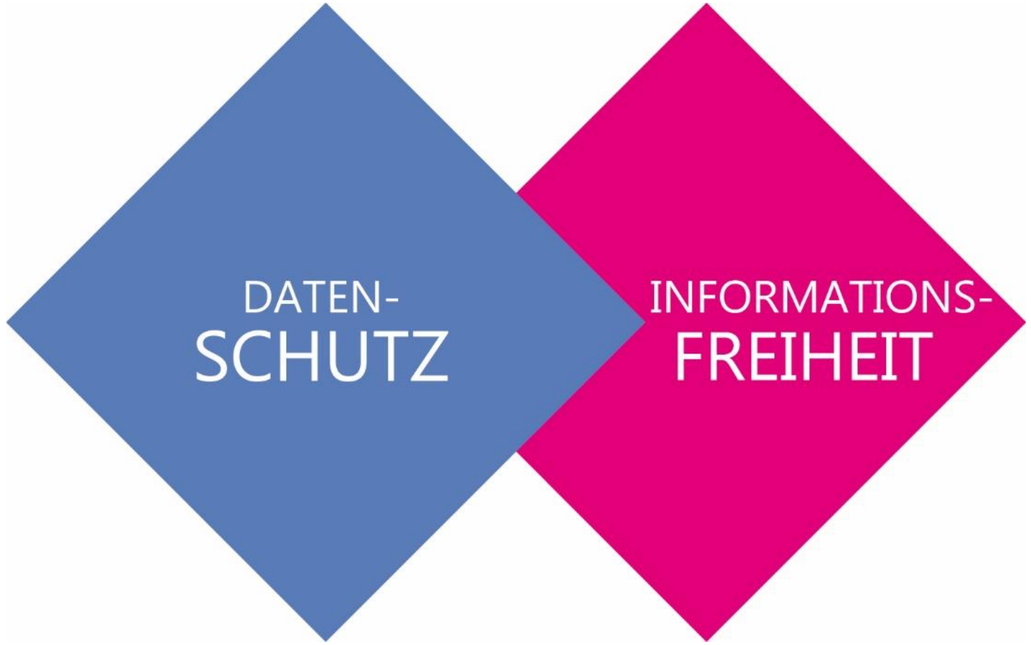


Das neue Datenschutzrecht

Die Datenschutz-Grundverordnung (DS-GVO)

UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

Disclaimer

Dieser Vortrag dient als erste Orientierung wie nach derzeitiger Auffassung des UDZ Saarland die DS-GVO im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung der deutschen Aufsichtsbehörden und des Europäischen Datenschutzausschusses.

Zielgruppe der Präsentation

- DS-GVO gilt u.a. für alle Unternehmen und deren Niederlassungen in der EU, die als Verantwortliche personenbezogene Daten verarbeiten.
- Personenbezogene Daten sind Daten von identifizierten oder identifizierbaren natürlichen Personen.
- Verantwortlicher ist jede natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

DS-GVO
Struktur des EU-Datschutzrechtes

Die Datenschutz-Grundverordnung ist ab dem 25. Mai 2018 in Deutschland unmittelbar anzuwendendes Recht.

Regel: In den dort geregelten Bereichen kann es kein abweichendes nationales Recht geben.

Ausnahme: Die DS-GVO sieht eine Öffnungsklausel vor (Beispiele: Datenschutzbeauftragte, Medien oder Beschäftigtendatenschutz).

Aufbau der Gesetze

EU-Datenschutz					
Datenschutz-Grundverordnung			E-Privacy-Richtlinie (künftig Verordnung)		
BDSG-neu	SDSG-neu (Landesrecht)	Bereichs-spezifisches Recht	TKG	TMG	UWG

DS-GVO – Erwägungsgründe – BDSG-neu

Die Artikel der Verordnung sind im Zusammenhang mit den dazugehörigen Erwägungsgründen (ErwGr.) zu lesen.

Diese sind integraler Bestandteil der Verordnung und enthalten etwa Definitionen oder weitere Ausführungen.

Das BDSG-neu enthält Regelungen zu den in der DS-GVO enthaltenen Öffnungsklauseln.

Exkurs: Prüfungsschema

1. Ist der Anwendungsbereich der DS-GVO eröffnet?
2. Eröffnet die spezifische Regelung den Mitgliedsstaaten einen Regelungsspielraum?
    a. Wenn nein > Anwendung der DS-GVO
    b. Wenn ja > Wurde der Regelungsspielraum genutzt?
        i. Wenn nein > Anwendung der DS-GVO.
        ii. Wenn ja > Ist die nationale Regelung mit der DS-GVO vereinbar?

Zum Einstieg:

7-Punkte-Plan

7-Punkte-Plan

1. Sensibilisierung für den Datenschutz
2. Verantwortlichkeit und Strukturen
3. Risikoanalyse „DS-GVO“
4. GAP-Analyse (Soll-Ist-Abgleich)
5. Bestandsaufnahme (Ist-Zustand)
6. Änderungen durch die DS-GVO (Soll-Zustand)
7. Planung der Unternehmensprozesse

1. Sensibilisierung für den Datenschutz im Unternehmen

UNABHÄNGIGES DATENSCHUTZ ZENTRUM SAARLAND

1. Sensibilisierung für den Datenschutz

Geschäftsführungen, Datenschutzbeauftragte und andere für das Thema Datenschutz Zuständige sollten innerhalb des Unternehmens dafür sensibilisieren, dass sich ab dem 25. Mai 2018 nicht nur der Name einer europäischen Datenschutzregelung ändert, sondern die DS-GVO direkte Auswirkungen auf Unternehmen als datenverarbeitende Stellen haben wird.

1. Sensibilisierung für den Datenschutz

Die DS-GVO bringt zahlreiche neue Anforderungen mit sich, die sich auf eine Vielzahl von Unternehmensbereichen auswirken (z.B. IT, Personal, Compliance, Recht, Revision oder Vertrieb).

An erster Stelle steht daher die unternehmensinterne Kommunikation.

