

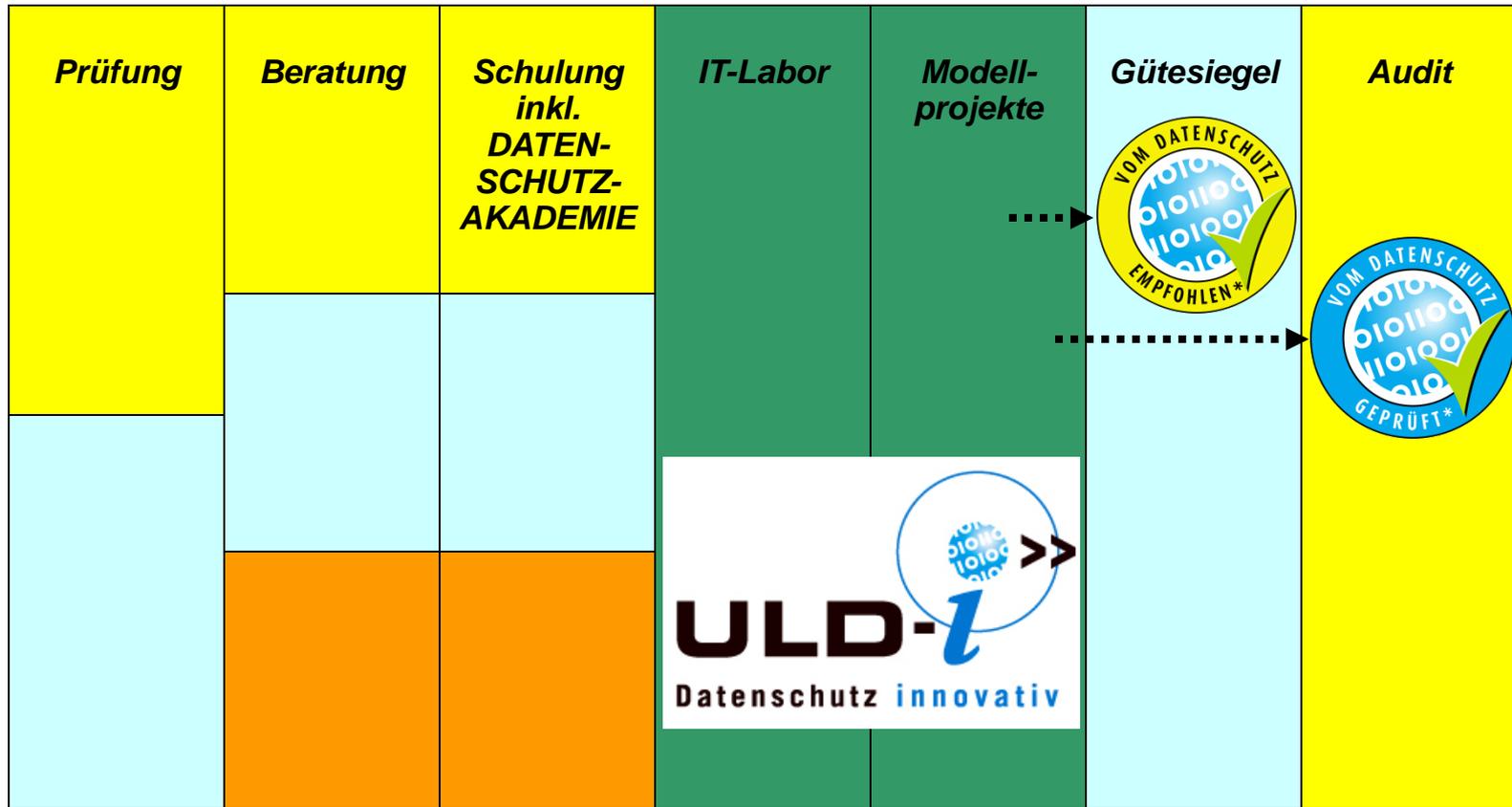
Die neue Datenschutz- Grundverordnung – was müssen Unternehmen künftig beachten?

