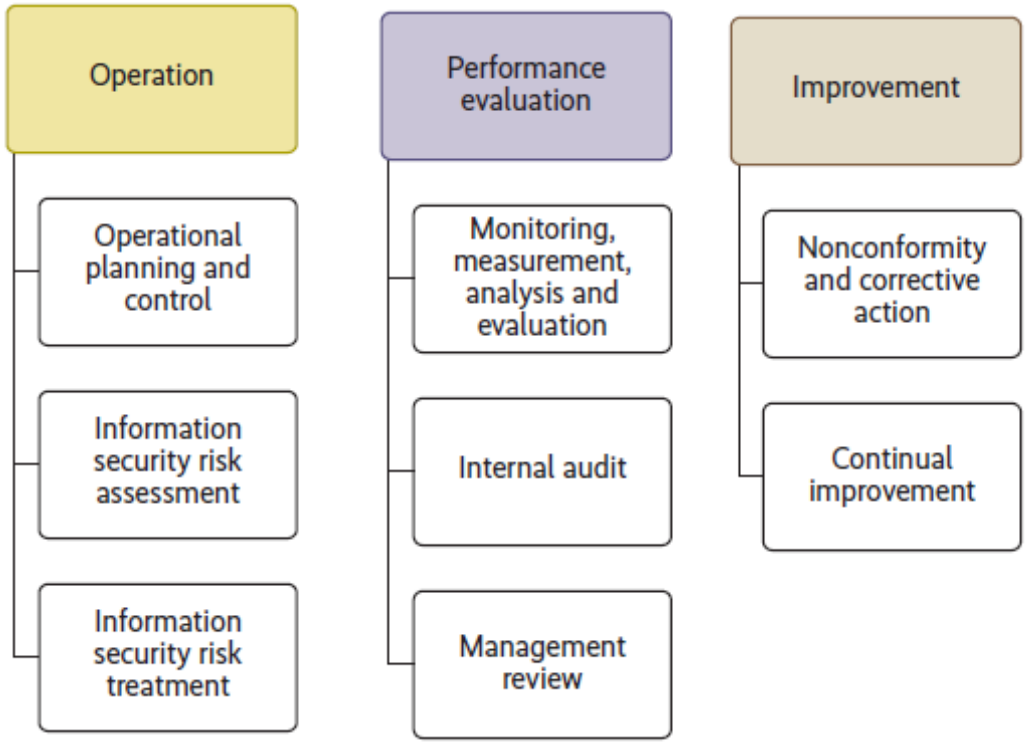
- Zielvorgaben zur IT-Sicherheit
- Überprüfbarkeit/Messbarkeit der Zielvorgaben
- Dokumentation der Zielvorgaben
- Dokumentation der Implementierung

ISO 27001

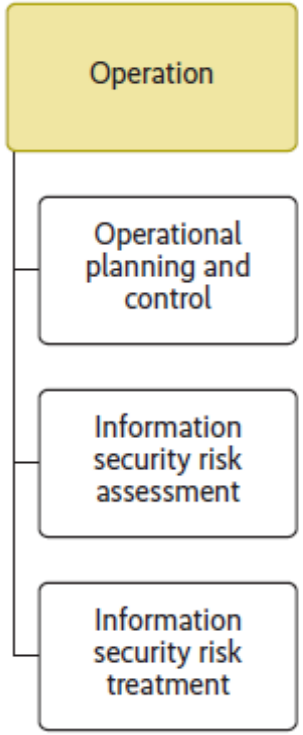


- Bereitstellung notwendiger Ressourcen
- Qualifikation / Nachweise
- Aktive Kommunikation der Sicherheitsleitlinien (Policy)
- Berücksichtigung externer Ressourcen

ISO 27001


Operation
Operational planning and control
Information security risk assessment
Information security risk treatment
Performance evaluation
Monitoring, measurement, analysis and evaluation
Internal audit
Management review
Improvement
Nonconformity and corrective action
Continual improvement

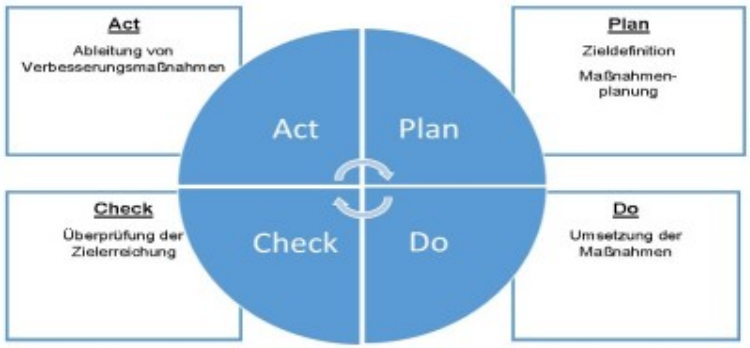
ISO 27001



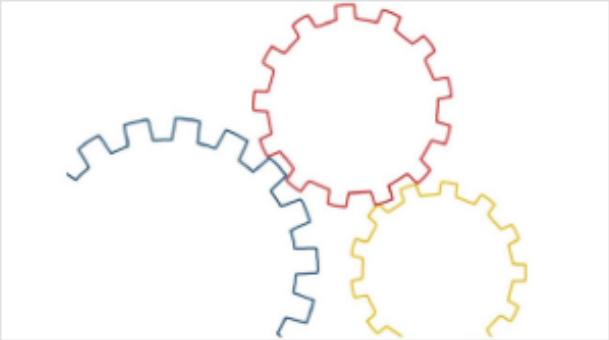
- Risikobetrachtung und Bewertung
- Methodische Behandlung identifizierter Risiken
- Verantwortlichkeiten (risk owner)
- Reaktion auf Sicherheitsvorfälle
- Maßnahmenplanung (Annex A); Erklärung zur Anwendung (statement of applicability)

ISO 27001 (2013)

- Zielvorgaben
- Risikoanalyse
- Maßnahmen
- Ressourcen
- Verantwortlichkeiten
- Umsetzung