Praxis-Tipp

- Alle Entscheidungsträger in einem Unternehmen sollten sich der Auswirkungen der DS-GVO bewusst sein und wissen, was dies für den alltäglichen Betrieb in ihrem Unternehmen bedeutet.
- Sofern dies noch nicht der Fall ist, sollte der betrieblichen Datenschutzbeauftragte und/oder der IT-Verantwortliche die Geschäftsleitung informieren.

Praxis-Tipp

- Umgekehrt sollte der Datenschutzbeauftragte in alle Frage, die mit dem Schutz personenbezogener Daten zusammenhängen, rechtzeitig eingebunden werden.
- Die Mitarbeiter sollten weiterhin auf das Datengeheimnis verpflichtet werden, auch wenn dies in der DS-GVO nicht mehr ausdrücklich geregelt ist. Dies kann auch eine erste Maßnahme zur Sensibilisierung der Mitarbeiter darstellen.

2. Verantwortlichkeit und Struktur bei der Umsetzung der DS-GVO

2. Verantwortlichkeit und Struktur

Mit Geltung der DS-GVO haben sich Unternehmen bei der Verarbeitung personenbezogener Daten erstmals unmittelbar an europäisches Recht zu halten. Dies führt teilweise zu einer Verschiebung der datenschutzrechtlichen Zuständigkeiten und Verantwortlichkeiten bei den Daten verarbeitenden Unternehmen. Daher sollten die Verantwortlichkeiten und Strukturen im Unternehmen bei der Umsetzung der DS-GVO vorab geklärt werden.

Exkurs: Accountability
Definition

- Verlagerung der Verantwortung für den Schutz der Privatsphäre auf den Datenverarbeiter
- Klare Zielvorgaben des Gesetzgebers (dazu später)
- Wie die vorgegebenen Ziele erreicht werden, bleibt dem Ermessen des Datenverarbeiters überlassen

Spielraum, um Technologie und Geschäftsmodell datenschutzfreundlich auszugestalten

Exkurs: Accountability
Ziel

- Eigenverantwortung und Rechenschaftspflicht zwei Seiten der gleichen Medaille
- Rechenschaft macht Eigenverantwortung erst überprüfbar

angemessene und wirksame Maßnahmen, um die Grundsätze und Verpflichtungen der Verordnung einzuhalten

Exkurs: Accountability
Umsetzung in der DSGVO

- Der Datenverarbeiter muss sicherstellen und den Nachweis dafür erbringen können, dass die Verarbeitung gemäß der DS-GVO erfolgt:

  - Umsetzung von geeigneten technischen und organisatorischen Maßnahmen
  - Bestellung eines Datenschutzbeauftragten
  - Verzeichnis von Verarbeitungstätigkeiten
  - Datenschutzfolgeabschätzung / vorherige Konsultation der Aufsichtsbehörde
  - Meldung von Datenschutzverletzungen
  - Verpflichtung zur Zusammenarbeit mit der Aufsichtsbehörde

2. Verantwortlichkeit und Struktur

- Die Gesamtverantwortung für den Datenschutz liegt bei der Leitung des Unternehmens (AG-Vorstand, Geschäftsführung etc.). Damit trägt sie auch die Verantwortung für die Umsetzung der DS-GVO; sowohl im Hinblick auf die Organisation (Vermeidung von Organisationsverschulden) als auch die Überwachung (Vermeidung des Überwachungsversagens).

2. Verantwortlichkeit und Struktur

- Die Abteilungen führen die Anweisungen der Geschäftsführung aus und tragen damit die Prozessverantwortung (u.a. Erfüllung von Dokumentationspflichten; Gewährleistung der Betroffenenrechte; Vermeidung datenschutzrechtlicher Risiken durch Prozess-, Produkt- und Technikgestaltung). Sie sollten aber auch für die arbeitsplatzbezogene Instruktion der einzelnen Mitarbeiter sorgen.

2. Verantwortlichkeit und Struktur

- Der Datenschutzbeauftragte soll bei der Umsetzung der DS-GVO beraten (etwa Erläuterung der gesetzlichen Anforderungen oder über den Aufbau eines Datenschutzmanagements usw.). Er soll aber auch u.a. die Einhaltung der gesetzlichen Vorschriften überwachen.

3. Risikoanalyse

3. Risikoanalyse

- Ausgangspunkt einer Risikoanalyse im Bereich des Datenschutzes sind die möglichen Auswirkungen der Datenverarbeitung für die davon betroffenen Personen. Hier sind Eintrittswahrscheinlichkeit, Eingriffsintensität sowie Möglichkeiten zur Risikovermeidung oder –minimierung zu berücksichtigen. Diese Risikoanalyse wird auch bei vielen Vorschriften der DS-GVO vorausgesetzt.

3. Risikoanalyse
Übersicht nach der DS-GVO

Risikobasierter Ansatz	Anwendungsbereich	Art.	ErwGr.
Risikobeurteilung und Risikobehandlung	Datenschutzkonforme Verarbeitung	24	74-77
	Datenschutz durch Technikgestaltung	25	78
	Sicherheit der Verarbeitung	32	83
	Datenschutz-Folgeabschätzung (bei hohem Risiko)	35 und 36	84, 89-93 und 94-96
Datenschutzverletzung	Meldung an die Aufsichtsbehörde	33	85, 87, 88
	Benachrichtigung der betroffenen Personen (bei hohem Risiko)	34	86-88

3. Risikoanalyse

- Für die unternehmensinterne Risikobewertung sind aber neben mögliche Bußgeldern bei einem datenschutzrechtlichen Verstoß auch zivilrechtliche Haftungsrisiken zu berücksichtigen (Art. 82. Abs. 1 sieht neben dem Ersatz von materiellen Schäden auch den Ersatz von immateriellen Schäden vor).

3. Risikoanalyse

- Im „worst case“ besteht das Risiko, dass die Aufsichtsbehörde dem Unternehmen einzelne Datenverarbeitungen untersagt.

4. GAP-Analyse (Soll-Ist-Abgleich)

4. GAP-Analyse (Soll-Ist-Abgleich)

- Feststellung des betrieblichen Ist-Zustandes.
- Feststellung des Soll-Zustandes anhand der neuen gesetzlichen Bestimmungen.
- Bestimmung des Handlungsbedarfs.