Referent:
Dr. Sven Polenz



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Die 7 Säulen des ULD



Primäre Adressaten:



Öffentl. Verwaltungen



Unternehmen



Bürger, Kunden, Nutzer



Wirtschaft,
Wissenschaft,
Forschung,
Verwaltung

Auswahl

I. Allgemeine Grundsätze, Art. 5 DSGVO

II. Spezielle Punkte

1. Marktortprinzip, Art. 3 Abs. 2 DSGVO
2. Anforderungen für eine Einwilligung, Art. 7 DSGVO, und Informationspflichten, Art. 13 DSGVO
3. Einwilligung eines Kindes, Art. 8 DSGVO
4. Fristen bei der Gewährleistung von Rechten betroffener Personen sowie Eskalationsfälle, Art. 12 Abs. 3-5 DSGVO
5. Erweitertes Auskunftsrecht, Art. 15 DSGVO
6. Mitteilungspflicht, Art. 19 DSGVO
7. Verarbeitungsverzeichnisse, Art. 30 DSGVO
8. Gemeinsame Datenverarbeitung, Art. 26 DSGVO
9. Zusätzliche Anforderungen bei Auftragsverarbeitung, Art. 28 DSGVO
10. Meldepflichten, Art. 33 und 34 DSGVO
11. Bestellung von Datenschutzbeauftragten, Art. 37 DSGVO

III. Zusammenfassung

I. Allgemeine Grundsätze, Art. 5 DSGVO

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, in nachvollziehbarer Weise (Transparenz)
- für festgelegte, eindeutige & legitime Zwecke (Zweckbindung)
- dem Zweck angemessen und auf das notwendige Maß beschränkte Verarbeitung (Datenminimierung)
- Richtigkeit der Daten
- Speicherbegrenzung bzw. Erforderlichkeit
- Integrität und Vertraulichkeit
- Rechenschaftspflicht (→ **Dokumentationspflicht**)

II. Spezielle Punkte

1. Marktortprinzip <-> Territorialprinzip

- Aufsichtsbehörden sind zur Aufgabenerfüllung/Ausübung der Befugnisse im **eigenen Hoheitsgebiet** zuständig (Art. 55 Abs. 1 DSGVO).
- Bei grenzüberschreitenden Verarbeitungen ist die Aufsichtsbehörde der **Hauptniederlassung** oder der **einzigsten Niederlassung** des **Verantwortlichen** oder **Auftragsverarbeiters** zuständig (Art. 56 Abs. 1 DSGVO).
- Es gelten die Grundsätze zur Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden (Art. 60 DSGVO).

II. Spezielle Punkte

1. Marktortprinzip <-> Territorialprinzip

- Dies wird angewendet auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen **nicht in der Union niedergelassenen** Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht
 - a) betroffenen Personen **in der Union Waren oder Dienstleistungen anzubieten**, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist,
 - b) das **Verhalten betroffener Personen zu beobachten**, soweit ihr Verhalten in der Union erfolgt.

II. Spezielle Punkte

2. Anforderungen für eine Einwilligung

neu:

→ „**opt-in**“, nicht „opt-out“ (EG 32 DSGVO)

→ Belehrung über **Widerrufsrecht** vor Abgabe der Erklärung, Art. 7 Abs. 3 Satz 3 DSGVO

→ besondere Anforderungen an die **Freiwilligkeit der Erklärung** (Ist die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung personenbezogener Daten **abhängig**, die für die Erfüllung des Vertrags nicht erforderlich sind?), Art. 7 Abs. 4 DSGVO

→ zusätzlich **Erfüllung von Informationspflichten** nach Art. 13 DSGVO

II. Spezielle Punkte

(2. Anforderungen an eine Einwilligung – Auszug aus Art. 6 DSGVO)

Artikel 6

Rechtmäßigkeit der Verarbeitung

- (1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
- a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
 - b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

II. Spezielle Punkte

(2. Anforderungen an eine Einwilligung – Art. 7 DSGVO)

Artikel 7

Bedingungen für die Einwilligung

- (1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.
- (2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.
- (3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.
- (4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

II. Spezielle Punkte

2. Anforderungen für eine Einwilligung

- a) Anton kauft einen Rasenmäher auf Rechnung. Der Verkäufer erhebt die Rechnungsadresse.