ISO 27001 und IT-Grundschutz



IT-Grundschutz-Standards

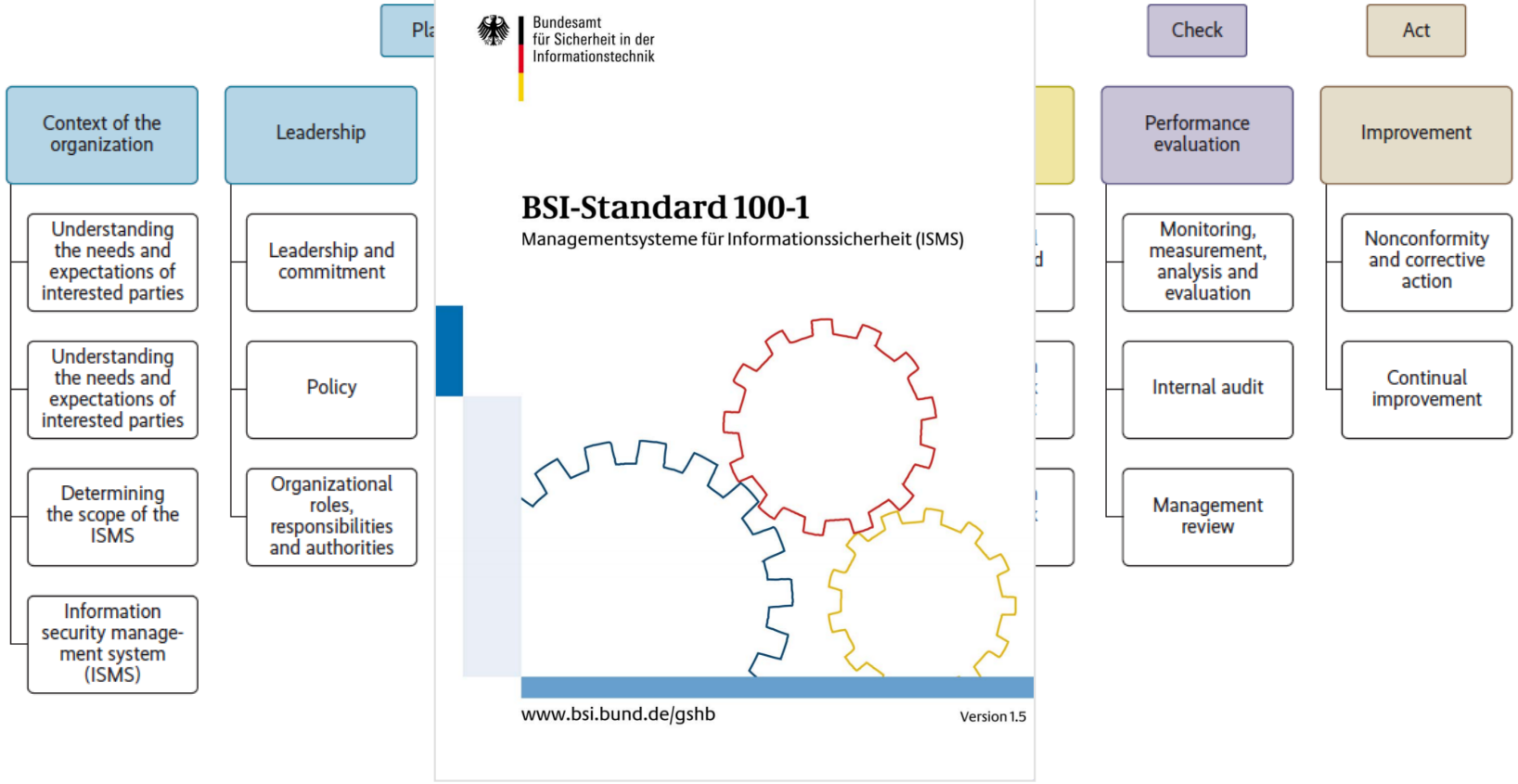
Die BSI-Standards enthalten Empfehlungen zu Methoden, Prozessen, Vorgehensweisen und Maßnahmen zur Informationssicherheit.

IT-Grundschutz-Kataloge

Die IT-Grundschutz-Kataloge beinhalten organisatorische, technische, personelle und infrastrukturelle Empfehlungen.

ISMS nach ISO 27001 Annex A -Alternative

IT-Sicherheitsmanagment ISO 27001



EU DSGVO Art. 32 – **Sicherheit der Verarbeitung**

Risikoanalyse

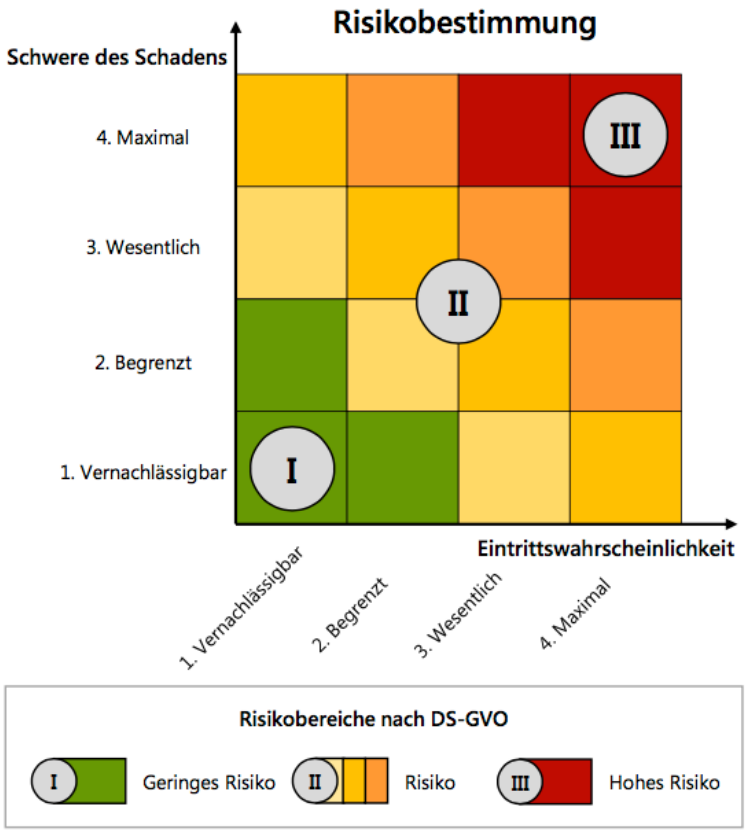
(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Risikoanalyse und -bewertung

New!

EU DSGVO Art. 32 – **Sicherheit der Verarbeitung**

Risikoanalyse



https://www.lda.bayern.de/media/baylda_ds-gvo_18_privacy_impact_assessment.pdf

EU DSGVO Art. 32 – **Sicherheit der Verarbeitung**

Risikoanalyse

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 100-3

Risikoanalyse auf der Basis von IT-Grundschutz

EU DSGVO Art. 32 – **Sicherheit der Verarbeitung**

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

„Codes of Conduct“
(Selbstverpflichtung)

EU DSGVO Erwägungsgrund 77 - **Verhaltensregeln**

(77) Anleitungen, wie der Verantwortliche oder Auftragsverarbeiter geeignete Maßnahmen durchzuführen hat und wie die Einhaltung der Anforderungen nachzuweisen ist, insbesondere was die Ermittlung des mit der Verarbeitung verbundenen Risikos, dessen Abschätzung in Bezug auf Ursache, Art, Eintrittswahrscheinlichkeit und Schwere und die Festlegung bewährter Verfahren für dessen Eindämmung betrifft, könnten insbesondere in Form von genehmigten Verhaltensregeln, genehmigten Zertifizierungsverfahren, Leitlinien des Ausschusses oder Hinweisen eines Datenschutzbeauftragten gegeben werden. Der Ausschuss kann ferner Leitlinien für Verarbeitungsvorgänge ausgeben, bei denen davon auszugehen ist, dass sie kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, und angeben, welche Abhilfemaßnahmen in diesen Fällen ausreichend sein können.

EU DSGVO Art. 40 - **Verhaltensregeln**

ABSCHNITT 5

VERHALTENSREGELN UND ZERTIFIZIERUNG

Datenschutzausschuss = ehem. Art. 29-Gruppe

Artikel 40

Verhaltensregeln

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen.

h) die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32;

EU DSGVO Art. 40 - **Verhaltensregeln**

Art. 29 - Gruppe ➔ Art. 29 der EU Datenschutzrichtlinie 95/46/EG

⬇

Europäischer Datenschutzausschuss (Art. 68 DSGVO)

„Es wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten eingesetzt. Die Gruppe ist unabhängig und hat beratende Funktion.“

Aufgaben*:*

- Prüfung der Rechtsumsetzung in den einzelnen Staaten, Mitwirkung an der Herstellung eines europaweit einheitlichen Schutzniveaus,
- Stellungnahmen zu Verhaltensregeln,
- Ausarbeitung von Empfehlungen

EU DSGVO Art. 40 - Verhaltensregeln

Aktuelle Leitlinien der Art. 29-Gruppe zur DSGVO:

- Datenübertragbarkeit (Art. 20 DSGVO) WP242*
- Zuständigkeit der federführenden Aufsichtsbehörde (Art. 56 DSGVO) WP243*
- Datenschutzbeauftragter (Art. 37 ff. DSGVO) WP 244*

Angekündigte Leitlinien der Art. 29-Gruppe zur DSGVO:

- Einwilligung (Art. 7 DSGVO)
- Profiling (Art. 22 DSGVO)
- Transparenz (Art. 12 DSGVO)
- Datenübermittlungen in Drittländer (Art. 44 ff. DSGVO)
- Mitteilungen bei Sicherheitsvorfällen (Art. 32 f. DSGVO)

**http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf*
**http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf*
**http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf*

EU DSGVO Erwägungsgründe 100, 166 – **Zertifizierung**

(100) Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.