> Aktionsplan und Umsetzung.

5. Bestandsaufnahme (Ist-Zustand)

5. Bestandsaufnahme (Ist-Zustand)

Um ein genaues Verständnis davon zu bekommen, wie in einem Unternehmen mit personenbezogenen Daten umgegangen wird, sollten die aktuellen Grundlagen der Datenverarbeitung analysiert werden (Ist-Zustand).

Praxis-Tipp

Ein bestehendes Verfahrensverzeichnis kann für die Bestandsaufnahme einen Ausgangspunkt bilden. Aber auch weitere Dokumente, wie etwa Verarbeitungsübersichten oder eine Liste der technischen und organisatorischen Maßnahmen, erleichtern die Feststellung des Status-Quo.

5. Bestandsaufnahme (Ist-Zustand)

Wichtige Elemente der Bestandsaufnahme sollten sein:

- die derzeitigen Prozesse im Unternehmen, in denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden,
- die dazugehörigen Rechtsgrundlagen (Grundprinzip: Verbot mit Erlaubnisvorbehalt),

5. Bestandsaufnahme (Ist-Zustand)

- die Datenschutzorganisation (d.h., alle Vorkehrungen und Maßnahmen, die im Unternehmen zum Schutz personenbezogener Daten getroffen werden),
- die Dienstleistungsbeziehungen (wie etwa Verträge über eine Auftragsdatenverarbeitung),
- die Dokumentation (z.B. Verfahrensverzeichnisse),

Praxis-Tipp

Künftig müssen sich Unternehmen darauf einstellen, dass sie im Streitfall nachweisen müssen, die Anforderungen der DS-GVO umgesetzt zu haben. Umso wichtiger wird es sein, Datenschutzmaßnahmen bereits jetzt umfassend zu dokumentieren.

Die Abfrage und Feststellung des Status-Quo kann bereits als Teilarbeit für den Aufbau eine Dokumentation genutzt werden.

5. Bestandsaufnahme (Ist-Zustand)

- die IT-Sicherheit (ggf. Untersuchung früherer Sicherheitslücken im System) und
- sofern vorhanden: die Betriebsvereinbarungen, denn diese können auch Regelungen zum Umgang mit den Daten der Beschäftigten enthalten.

6. Änderungen durch die DS-GVO (Soll-Zustand)

6. Änderungen durch die DS-GVO (Soll-Zustand)
Wesentliche Datenschutzvorschriften der DS-GVO

Verantwortlicher muss rechtmäßigen Datenumgang nachweisen (Rechenschaftspflicht, Art. 5 Abs. 2)

Pflichten des Verantwortlichen im Hinblick auf die zu ergreifenden technischen und organisatorischen Maßnahmen (Art. 24 Abs. 1)

Transparente Information, Kommunikation und Modalitäten (Art. 12)

6. Änderungen durch die DS-GVO (Soll-Zustand)
Einhaltung der Datenschutzgrundsätze, Art. 5

Verantwortlicher muss rechtmäßigen Datenumgang nachweisen (Rechenschaftspflicht, Art. 5 Abs. 2)

Grundsätze der Verarbeitung personenbezogener Daten (Art. 5 Abs. 1)

Rechtmäßigkeit

Transparenz, Verarbeitung nach Treu und Glauben

Zweckbindung

Richtigkeit und Aktualität

Richtigkeit und Aktualität

Integrität und Vertraulichkeit

6. Änderungen durch die DS-GVO (Soll-Zustand)
Pflichten des Verantwortlichen, Art. 24 bis 43

Pflichten des Verantwortlichen im Hinblick auf die zu ergreifenden technischen und organisatorischen Maßnahmen (Art. 24)

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, Art. 25

Auftragsverarbeiter, Art. 28

Verarbeitungs-verzeichnis, Art. 30

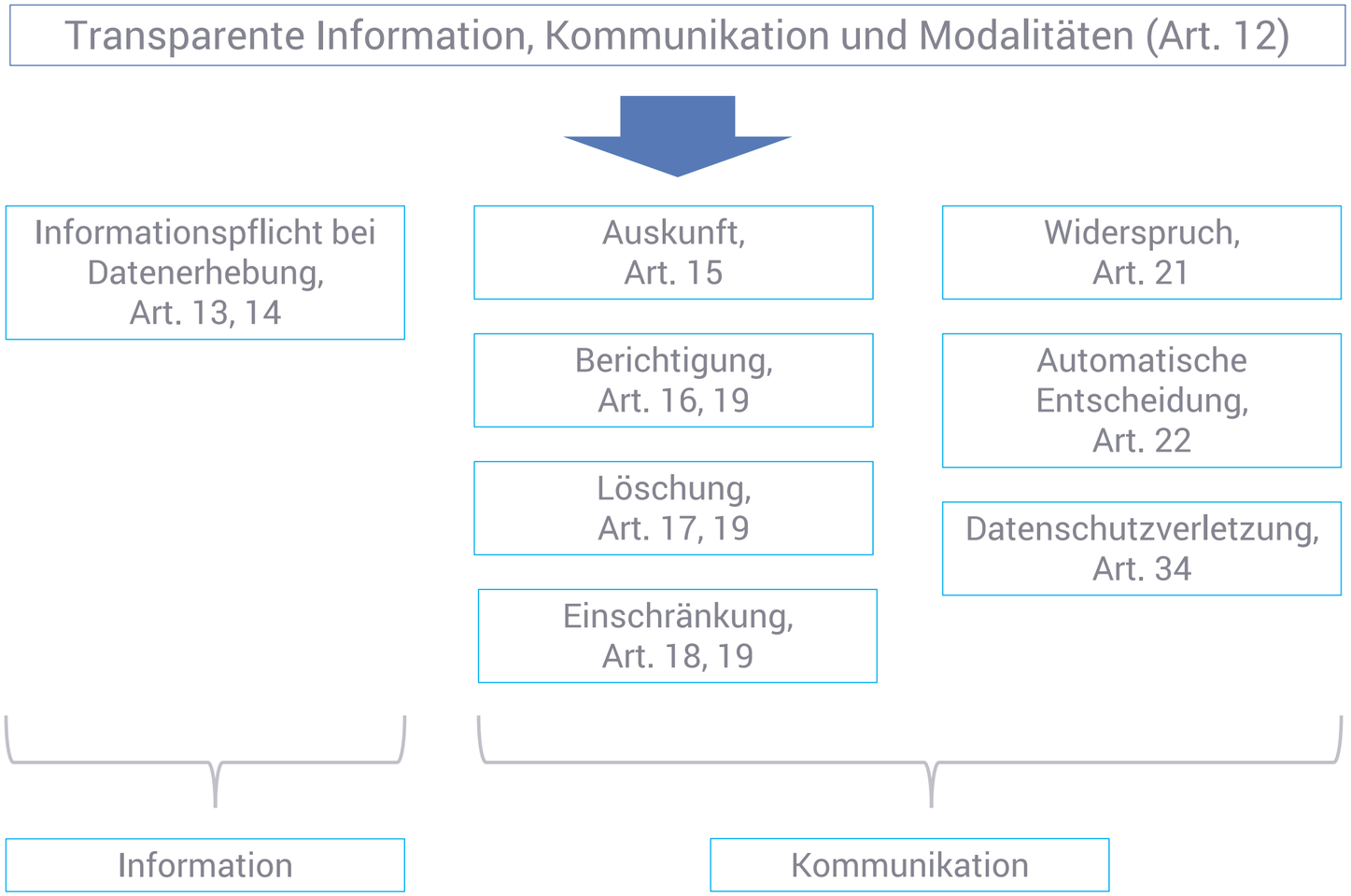
Sicherheit der Datenverarbeitung, Art. 32