- b) Abwandlung 1: Der Rasenmäher wird nur dann geliefert, wenn Anton drei weitere technische Geräte zur Pflege seines Gartens benennt, an denen er Interesse hätte.

- c) Abwandlung 2: Der Rasenmäher wird geliefert. Anton wird vom Verkäufer gebeten, drei weitere technische Geräte zur Pflege seines Gartens zu benennen, an denen er Interesse hätte.

- d) Abwandlung 3: Der Verkäufer bietet Anton einen Rabatt auf den Kaufpreis, wenn er drei weitere Geräte zur Gartenpflege benennt, an denen Interesse besteht.

II. Spezielle Punkte

Artikel 13

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

- a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

2016

DE

Amtsblatt der Europäischen Union

L 119/41

- d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
- f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

II. Spezielle Punkte

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

- a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
- f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

II. Spezielle Punkte

3. Einwilligung eines Kindes

- Die Datenverarbeitung ist rechtmäßig, wenn das Kind das **sechzehnte Lebensjahr vollendet** hat.
- Bei Nichtvollendung des sechzehnten Lebensjahres kommt es auf die Einwilligung des **Trägers der elterlichen Verantwortung** für das Kind an oder auf dessen Zustimmung.
- Die zivilrechtlichen Bestimmungen zum **Zustandekommen von Verträgen** bleiben unberührt.

II. Spezielle Punkte

4. Fristen bei der Gewährleistung von Rechten betroffener Personen sowie Eskalationsfälle, Art. 12 Abs. 3-5 DSGVO

- Die Ergreifung von Maßnahmen nach den Art. 15-22 muss durch den Verantwortlichen unverzüglich, längstens jedoch innerhalb eines Monats nach Eingang eines Antrages auf Auskunft durch die betroffene Person erfolgen (Art. 15 Abs. 3 DSGVO).
- Eine Fristverlängerung um bis zu weitere 2 Monate kann zulässig sein (→ Benachrichtigungs- und Begründungspflicht beachten).
- Sollte der Verantwortliche nicht tätig werden, hat er die betroffene Person ohne Verzögerung über die Gründe hierfür und seine rechtlichen Möglichkeiten zu informieren.
- Bei offenkundig unbegründetem oder exzessivem Charakter des Antrages kann der Verantwortliche ein Entgelt verlangen oder sich weigern, aufgrund des Antrags tätig zu werden (→ Nachweispflichten beachten).

II. Spezielle Punkte

5. Erweitertes Auskunftsrecht, Art. 15 DSGVO

- Art. 15 DSGVO enthält das Recht der betroffenen Person, von dem Verantwortlichen einen ausführlichen Katalog an Informationen zu erhalten.
- Die betroffene Person hat das Recht auf Erhalt einer kostenfreien Kopie über die personenbezogenen Daten, die verarbeitet werden.
- Wird der Antrag auf Auskunft elektronisch gestellt, so sind die Informationen grds. auch elektronisch zur Verfügung zu stellen.
- Es sind die allgemeinen Grundsätze nach Art. 12 DSGVO zu beachten, insbesondere Vorgaben zu Fristen, Kosten & Identitätsnachweise.

II. Spezielle Punkte

6. Mitteilungspflicht, Art. 19 DSGVO

- Die verantwortliche Stelle ist verpflichtet, allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung, Löschung oder Nutzungseinschränkung mitzuteilen. Dementsprechend ist zu dokumentieren, welche Daten an welche Empfänger gegeben wurden.
- Eine Ausnahme besteht, wenn die Mitteilung unmöglich oder nur mit unverhältnismäßigem Aufwand möglich ist (→ Dokumentationspflicht).
- Auf Verlangen hat der Verantwortliche die betroffene Person über die Empfänger zu unterrichten.