(166) Um die Zielvorgaben dieser Verordnung zu erfüllen, d. h. die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz ihrer personenbezogenen Daten zu schützen und den freien Verkehr personenbezogener Daten innerhalb der Union zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen. Delegierte Rechtsakte sollten insbesondere in Bezug auf die für Zertifizierungsverfahren geltenden Kriterien und

EU DSGVO Art. 24, 25 – **Zertifizierung**

Artikel 24

Verantwortung des für die Verarbeitung Verantwortlichen

(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

EU DSGVO Art. 42 – **Zertifizierung**

Artikel 42

Zertifizierung

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.

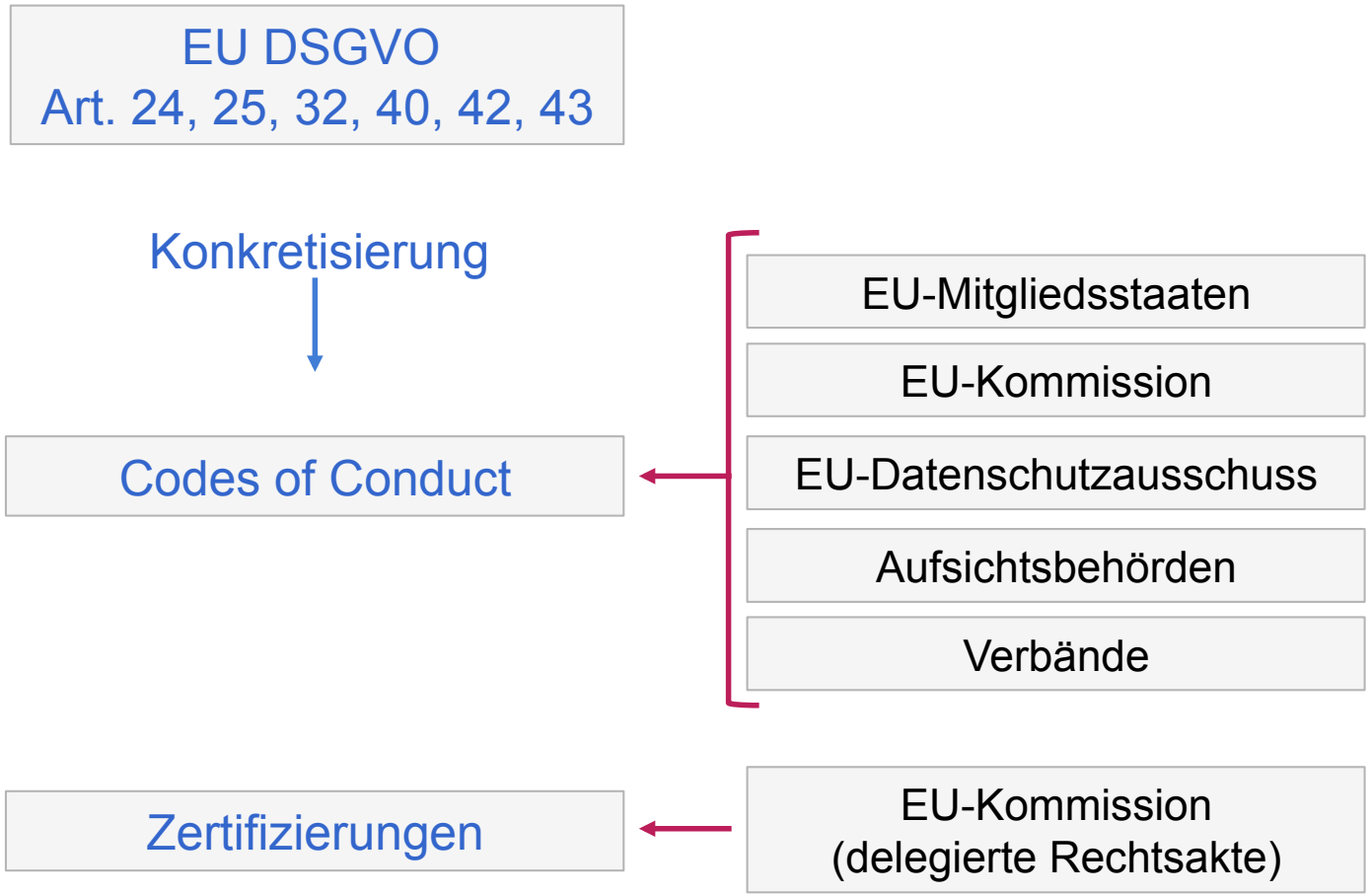
Zertifizierungsverfahren

Gütesiegel / Zertifikate

(8) Der Ausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen in ein Register auf und veröffentlicht sie in geeigneter Weise.

Art. 43 Abs. 8 EU DSGVO

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zu erlassen, um die Anforderungen festzulegen, die für die in Artikel 42 Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren zu berücksichtigen sind.


EU DSGVO
Art. 24, 25, 32, 40, 42, 43
Konkretisierung
Codes of Conduct
EU-Mitgliedsstaaten
EU-Kommission
EU-Datenschutzausschuss
Aufsichtsbehörden
Verbände
Zertifizierungen
EU-Kommission
(delegierte Rechtsakte)

Was ist zu erwarten?

EU-Mitgliedsstaaten

EU-Kommission

EU-Datenschutzausschuss

Aufsichtsbehörden

Verbände

Codes of Conduct

z.B.:

BSI:

BSI Standards 100-1 bis 4

Common Criteria

ISO / IEC 15408

- EU-Mitgliedsstaaten
- EU-Kommission
- EU-Datenschutzausschuss
- Aufsichtsbehörden
- Verbände

Codes of Conduct

z.B.:

ENISA:
Leitlinien für Sicherheitsmaßnahmen Zu Art. 4/13 der e-Privacy-Richtlinie (2992/58/EC)

EuroPrise:
Sichereheitsmaßnahmen nach dem Europäischen Datenschutzsiegel

2013/0027 (COD):
Entwurf EU-Richtlinie zur Netzwer-Informationssicherheit

EU-Mitgliedsstaaten

EU-Kommission

Codes of Conduct ← EU-Datenschutzausschuss

Aufsichtsbehörden

Verbände

z.B.:

DSB-Konferenez (D)

CNIL (F)

[…]

Standard Datenschutzmodell

Good Practice Catalogue

[…]

Art. 29-Gruppe

EU-Mitgliedsstaaten

EU-Kommission

EU-Datenschutzausschuss

Aufsichtsbehörden

Verbände

Codes of Conduct

GDD

Gesellschaft für Datenschutz und Datensicherheit e.V.

BvD e.V.

Die Datenschützer

Standard "Anforderungen an Auftragnehmer nach § 11 BDSG"

- DATENSCHUTZSTANDARD DS-BvD-GDD-01 -

GESELLSCHAFT FÜR DATENSCHUTZ UND DATENSICHERHEIT (GDD) E.V. /
BERUFSVERBAND DER DATENSCHUTZBEAUFTRAGTEN DEUTSCHLANDS (BVD) E.V.

Version Stand: 07.09.2012

Verhaltensregeln
für den Umgang mit personenbezogenen Daten
durch die deutsche Versicherungswirtschaft

I. EINLEITUNG

Der Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) mit Sitz in Berlin ist die Dachorganisation der privaten Versicherer in Deutschland. Ihm gehören über 450 Mitgliedsunternehmen an. Diese bieten als Risikoträger Risikoschutz und Unterstützung sowohl für private Haushalte als auch für Industrie, Gewerbe und öffentliche Einrichtungen. Der Verband setzt sich für alle die Versicherungswirtschaft betreffenden Fachfragen und für ordnungspolitische Rahmenbedingungen ein, die den Versicherern die optimale Erfüllung ihrer Aufgaben ermöglichen.