Datenschutzverletzung, Art. 33, 34

Datenschutz-Folgeabschätzung, Art. 35, 36

Datenschutzbeauftragter, Art. 37 bis 39

6. Änderungen durch die DS-GVO (Soll-Zustand)
Rechte der betroffenen Person, Art. 12 bis 23



6. Änderungen durch die DS-GVO (Soll-Zustand)
Ablaufdiagramm

Verarbeitung personenbezogener Daten		
Einhaltung der Datenschutzgrundsätze, Rechenschaftspflicht (Art. 5 Abs. 1, 2)		
1	Rechtmäßigkeit der Datenverarbeitung basierend auf einer Rechtgrundlage (Art. 6)	Spezifischer Zweck
2	Transparenz bei der Datenerhebung (Art. 12)	Informationspflichten nach Art. 13 bzw. Art. 14
3	Sicherheit der Verarbeitung durch geeignete technische und organisatorische Maßnahmen (Art. 24, 32)	Nachweis
4	Datenschutzkonforme Auftragsverarbeitung (Art. 28)	Nachweis
5	Datenübermittlung in ein Drittland (Art. 44)	Sicherstellung des Schutzniveaus
6	Verzeichnis der Verarbeitungstätigkeiten (Art. 30)	Dokumentation

Datenschutzgrundsätze

Grundsatz	Fragestellung
Rechtmäßigkeit	Was ist die Rechtsgrundlage der Datenverarbeitung?
Verarbeitung nach Treu und Glauben, Transparenz	Werden die Risiken für die betroffene Person ausreichend berücksichtigt? Wird die Datenverarbeitung der betroffenen Person transparent erläutert?
Zweckbindung	Ist gewährleistet, dass die Verarbeitung nur für die zuvor festgelegten und der betroffenen Person mitgeteilten Zwecke erfolgt?
Richtigkeit und Aktualität	Sind die personenbezogenen Daten richtig und auf dem neuesten Stand?
Datenminimierung und Speicherbegrenzung	Ist die Datenverarbeitung auf das für die Zwecke notwendige Maß beschränkt (inhaltliche Beschränkung)? Werden die Daten der betroffenen Person nur solange gespeichert, wie dies für die festgelegten Zwecke erforderlich ist (zeitliche Beschränkung)?
Integrität und Vertraulichkeit	Wird in Bezug auf die Umstände der Datenverarbeitung und der Risiken für die betroffene Person eine angemessene Sicherheit der Daten gewährleistet?

6. Änderungen durch die DS-GVO (Soll-Zustand)
Ablaufdiagramm

Verarbeitung personenbezogener Daten		
Einhaltung der Datenschutzgrundsätze, Rechenschaftspflicht (Art. 5 Abs. 1, 2)		
1	Rechtmäßigkeit der Datenverarbeitung basierend auf einer Rechtgrundlage (Art. 6)	Spezifischer Zweck
2	Transparenz bei der Datenerhebung (Art. 12)	Informationspflichten nach Art. 13 bzw. Art. 14
3	Sicherheit der Verarbeitung durch geeignete technische und organisatorische Maßnahmen (Art. 24, 32)	Nachweis
4	Datenschutzkonforme Auftragsverarbeitung (Art. 28)	Nachweis
5	Datenübermittlung in ein Drittland (Art. 44)	Sicherstellung des Schutzniveaus
6	Verzeichnis der Verarbeitungstätigkeiten (Art. 30)	Dokumentation

6. Änderungen durch die DS-GVO (Soll-Zustand)
Rechtmäßigkeit der Verarbeitung

Art. 7
Einwilligung

Nationales
Recht

Art. 8
Einwilligung
eines Kindes

**Art. 6
Rechtmäßigkeit
der Verarbeitung**

Art. 11
Verarbeitung ohne
Bestimmung der
Betroffenen

Art. 9
besondere
Datenkategorien

Art. 10
Strafurteile und
Straftaten

Bsp.: Verarbeitung personenbezogener Daten für Werbung

- Keine Detailregelung für Werbung in der DS-GVO
- Keine Öffnungsklausel für nationale Regelungen
- Grundlage für die Beurteilung der Zulässigkeit der Verarbeitung: Interessenabwägung nach Art. 6 Abs. 1 lit. f oder Einwilligung nach Art. 6 Abs. 1 lit. a.

Bsp.: Verarbeitung personenbezogener Daten für Werbung

- Interessenabwägung nach Art. 6 Abs. 1 lit. f: Auf Grundlage der konkreten Umstände ist zwischen dem Interesse an einer Datenverarbeitung durch den Verantwortlichen und den Interessen und Grundrechten der betroffenen Person abzuwägen (Einzelheiten ErwGr. 47).
  - Zweck der jeweiligen Werbung
  - Kundenbeziehung
  - Intensität des Eingriffs durch die Werbemaßnahme

Bsp.: Verarbeitung personenbezogener Daten für Werbung

- Zu beachten sind weiterhin:
  - Informationspflichten nach Art. 13 oder 14
  - Werbewiderspruch nach Art. 21 Abs. 2 und 3
  - Allgemeine Grundsätze nach Art. 5 Abs. 1 (faire Verfahrensweise, dem Verarbeitungszweck angemessen, in einer für die betroffene Person nachvollziehbaren Weise)
  - Sonderregelungen, z.B. § 7 UWG für Telefon- und Faxwerbung sowie SMS- und E-Mail-Werbung

Bsp.: Verarbeitung personenbezogener Daten für Werbung

- Voraussetzungen für eine Einwilligung (Art. 7):
  - Freiwilligkeit (> Möglichkeit eine Einwilligung zu verweigern oder zurückzuziehen ohne Nachteile zu erleiden; insbesondere Kopplungsverbot).
  - In informierter Weise (z.B. in verständlicher und leicht zugänglicher Form, in einer klaren und einfachen Sprache).

Bsp.: Verarbeitung personenbezogener Daten für Werbung

- Voraussetzungen für eine Einwilligung (Art. 7):
  - Die Schriftform ist nicht mehr erforderlich; ausreichend ist vielmehr eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung (aktives Verhalten). Die bestätigende Handlung kann z.B. auch elektronisch, durch „Anklicken“ eines Feldes im Internet oder auch mündlich erfolgen.

Bsp.: Verarbeitung personenbezogener Daten für Werbung

- Voraussetzungen für eine Einwilligung (Art. 7):
  - ➢ Nachweis- und Beweispflicht des Verantwortlichen.
  - ➢ Widerrufsrecht der betroffenen Person (mit Wirkung für die Zukunft).
- Weitere Voraussetzungen, wie etwa die Informationspflichten nach Art. 13 DS-GVO oder Einwilligung eines Kindes nach Art. 8 DS-GVO.

Bsp.: Verarbeitung personenbezogener Daten für Werbung

- „Alt“-Einwilligungen für Werbung (nach dem BDSG) können fortgelten, sofern sie der Art nach den Bedingungen der DS-GVO entsprechen (ErwGr. 171):
  - Informationspflichten nach Art. 13 müssen nicht erfüllt sein, wenn und soweit sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind (unabdingbar ist etwa das Widerrufsrecht).
  - Freiwilligkeit muss gegeben sein (Kopplungsverbot).
  - Einwilligungsfähigkeit liegt vor (Art. 8).

Praxis-Tipp

Das Kopplungsverbot (ErwGr. 43) erschwert gerade im Falle der Einwilligung Datenverarbeitungen, die mit der eigentlichen Leistung nicht in Zusammenhang stehen.

Ist eine erteilte Einwilligung unwirksam, so widerspricht der Grundsatz der Fairness und Transparenz ein Wechseln auf eine andere Rechtsgrundlage.

Unternehmen sollten daher ihre Einwilligungen daraufhin prüfen, welche Datenverarbeitungen künftig auf Art. 6 Abs. 1 lit. f gestützt werden können.

6. Änderungen durch die DS-GVO (Soll-Zustand)
Ablaufdiagramm

Verarbeitung personenbezogener Daten		
Einhaltung der Datenschutzgrundsätze, Rechenschaftspflicht (Art. 5 Abs. 1, 2)		
1	Rechtmäßigkeit der Datenverarbeitung basierend auf einer Rechtgrundlage (Art. 6)	Spezifischer Zweck
2	Transparenz bei der Datenerhebung (Art. 12)	Informationspflichten nach Art. 13 bzw. Art. 14
3	Sicherheit der Verarbeitung durch geeignete technische und organisatorische Maßnahmen (Art. 24, 32)	Nachweis
4	Datenschutzkonforme Auftragsverarbeitung (Art. 28)	Nachweis
5	Datenübermittlung in ein Drittland (Art. 44)	Sicherstellung des Schutzniveaus
6	Verzeichnis der Verarbeitungstätigkeiten (Art. 30)	Dokumentation

Informationspflichten - Form

- Regelungen der DS-GVO für die Informationspflichten des Verantwortlichen nach Art. 13 und 14
- Art. 12: Grundregelung der Betroffenenrechte (Information in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache).
- Die Informationen sind schriftlich oder in anderer Form (ggf. elektronisch) zur Verfügung zu stellen.

Informationspflichten - Zeitpunkt

- Art. 13: **Direkterhebung** = Erhebung bei der betroffenen Person (Information des Betroffenen zum Zeitpunkt der Erhebung).
- Art. 14: **Dritterhebung** (Information des Betroffenen nachträglich innerhalb einer angemessenen Frist von maximal einem Monat oder spätestens bei der ersten Kontaktaufnahme mit der betroffenen Person oder spätestens bei ersten Übermittlung an Dritte).

Informationspflichten - Nachweis

- Der Verantwortliche hat im Hinblick auf das Transparenzgebot stets den Nachweis ordnungsgemäßer Erledigung der Informationspflichten zu erbringen (Art. 5 Abs. 1 lit. a und Abs. 2).

Informationspflichten - Inhalt

- Die in Art. 13 und 14 geforderten Informationen und Rechtsbelehrungen sind in wesentlichen Punkten identisch.
- Information über Name und Kontaktdaten der verantwortlichen Stelle bzw. des Vertreters, ggf. Kontaktdaten des Datenschutzbeauftragten, Verarbeitungszwecke und deren Rechtsgrundlage etc..

Informationspflichten - Inhalt

- Rechtsbelehrungen über Auskunftsrecht, Berichtigung, Löschung, Sperrung, Recht zum Widerruf der Einwilligung etc..
- Art. 21 Absatz 4: der Hinweis auf das Widerspruchsrecht muss in einer verständlichen und von anderen Informationen getrennten Form erfolgen.