Die Versicherungswirtschaft ist von jeher darauf angewiesen, in großem Umfang personenbezogene Daten der Versicherten zu verwenden. Sie werden zur Antrags-, Vertrags- und Leistungsabwicklung erhoben, verarbeitet und genutzt um Versicherte zu betreuen und zu beraten sowie um das zu versichernde Risiko einzuschätzen, die Leistungspflicht zu prüfen und Versicherungsmissbrauch im Interesse der Versichertengemeinschaft zu verhindern. Versicherungen können dabei heute ihre Aufgaben nur noch mit Hilfe der elektronischen Datenverarbeitung erfüllen.

Die Wahrung der informationellen Selbstbestimmung und der Schutz der Privatsphäre sowie die Sicherheit der Datenverarbeitung sind für die Versicherungswirtschaft ein Kernanliegen, um das Vertrauen der Versicherten zu gewährleisten. Alle Regelungen müssen nicht nur im Einklang mit den Bestimmungen der Europäischen Datenschutzrichtlinie, des Bundesdatenschutzgesetzes und aller bereichsspezifischen Vorschriften über den Datenschutz stehen, sondern die beigetretenen Unternehmen der Versicherungswirtschaft verpflichten sich darüber hinaus, den Grundsätzen der Transparenz, der Erforderlichkeit der verarbeiteten Daten und der Datenvermeidung und -sparsamkeit in besonderer Weise nachzukommen.

Hierzu hat der GDV im Einvernehmen mit seinen Mitgliedsunternehmen die folgenden Verhaltensregeln für den Umgang mit den personenbezogenen Daten der Versicherten aufgestellt. Sie schaffen für die Versicherungswirtschaft weitestgehend einheitliche Standards und fördern die Einhaltung von datenschutzrechtlichen Regelungen. Die für die Mitgliedsunternehmen zuständigen Aufsichtsbehörden haben den Verhaltensregeln zugestimmt. Daraufhin sind sie dem Beirrer Beauftragten für Datenschutz und Informationsfreiheit als für den GDV zuständige Aufsichtsbehörde nach § 38 a Bundesdatenschutzgesetz unterstellt und von ihm als mit dem geltenden Datenschutzrecht vereinbar erklärt worden. Die Mitgliedsunternehmen des GDV, die diesen Verhaltensregeln gemäß Artikel 30 beitreten, verpflichten sich damit zu deren Einhaltung.

Die Verhaltensregeln sollen den Versicherten der beigetretenen Unternehmen die Gewähr bieten, dass Datenschutz- und Datensicherheitsbelange bei der Gestaltung und Bearbeitung von Produkten und Dienstleistungen berücksichtigt werden. Der GDV versichert seine Unterstützung bei diesen Anliegen. Die beigetretenen Unternehmen weisen ihre Führungskräfte und ihre Mitarbeiterinnen und Mitarbeiter an, die Verhaltensregeln einzuhalten. Antragsteller und Versicherte werden über die Verhaltensregeln informiert.

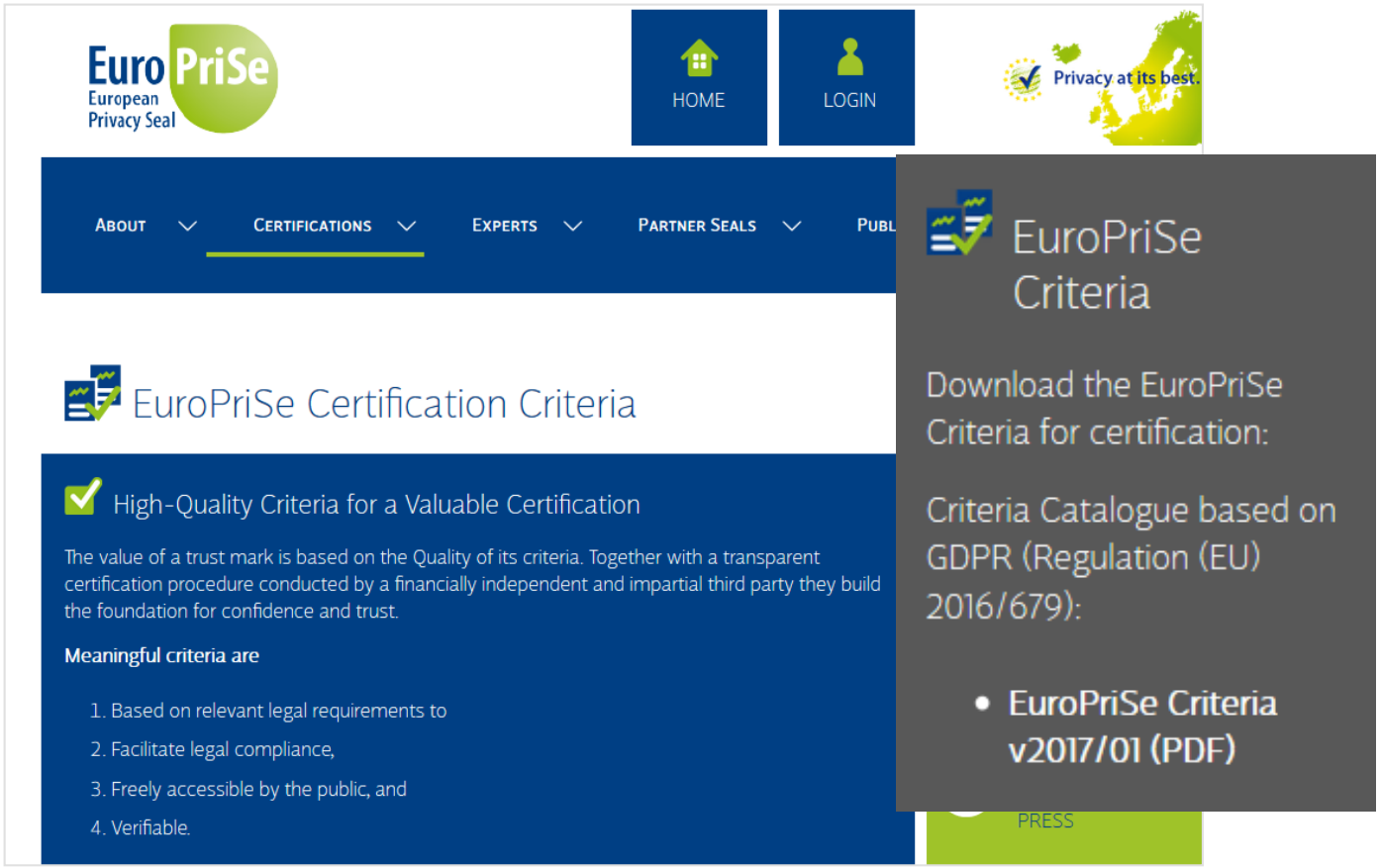
z.B.:
Datenschutzstandard DS-BvD-GDD-01

CoC Versicherungswirtschaft
CoC Online-Werbung

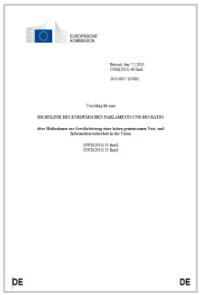
[…]

Zertifizierungen

EU-Kommission
(delegierte Rechtsakte)



https://www.european-privacy-seal.eu/EPS-en/Criteria



- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Authentizität
- Revisionsfähigkeit
- Systemdatenschutz
- Audit / Zertifizierung

Common Criteria

Sicherheitsmanagement

ISO/IEC 27001	Information security management systems – Requirements Informationssicherheits-Managementsysteme– Anforderungen
ISO/IEC 27002	Code of practice for information security management Leitfaden zum Informationssicherheitsmanagement
ISO/IEC 27005	Information security risk management Informationssicherheits-Risikomanagement
ISO/IEC 27014	Governance of information security Governance von Informationssicherheit

BDSG / LDSG

Rechtsanpassung:

BDSG-Neu ?
LDSG-Neu ?
DS-Regelungen in SpezialG neu ?

Mai 2016

Verabschiedung
EU DSGVO

25. Mai 2018

In-Kraft-Treten
EU DSGVO

Technische Datenschutzvorgaben:

Codes of Conduct ?
Best Practice ?
Audit/Zertifizierung ?

Neu! Bußgeld.