6. Änderungen durch die DS-GVO (Soll-Zustand)
Ablaufdiagramm

Verarbeitung personenbezogener Daten		
Einhaltung der Datenschutzgrundsätze, Rechenschaftspflicht (Art. 5 Abs. 1, 2)		
1	Rechtmäßigkeit der Datenverarbeitung basierend auf einer Rechtgrundlage (Art. 6)	Spezifischer Zweck
2	Transparenz bei der Datenerhebung (Art. 12)	Informationspflichten nach Art. 13 bzw. Art. 14
3	Sicherheit der Verarbeitung durch geeignete technische und organisatorische Maßnahmen (Art. 24, 32)	Nachweis
4	Datenschutzkonforme Auftragsverarbeitung (Art. 28)	Nachweis
5	Datenübermittlung in ein Drittland (Art. 44)	Sicherstellung des Schutzniveaus
6	Verzeichnis der Verarbeitungstätigkeiten (Art. 30)	Dokumentation

Technisch / organisatorischer Datenschutz
Grundsatz

Art. 24 Abs. 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. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Technisch / organisatorischer Datenschutz
Sicherheit der Verarbeitung

Pflicht zur Implementierung technischer und organisatorischer Maßnahmen

Zielvorgabe

- Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Risiken für Rechte und Freiheiten der Betroffenen.

Vernichtung	unbeabsichtigt
Verlust	
Veränderung	unrechtmäßig

Offenlegung von	unbefugt
Zugang zu	

Mögliche Risiko-Quellen
Cyberkriminelle
Interne Administratoren
Wettbewerber
„Normale“ Mitarbeiter
Geschäfts-/Abteilungsleitung
Dienstleister
Staatliche Organisationen

Technisch / organisatorischer Datenschutz
Sicherheit der Verarbeitung

Geeignet; Beispielmaßnahmen:

- Pseudonymisierung & Verschlüsselung
- Dauerhafte Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
- Wiederherstellung von Verfügbarkeit bei Zwischenfällen
- Verfahren zur regelmäßigen Überprüfung der Wirksamkeit

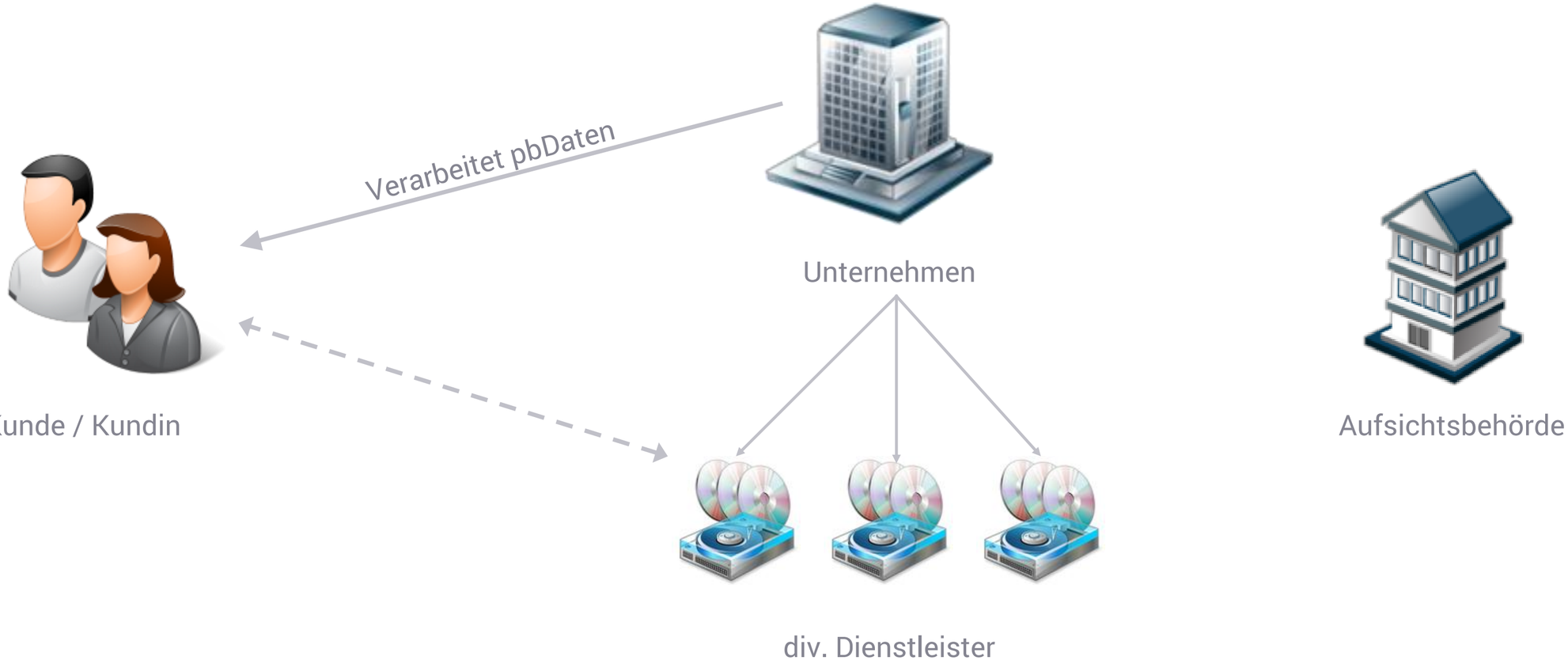
Maßstab

- Stand der Technik
- Kosten für die Implementierung (nicht Folgekosten)
- Art, Umfang, Zweck und Umstände der Verarbeitung
- Eintrittswahrscheinlichkeit und Schwere der Risiken

6. Änderungen durch die DS-GVO (Soll-Zustand)
Ablaufdiagramm

Verarbeitung personenbezogener Daten		
Einhaltung der Datenschutzgrundsätze, Rechenschaftspflicht (Art. 5 Abs. 1, 2)		
1	Rechtmäßigkeit der Datenverarbeitung basierend auf einer Rechtgrundlage (Art. 6)	Spezifischer Zweck
2	Transparenz bei der Datenerhebung (Art. 12)	Informationspflichten nach Art. 13 bzw. Art. 14
3	Sicherheit der Verarbeitung durch geeignete technische und organisatorische Maßnahmen (Art. 24, 32)	Nachweis
4	Datenschutzkonforme Auftragsverarbeitung (Art. 28)	Nachweis
5	Datenübermittlung in ein Drittland (Art. 44)	Sicherstellung des Schutzniveaus
6	Verzeichnis der Verarbeitungstätigkeiten (Art. 30)	Dokumentation

Beteiligten



Verantwortlichkeiten
Definitionen

Für die Verarbeitung Verantwortlicher

die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet

Auftragsverarbeiter

eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet

Auftragsverarbeiter
Voraussetzungen

Voraussetzungen für die Einschaltung von Auftragsverarbeitern

- Form des Auftrags: schriftlich oder elektronisch
- Hinreichende Garantien
- Grundlage der Auftragsverarbeitung: Vertrag
- Vertragliche Kerninhalte

!! Auftragsverarbeiter müssen transparent gemacht werden !!

Auftragsverarbeiter
Mindestinhalte des Vertrages

- Gegenstand und Dauer der Beauftragung
- Art und Zweck der Verarbeitung
- Art der Daten, Kategorien betroffener Personen
- Rechte und Pflichten des Verantwortlichen
- Zu dokumentierende Weisungen / Remonstrationspflicht bei rechtswidrigen Weisungen
- Verschwiegenheitspflicht
- Technische / organisatorische Maßnahmen
- Regelungen zu weiteren Auftragsverarbeitern
- Unterstützungspflichten
- Lösch- und Rückgabepflichten
- Nachweis der Pflichteinhaltung

6. Änderungen durch die DS-GVO (Soll-Zustand)
Ablaufdiagramm

Verarbeitung personenbezogener Daten		
Einhaltung der Datenschutzgrundsätze, Rechenschaftspflicht (Art. 5 Abs. 1, 2)		
1	Rechtmäßigkeit der Datenverarbeitung basierend auf einer Rechtgrundlage (Art. 6)	Spezifischer Zweck
2	Transparenz bei der Datenerhebung (Art. 12)	Informationspflichten nach Art. 13 bzw. Art. 14
3	Sicherheit der Verarbeitung durch geeignete technische und organisatorische Maßnahmen (Art. 24, 32)	Nachweis
4	Datenschutzkonforme Auftragsverarbeitung (Art. 28)	Nachweis
5	Datenübermittlung in ein Drittland (Art. 44)	Sicherstellung des Schutzniveaus
6	Verzeichnis der Verarbeitungstätigkeiten (Art. 30)	Dokumentation

Datenübermittlung in ein Drittland

- Für jede Übermittlung von personenbezogenen Daten in Drittland (= Land außerhalb der EU oder des EWR) ist eine Datenübermittlung nur zulässig, wenn
  - ✓für das Empfängerland ein Angemessensheitsbeschluss der EU vorliegt (Art. 45)
  - ✓die Unternehmen geeignete Garantien bieten (Art. 46, 47)
  - ✓eine Ausnahme gegeben ist (Art. 49).

6. Änderungen durch die DS-GVO (Soll-Zustand)
Ablaufdiagramm

Verarbeitung personenbezogener Daten		
Einhaltung der Datenschutzgrundsätze, Rechenschaftspflicht (Art. 5 Abs. 1, 2)		
1	Rechtmäßigkeit der Datenverarbeitung basierend auf einer Rechtgrundlage (Art. 6)	Spezifischer Zweck
2	Transparenz bei der Datenerhebung (Art. 12)	Informationspflichten nach Art. 13 bzw. Art. 14
3	Sicherheit der Verarbeitung durch geeignete technische und organisatorische Maßnahmen (Art. 24, 32)	Nachweis
4	Datenschutzkonforme Auftragsverarbeitung (Art. 28)	Nachweis
5	Datenübermittlung in ein Drittland (Art. 44)	Sicherstellung des Schutzniveaus
6	Verzeichnis der Verarbeitungstätigkeiten (Art. 30)	Dokumentation

Verzeichnis der Verarbeitungstätigkeiten
Gegenstand

- schriftliche Dokumentation der wesentlichen Informationen einer (aller) Datenverarbeitung/en
- Dient der Transparenz über die Verarbeitung personenbezogener Daten
- Grundlage & Nachweis der Einhaltung der DSGVO
- Grundlage für Aufgabenerfüllung von dem betrieblichen Datenschutzbeauftragten und Aufsichtsbehörde => (nur) diesen zur Verfügung zu stellen
- Neu: Gilt auch für Auftragsverarbeiter

Verzeichnis der Verarbeitungstätigkeiten
Inhalte beim Verantwortlichen

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie geeigneter Garantien
- Fristen für die Löschung der verschiedenen Datenkategorien
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Verzeichnis der Verarbeitungstätigkeiten
Inhalte beim Auftragsverarbeiter

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden
- Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie geeigneter Garantien
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Verzeichnis der Verarbeitungstätigkeiten
Ausnahmen

- Ausnahme für Unternehmen mit weniger als 250 Mitarbeitern, außer
  - ➢ hohes Risiko für die Rechte und Freiheiten der betroffenen Personen
  - ➢ besondere Datenkategorien (Art. 9) oder personenbezogener Daten über strafrechtliche Verurteilungen / Straftaten (Art. 10)
  - ➢ Datenverarbeitung erfolgt nicht nur gelegentlich

6. Änderungen durch die DS-GVO (Soll-Zustand)
Betroffenenrechte

- Informationsrechte, Art. 13 und 14
- Recht auf Auskunft, Art. 15
- Recht auf Berichtigung, Art. 16
- Recht aus Löschung, Art. 17
- Recht auf Einschränkung der Verarbeitung, Art. 18
- Recht auf Datenübertragbarkeit, Art. 20
- Recht auf Widerspruch, Art. 21
- Recht auf eine nichtautomatisierten Entscheidung, Art. 22 Abs. 3
- Recht auf Widerruf einer Einwilligung, Art. 7 Abs. 3

Auskunftsrecht - Grundsatz

- Nach Art. 15 Auskunftsrecht der betroffenen Person gegenüber dem Verantwortlichen
- Formloser Antrag ohne Begründung
- Bei Bedarf weitere Rechte: Berichtigung, Löschung oder Einschränkung der Verarbeitung („Sperrung“)
- Einzelheiten in ErwGr. 63
- Eingrenzung in § 34 BDSG-neu

Auskunftsrecht - Umfang

- Abgestuftes Auskunftsrecht nach Art. 15 Abs. 1
- Bestätigung darüber, ob überhaupt von dem Verantwortlichen personenbezogene Daten der betroffenen Person verarbeitet werden, d.h. auch eine Negativauskunft ist möglich, wenn
  - ➢keine Daten zu dieser Person verarbeitet werden oder
  - ➢die personenbezogenen Daten unumkehrbar anonymisiert wurden.