Derzeitige Situation § 38 Abs. 5 BDSG

Bundesdatenschutzgesetz (BDSG)
§ 38 Aufsichtsbehörde

(1) Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5. Sie berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten und nutzen; § 14 Abs. 2 Nr. 1 bis 3, 6 und 7 gilt entsprechend. Insbesondere darf die Aufsichtsbehörde zum Zweck der Aufsicht Daten an andere Aufsichtsbehörden übermitteln. Sie leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe). Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie befugt, die Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten. Sie veröffentlicht regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht. § 21 Satz 1 und § 23 Abs. 5 Satz 4 bis 7 gelten entsprechend.
(2) Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1. Das Register kann von jedem eingesehen werden. Das Einsichtsrecht erstreckt sich nicht auf die Angaben nach § 4e Satz 1 Nr. 9 sowie auf die Angabe der zugriffsberechtigten Personen.
(3) Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.
(4) Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. § 24 Abs. 6 gilt entsprechend. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.
(5) Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.
(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.
(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnittes unterliegenden Gewerbebetriebe bleibt unberührt.

- Schwerwiegender techn.-org. Mangel
- Anordnungsverfahren
- Zwangsgeldandrohung
- Zwangsgeldverhängung

Bußgeld

EU DSGVO Art. 83

Artikel 83

Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43;

New!

Technisch-organisatorische Maßnahmen

Datenschutzmanagment

Agenda

- Datenschutzfolgeabschätzung

Bundesdatenschutzgesetz (BDSG)
§ 4d Meldepflicht

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.
(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.
(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.
(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zweck der Übermittlung,
2. zum Zweck der anonymisierten Übermittlung oder
3. für Zwecke der Markt- oder Meinungsforschung

gespeichert werden.
(5) Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder
2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.
(6) Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu wenden.

EU Datenschutzrichtlinie 95/46

- Erwägungsgrund (53)

> *Bestimmte Verarbeitungen können jedoch aufgrund ihrer Art, ihrer Tragweite oder ihrer Zweckbestimmung - wie beispielsweise derjenigen, betroffene Personen von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrags auszuschließen - oder aufgrund der besonderen Verwendung einer neuen Technologie* ***besondere Risiken*** *im Hinblick auf die Rechte und Freiheiten der betroffenen Personen aufweisen.*

Hintergrund

EU Datenschutzrichtlinie 95/46

- Erwägungsgrund (53)
  Art der Daten
  Tragweite (z.B. Automatisierte Einzelentscheidung,
  (neue) **Technologie**

- Art. 20 Vorabkontrolle
  Verarbeitungen mit spezifischen Risiken
  Prüfung **vor** Aufnahme des Verfahrens

Hintergrund

EU Datenschutzrichtlinie 95/46

- Erwägungsgrund (53)
  Art der Daten
  Tragweite (z.B. Automatisierte Einzelentscheidung,
  (neue) **Technologie**

Artikel 20 Vorabkontrolle

*(1) Die Mitgliedstaaten legen fest, **welche Verarbeitungen** spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können, und tragen dafür Sorge, daß diese Verarbeitungen vor ihrem Beginn geprüft werden.*
*(2) Solche Vorabprüfungen nimmt die Kontrollstelle nach Empfang der Meldung des für die Verarbeitung Verantwortlichen vor, oder sie erfolgen durch den **Datenschutzbeauftragten**, der im Zweifelsfall die Kontrollstelle konsultieren muß.*

Hintergrund

EU Datenschutzrichtlinie 95/46

- Erwägungsgrund (53)
  Art der Verarbeitung (vgl. § 29a, 29b DSG NRW)
  Tragweite (z.B. Automatisierte Einzelentscheidung,

- Art. 20 Vorabkontrolle
  Verarbeitungen mit spezifischen Risiken
  Prüfung vor Aufnahme des Verfahrens

Umsetzung in nationales Recht

- BDSG ➔ § 4 d Abs. 5 BDSG
- LDSGe ➔ § 9 Abs. 5 LDSG i.V.m. § 3 Abs. 9 LDSG

Prüfungsgesichtspunkte der Vorabkontrolle

- **inhaltliche / rechtliche Anforderungen**
- **formale Anforderungen**
- **technisch-organisatorische Anforderungen**

Vorabkontrolle- Inhaltliche Anforderungen

- **Zulässigkeit (Rechtsgrundlage/Einwilligung)**
- **Grundsätze der Datensparsamkeit und Datenvermeidung**

  Datenumfang
  Personenbezug / Pseudonymisierung

- **Voraussetzungen für die Verarbeitung besonderer personenbezogener Daten**
- **Wahrung/Gewährleistung der Rechte der Betroffenen**

  Beteiligung, Auskunft, Sperrung

Vorabkontrolle- Inhaltliche Anforderungen

- **Auftragsdatenverarbeitung**

  schriftlicher Auftrag
  Gewährleistung Sicherheitsmaßnahmen
  Wahrnehmung der Kontrollpflichten
  Verpflichtung
  ggf. Unterrichtung/Genehmigung der Aufsichtsbbehörde
  Berücksichtigung besonderer Berufs- und Amtsgeheimnisse

- **Löschung**

  Erforderlichkeit
  Fristen

Vorabkontrolle- Formale Anforderungen

- **Verfahrensverzeichnis**
- **Anhörung des LfD**
- **Zulassungen soweit erforderlich**
- **Information / Unterrichtung des Betroffenen**
- **Dienstanweisung**
- **Verpflichtung**

Vorabkontrolle- Technisch-organisatorische Anforderungen

- **Technisch-organisatorische Maßnahmen** **§ 9 Abs. 2 LDSG**

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Zweckbindungskontrolle
- Dokumentationskontrolle
- Verarbeitungskontrolle

→

Kernbereiche

- Benutzerverwaltung
- Berechtigungskonzept
- Dokumentation
- Protokollierung
- Löschung

Art 35 EU DSGVO - Datenschutzfolgeabschätzung

Artikel 35

Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Technologie, Art+Umfang, Umstände, Zweck ...

Art 35 EU DSGVO - Datenschutzfolgeabschätzung

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

z.B. Scoring

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

z.B. Geschäfts-zweck

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;

z.B. Video-überwachung

Art 35 EU DSGVO - Datenschutzfolgeabschätzung

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

Art 35 EU DSGVO - Datenschutzfolgeabschätzung

(7) Die Folgenabschätzung enthält zumindest Folgendes:

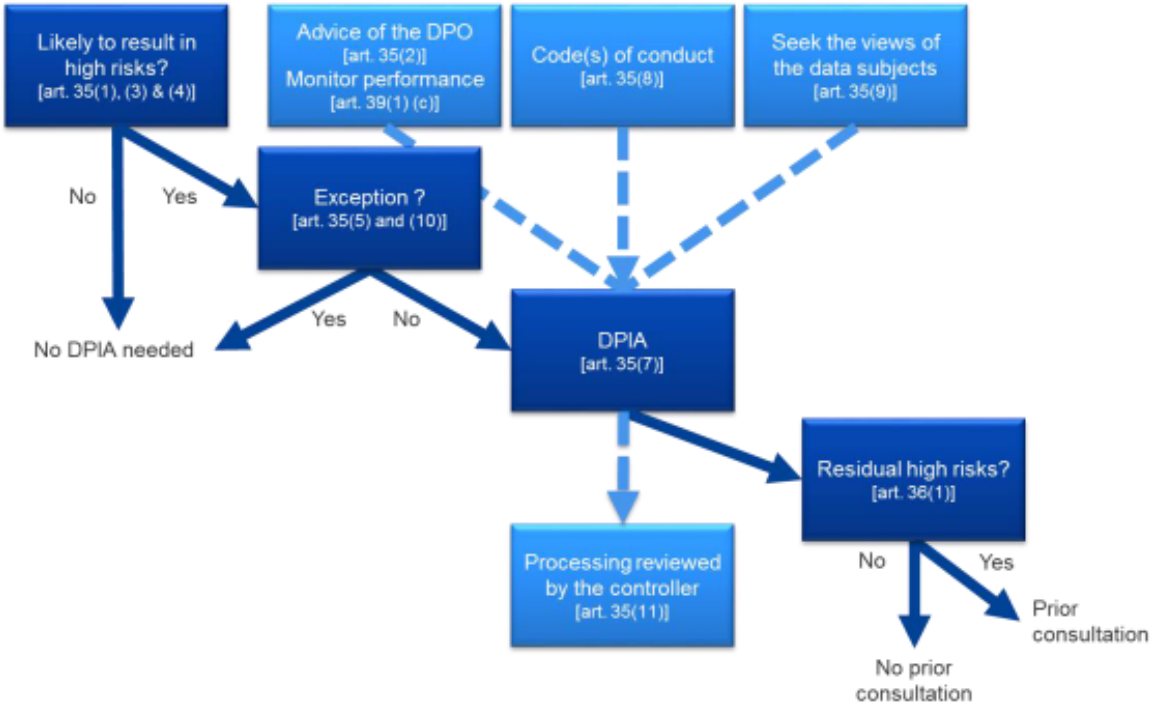
a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