Auskunftsrecht - Umfang

- Wenn personenbezogene Daten verarbeitet werden, kann die betroffene Person Auskunft darüber verlangen, welche Daten dies sind (z.B. Name, Anschrift, Geburtsdatum, Beruf etc.).
- Als weitere Informationen sind beispielsweise mitzuteilen: Verarbeitungszwecke, geplante Speicherdauer, Rechte auf Berichtigung oder Löschung oder „Sperrung“, Widerspruchsrecht, Beschwerderecht, Herkunft der Daten bei Dritterhebung usw.

Auskunftsrecht - Form

- Grundsatz des Art. 12 Abs. 1 S. 1 bis 3: schriftlich, elektronisch (ggf. Identitätsprüfung, Art. 12 Abs. 6) oder mündlich (auf Wunsch der betroffenen Person) in verständlicher Form.
- Der Verantwortliche stellt dabei eine Kopie der Daten zur Verfügung (Art. 15 Abs. 3 S. 1).
- Die datenschutzfreundlichste Gestaltung ist der Fernzugriff der betroffenen Person auf ihre eigene Daten (ErwGr. 63 S. 4).

Auskunftsrecht - Frist

- Die Auskunftserteilung muss unverzüglich erfolgen (spätestens innerhalb eines Monats).
- Der Verantwortliche muss hierzu geeignete organisatorische Maßnahmen ergreifen.
- Ausnahme in begründeten Fällen, worüber aber die betroffene Person zu informieren ist.

Auskunftsrecht - Kosten

- Die Auskunftserteilung muss grundsätzlich unentgeltlich erfolgen (Art. 12 Abs. 5 S. 1). Dies gilt für die erste Kopie.
- Ausnahme: die betroffene Person fordert mehrere Kopien an (> angemessenes Entgelt).
- Weitere Ausnahmen bei offenkundig unbegründeten oder exzessiven (häufige Wiederholung) Anträgen (> angemessenes Entgelt oder Ablehnung).

Auskunftsrecht – Rechte Dritter

- Die Auskunftserteilung an die betroffene Person darf nach Art. 15 Abs. 4 sowie ErwGr. 63 Satz 5 die Rechte des Verantwortlichen oder anderer Personen nicht beeinträchtigen, was bei Geschäftsgeheimnissen oder bei Daten mit Bezug auch auf andere Personen der Fall sein kann. Dies darf im Ergebnis aber nicht dazu führen, dass jegliche Auskunft verweigert wird (ErwGr. 63 Satz 6).

6. Änderungen durch die DS-GVO (Soll-Zustand)
Datenpannen

Risikobasierter Ansatz	Anwendungsbereich	Art.	ErwGr.
Risikobeurteilung und Risikobehandlung	Datenschutzkonforme Verarbeitung	24	74-77
	Datenschutz durch Technikgestaltung	25	78
	Sicherheit der Verarbeitung	32	83
	Datenschutz-Folgeabschätzung (bei hohem Risiko)	35 und 36	84, 89-93 und 94-96
Datenschutzverletzung	Meldung an die Aufsichtsbehörde	33	85, 87, 88
	Benachrichtigung der betroffenen Personen (bei hohem Risiko)	34	86-88

6. Änderungen durch die DS-GVO (Soll-Zustand)
Datenpanne: Meldepflicht des Verantwortlichen

- Verletzung des Schutzes personenbezogener Daten
- Unverzügliche Meldung, spätestens innerhalb von 72 Stunden

Vernichtung	unbeabsichtigt
Verlust	
Veränderung	unrechtmäßig

Offenlegung von	unbefugt
Zugang zu	

- Inhalt:
  - Beschreibung von Art und Umfang der Verletzung
  - Kontaktdaten des betrieblichen Datenschutzbeauftragten
  - Beschreibung der wahrscheinlichen Folgen der Verletzung
  - die vom Verantwortlichen ergriffenen / vorgeschlagenen Maßnahmen

6. Änderungen durch die DS-GVO (Soll-Zustand)
Datenpanne: Benachrichtigungspflicht der Betroffenen

- Wenn Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheit
- Inhalt wie Meldepflicht, wobei keine Angaben über Umfang
- Ausnahmen
  - Kryptographische Sicherungen
  - Implementierung von Schutzmaßnahmen zur Eindämmung
  - Unverhältnismäßiger Aufwand, stattdessen öffentliche Bekanntmachung

7. Planung der Unternehmensprozesse im Datenschutz

7. Planung der Unternehmensprozesse im Datenschutz

- Beschwerdemanagement
- Vertragsmanagement
- Einwilligungsmanagement
- Dokumentations- und Meldemanagement
- Risikomanagement (Datenpannen)

Hilfestellungen

Zu vielen Themen haben die Aufsichtsbehörden bereits sogenannte Kurzpapiere im Zusammenhang mit der DS-GVO auf ihren Internetseiten veröffentlicht. Außerdem wurden Hinweise Muster zum Verzeichnis von Verarbeitungstätigkeiten erstellt. Diese finden Sie alles unter folgender Adresse:

https://datenschutz.saarland.de/

Vielen Dank für Ihre Aufmerksamkeit

UNABHÄNGIGES DATENSCHUTZZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz
und Informationsfreiheit

Fritz-Dobisch-Straße 12 • 66111 Saarbrücken
Telefon 0681 94781-0
Fax 0681 94781-29
E-Mail: poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de
www.informationsfreiheit.saarland.de