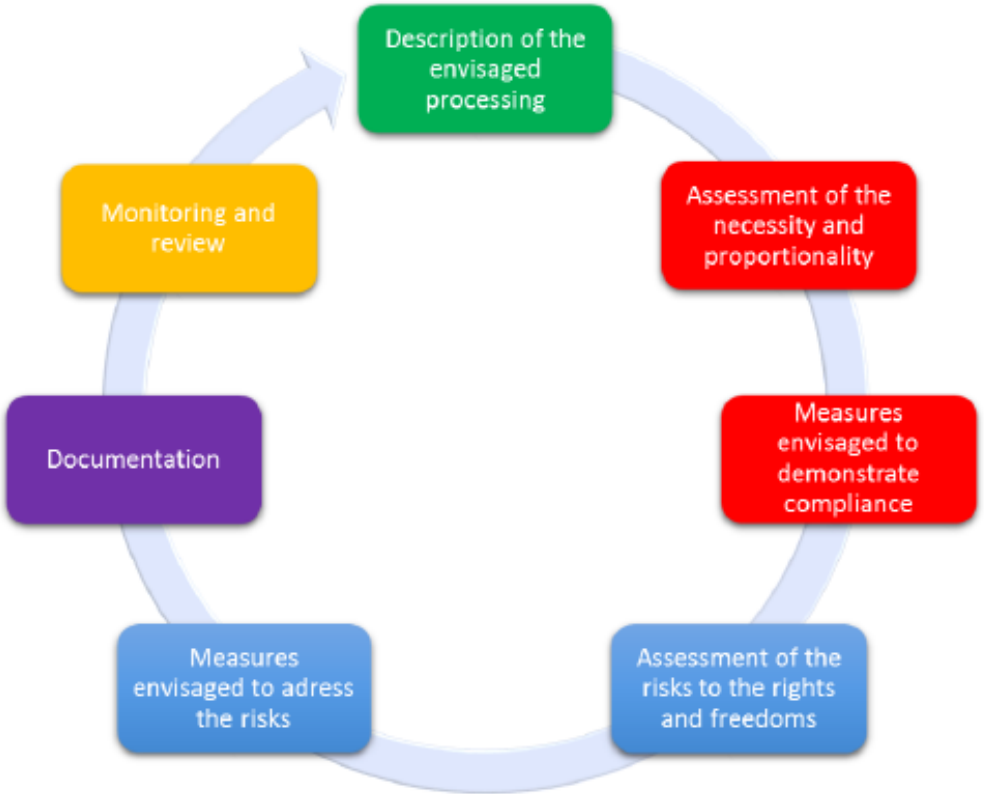
d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Art 35 EU DSGVO - Datenschutzfolgeabschätzung



https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_on_data_protection_impact_assessment_dpia.pdf

Art 35 EU DSGVO - Datenschutzfolgeabschätzung



https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_on_data_protection_impact_assessment_dpia.pdf

Neu! Bußgeld.

EU DSGVO Art. 30

Artikel 83

Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

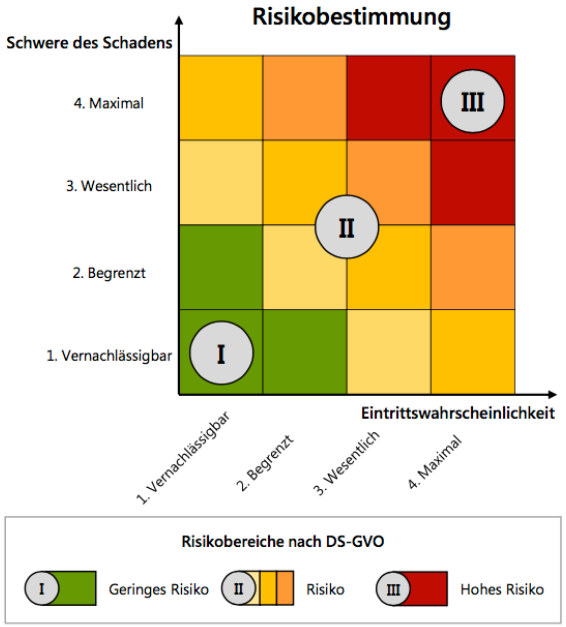
New!

Datenschutzfolgeabschätzung

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43;

EU DSGVO Art. 35 – **Datenschutzfolgeabschätzung**

Risikoanalyse



https://www.lda.bayern.de/media/baylda_ds-gvo_18_privacy_impact_assessment.pdf

- Verfahrensverzeichnis

Bundesdatenschutzgesetz (BDSG)
§ 4e Inhalt der Meldepflicht

Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

§ 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.

EU DSGVO Erwägungsgrund 82

(82) Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.

Art. 30 EU DSGVO Verfahrensverzeichnis

Artikel 30

Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

Art. 30 EU DSGVO Verfahrensverzeichnis

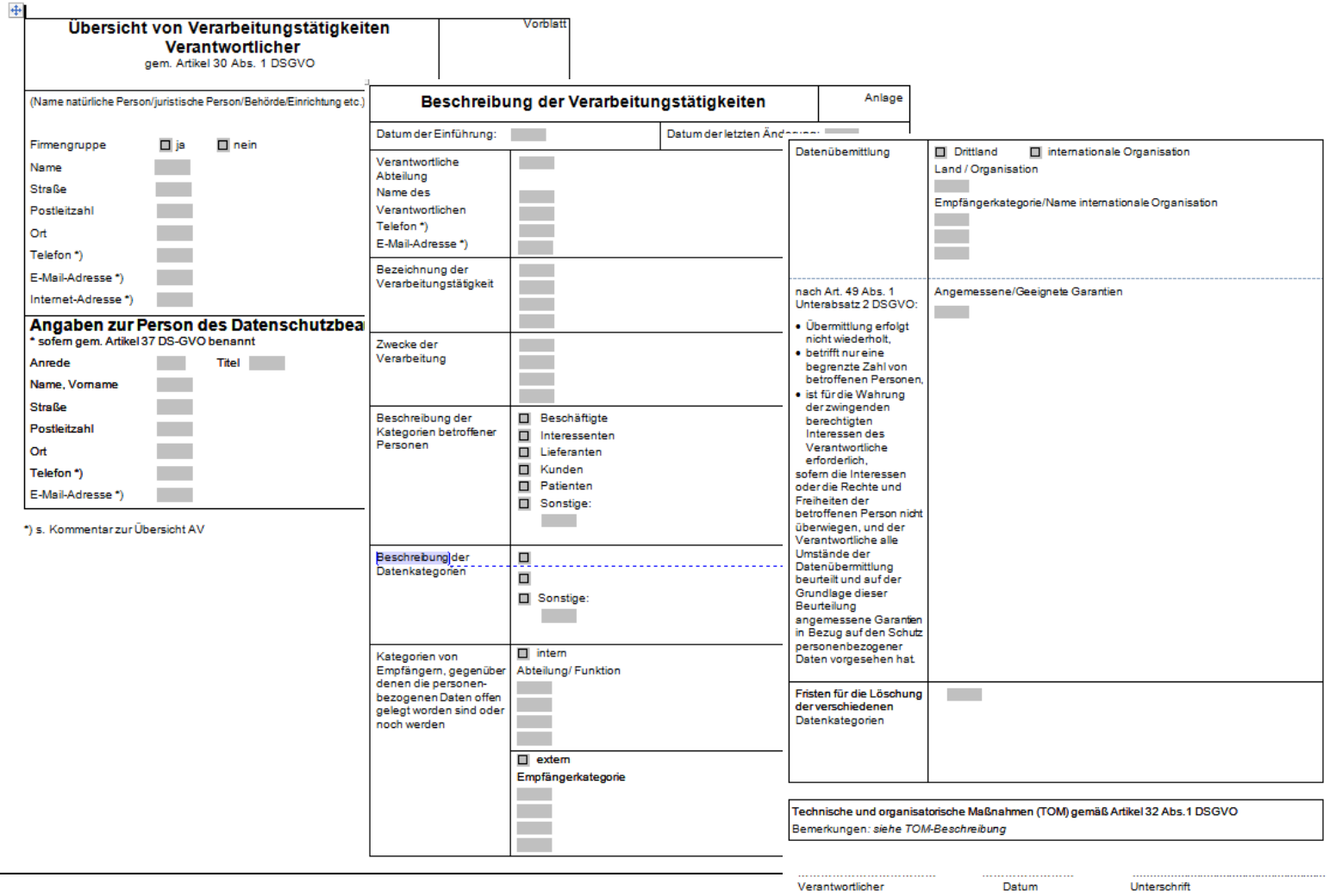
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Art. 30 EU DSGVO Verfahrensverzeichnis - Muster



Übersicht von Verarbeitungstätigkeiten
Verantwortlicher
gem. Artikel 30 Abs. 1 DSGVO

Vorblatt

(Name natürliche Person/juristische Person/Behörde/Einrichtung etc.)

Firmengruppe ☐ ja ☐ nein
Name
Straße
Postleitzahl
Ort
Telefon *)
E-Mail-Adresse *)
Internet-Adresse *)

Angaben zur Person des Datenschutzbea
* sofern gem. Artikel 37 DS-GVO benannt

Anrede Titel
Name, Vorname
Straße
Postleitzahl
Ort
Telefon *)
E-Mail-Adresse *)

*) s. Kommentar zur Übersicht AV

Beschreibung der Verarbeitungstätigkeiten

Anlage

Datum der Einführung:
Datum der letzten Änderung:

Verantwortliche Abteilung Name des Verantwortlichen Telefon *) E-Mail-Adresse *)	
Bezeichnung der Verarbeitungstätigkeit	
Zwecke der Verarbeitung	
Beschreibung der Kategorien betroffener Personen	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ Sonstige:
Beschreibung der Datenkategorien	☐ ☐ ☐ Sonstige:
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden	☐ intern Abteilung/ Funktion ☐ extern Empfängerkategorie

Datenübermittlung	☐ Drittland ☐ internationale Organisation Land / Organisation Empfängerkategorie/Name internationale Organisation
nach Art. 49 Abs. 1 Unterabsatz 2 DSGVO: • Übermittlung erfolgt nicht wiederholt, • betrifft nur eine begrenzte Zahl von betroffenen Personen, • ist für die Wahrung der zwingenden berechtigten Interessen des Verantwortliche erforderlich, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung angemessene Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat.	Angemessene/Geeignete Garantien
Fristen für die Löschung der verschiedenen Datenkategorien	

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs. 1 DSGVO
Bemerkungen: *siehe TOM-Beschreibung*

Verantwortlicher ..... Datum ..... Unterschrift .....

Art. 30 EU DSGVO Verfahrensverzeichnis - Muster

Technische und organisatorische Maßnahmen
gemäß Artikel 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

1. Pseudonymisierung

2. Verschlüsselung

3. Gewährleistung der Vertraulichkeit

4. Gewährleistung der Integrität

5. Gewährleistung der Verfügbarkeit

6. Gewährleistung der Belastbarkeit der Systeme

7. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Es liegen schriftlich vor
- ☐ interne Verhaltensregeln
- ☐ Risikoanalyse
- ☐ allgemeine Datensicherheitsbeschreibung
- ☐ umfassendes Datensicherheitskonzept
- ☐ Wiederanlaufkonzept
- ☐ Zertifikat:
  Zertifizierungsstelle:
- ☐ Sonstiges:

Datum _____ Unterschrift: _____

Art. 30 EU DSGVO Verfahrensverzeichnis

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

Art. 30 EU DSGVO Verfahrensverzeichnis

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

➔ Nicht bei weniger als 250 Mitarbeitern
es sei denn:
Risiko für Rechte und Freiheiten
und
- nicht nur gelegentlich oder
- Daten besonderer Kategorien nach Art. 9

EU DSGVO Erwägungsgrund (89)

(89) Gemäß der Richtlinie 95/46/EG waren Verarbeitungen personenbezogener Daten bei den Aufsichtsbehörden generell meldepflichtig. Diese Meldepflicht ist mit einem bürokratischen und finanziellen Aufwand verbunden und hat dennoch nicht in allen Fällen zu einem besseren Schutz personenbezogener Daten geführt. Diese unterschiedslosen allgemeinen Meldepflichten sollten daher abgeschafft und durch wirksame Verfahren und Mechanismen ersetzt werden, die sich stattdessen vorrangig mit denjenigen Arten von Verarbeitungsvorgängen befassen, die aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen. Zu solchen Arten von Verarbeitungsvorgängen

Neu! Bußgeld.

EU DSGVO Art. 30

Artikel 83

Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

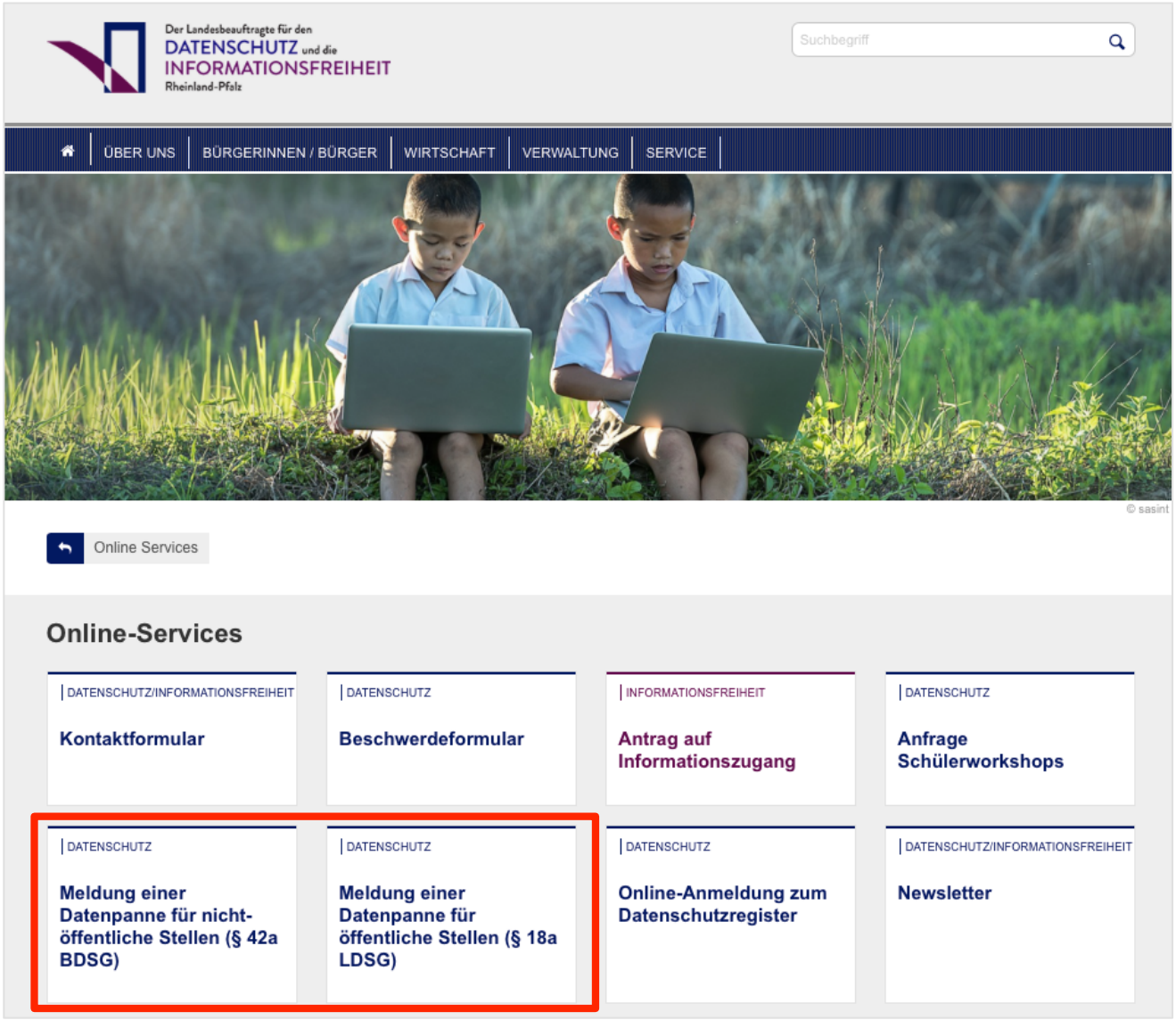
New!

Verfahrensverzeichnis

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43;

- Verfahren bei Datenpannen

Situation heute ...


Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz
Suchbegriff
ÜBER UNS
BÜRGERINNEN / BÜRGER
WIRTSCHAFT
VERWALTUNG
SERVICE
© sasint
Online Services
Online-Services
DATENSCHUTZ/INFORMATIONSFREIHEIT
Kontaktformular
DATENSCHUTZ
Beschwerdeformular
INFORMATIONSFREIHEIT
Antrag auf Informationszugang
DATENSCHUTZ
Anfrage Schülerworkshops
DATENSCHUTZ
Meldung einer Datenpanne für nicht-öffentliche Stellen (§ 42a BDSG)
DATENSCHUTZ
Meldung einer Datenpanne für öffentliche Stellen (§ 18a LDSG)
DATENSCHUTZ
Online-Anmeldung zum Datenschutzregister
DATENSCHUTZ/INFORMATIONSFREIHEIT
Newsletter

§ 42a BDSG – **Meldung Datenpanne**

Voraussetzungen

- Risikodaten
(besondere Arten pb Daten, Berufsgeheimnisse,
Bank-/Kreditkartenkonten, Straftaten/Ordnungswidrigkeiten)

- Unrechtmäßige Kenntniserlangung Dritter

- Schwerwiegende Beeinträchtigung
der Interessen Betroffener

§ 42a BDSG – **Meldung Datenpanne**

Pflichten

- Sicherungsmaßnahmen
- Unverzügliche Unterrichtung der Aufsichtsbehörde
  - Darlegung des Vorfall
  - Darlegung der Folgen
  - Maßnahmen zur Folgenminderung
- Benachrichtigung der Betroffenen (ggf. via Tageszeitungen)
  - Darlegung des Vorfalls
  - Empfehlungen zur Folgenminderung

Situation ab Mai 20128 ...

Informationspflichten bei Datenpannen – **Art. 33, 34 DSGVO**

Voraussetzungen

- Verletzung des Schutzes pb Daten
  - ➡ Art. 4 Nr.12 DSGVO:
    Vernichtung, Verlust, Veränderung,
    unbefugte Offenlegung,
    unbefugter Zugang,
    unrechtmäßig/unbeabsichtigt

- Nicht allein „Risikodaten“ (Art. 9 DSGVO)
- Nicht nur bei schwerwiegenden Beeinträchtigungen der Interessen Betroffener

New!

Informationspflichten bei Datenpannen – **Art. 33, 34 DSGVO**

Ausnahme

- Kein Risiko für Rechte und Freiheiten natürlicher Personen

➡ Risikoabschätzung
Erwägungsgrund 75 (Risikogründe)

New!

physischer, materieller, immaterieller Schaden
Verlust der Rechte und Freiheiten, Kontrollverlust
Verarbeitung besondere Kategorien pb Daten,
Persönlichkeitsbewertung, Profilbildung,
Daten Minderjähriger,
große Datenmenge,
große Anzahl Betroffene

Ausnahme

- Kein Risiko für Rechte und Freiheiten natürlicher Personen

  ➡ Risikoabschätzung
  Erwägungsgrund 75 (potentielle Risikogründe)
  wenn
  Diskriminierung, Rufschädigung, Identitätsdiebstahl,
  finanzieller Schaden, Vertraulichkeit von Berufsgeheimnissen,
  Aufhebung der Pseudonymisierung,
  erhebliche wirtschaftliche/gesellschaftliche Nachteile,
  möglich

Informationspflichten bei Datenpannen – **Art. 33, 34 DSGVO**

Wenn kein Risiko ➡ keine Meldung!

Nicht: Wenn geringes Risiko!

Beispiele: verschlüsselte Daten
starke Pseudonymisierung

Art. 35 Abs. 5: Dokumentationspflicht
für alle Verletzungen des Schutzes
personenbezogener Daten

Informationspflichten bei Datenpannen – **Art. 33, 34 DSGVO**

Wenn voraussichtlich hohes Risiko

➡ unverzügliche, direkte Unterrichtung der Betroffenen

Informationen nach Art. 33 Abs. 3 lit. b – d:

- Kontaktdaten bDSB
- mögliche Folgen
- ergriffene Maßnahmen

Absehen von der Unterrichtung (Art. 34 Abs. 3 lit. b):

- verschlüsselter Daten
- Risikoausschaltung
- unverhältnismäßiger Aufwand (➡ öffentlich)

Informationspflichten bei Datenpannen – **Art. 33, 34 DSGVO**

Meldung an die Aufsichtsbehörde

- Unverzüglich (binnen 72 Stunden)
- Darlegung des Vorfall
- Darlegung der Folgen
- Maßnahmen zur Folgenminderung
- Beschreibung der Datenkategorien
- Anzahl betroffener Datensätze

Informationspflichten bei Datenpannen – **Art. 33, 34 DSGVO**

Meldung des Auftrag-Datenverarbeiters

➡ in allen Fällen an den Auftraggeber
Unterstützungspflicht (Art. 28 Abs. 3 lit. f)

EU DSGVO Art. 30

Artikel 83

Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

Meldepflichten

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43;

EU DSGVO Art. 40 - Verhaltensregeln

Aktuelle Leitlinien der Art. 29-Gruppe zur DSGVO:

- Datenübertragbarkeit (Art. 20 DSGVO) WP242*
- Zuständigkeit der federführenden Aufsichtsbehörde (Art. 56 DSGVO) WP243*
- Datenschutzbeauftragter (Art. 37 ff. DSGVO) WP 244*

Angekündigte Leitlinien der Art. 29-Gruppe zur DSGVO:

- Einwilligung (Art. 7 DSGVO)
- Profiling (Art. 22 DSGVO)
- Transparenz (Art. 12 DSGVO)
- Datenübermittlungen in Drittländer (Art. 44 ff. DSGVO)
- Mitteilungen bei Sicherheitsvorfällen (Art. 32 f. DSGVO)

*http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf
*http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
*http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Helmut Eiermann

Stellvertretender Datenschutzbeauftragter / Leiter Bereich Technik

Postanschrift:	Postfach 30 40 55020 Mainz
Büroanschrift:	Hintere Bleiche 34 55116 Mainz
Telefon:	+49 (6131) 208-2226
Telefax:	+49 (6131) 208-2497
E-Mail:	h.eiermann@datenschutz.rlp.de
Web:	www.datenschutz.rlp.de