II. Spezielle Punkte

7. Verarbeitungsverzeichnisse, Art. 30 DSGVO

- Der Verantwortliche hat die Pflicht, ein Verzeichnis zu führen.
- Art. 30 enthält einen ausführlichen Katalog über die im Verzeichnis erforderlichen Angaben.
- **Auftragsverarbeiter** müssen künftig ein separates Verzeichnis über die von ihnen erbrachten, weisungsgebundenen Tätigkeiten führen.
- Es ist nicht mehr öffentlich zur Verfügung zu stellen.
- Es bestehen Ausnahmen für Betriebe bis 250 Mitarbeiter, sofern keine kritische Datenverarbeitung erfolgt, keine Daten besonderer Kategorien verarbeitet werden, nicht ein Risiko für Rechte und Freiheiten betroffener Personen besteht oder die Verarbeitung nicht nur gelegentlich erfolgt.

II. Spezielle Punkte

8. Gemeinsame Datenverarbeitung (Art. 26 DSGVO)

Artikel 26

Gemeinsam für die Verarbeitung Verantwortliche

(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

II. Spezielle Punkte

8. Gemeinsame Datenverarbeitung (Art. 26 DSGVO)

- **Beispiel:** Werbung auf Basis von Behavioural Targeting (Art. 29-Datenschutzgruppe, WP 169, S. 28): Der Anbieter von Online-Inhalten und ein Betreiber eines Werbenetzwerks können hinsichtlich der Datenverarbeitung zwecks Werbung auf Basis von Behavioural Targeting (Anbieter von Online-Inhalten leitet die Nutzer auf die Website eines Werbenetzwerk-Betreibers um) gemeinsame Verantwortliche sein.
- Art. 26 DSGVO führt **nicht zur Privilegierung** beteiligter Unternehmen. Bei gemeinsamer Verantwortlichkeit bedürfen die Datenübermittlungen unter den gemeinsam Verantwortlichen einer Rechtsgrundlage i.S.v. Art. 6 ff. DSGVO.

II. Spezielle Punkte

9. Anforderungen bei Auftragsverarbeitung

- Der Verantwortliche hat die Verpflichtung, nur mit solchen Auftragsverarbeitern zusammenzuarbeiten, welche **hinreichende Garantien** für geeignete technisch-organisatorische Maßnahmen bieten.
- **Unterbeauftragungen** müssen vom Verantwortlichen schriftlich autorisiert sein.
- Bei allgemeinen schriftlichen Genehmigungen stehen dem Verantwortlichen **Einspruchsrechte** gegen den Auftragsverarbeiter zu.
- Für den Vertrag über die Auftragsverarbeitung gilt die **Schriftform**.
- Dem Unterauftragnehmer müssen **die gleichen Datenschutzverpflichtungen** auferlegt werden wie dem Hauptauftragnehmer.
- Bestimmt der Auftragsverarbeiter verordnungswidrig Zwecke und Mittel der Verarbeitung, wird er **wie ein Verantwortlicher** behandelt (Art. 28 Abs. 10 DSGVO).

II. Spezielle Punkte

9. Anforderungen bei Auftragsverarbeitung

Verpflichtende Vertragsinhalte (Auswahl):

- Datenübermittlungen (auch in Drittstaaten) bedürfen einer **dokumentierten Weisung** des Verantwortlichen.
- Befugte Personen des Auftragsverarbeiters müssen einer vertraglichen oder gesetzlichen **Verschwiegenheitspflicht** unterliegen.
- Es besteht eine **Pflicht zur Unterstützung des Verantwortlichen** bezüglich der Meldepflichten gegenüber der Aufsichtsbehörde bei Datenschutzverstößen (Art. 33 DSGVO), bei der Benachrichtigung betroffener Personen bei Datenschutzverletzungen (Art. 34 DSGVO), bei der Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und bei Konsultationsverfahren nach Art. 36 DSGVO.

II. Spezielle Punkte (10. Meldepflichten)

Derzeit: Meldepflichten nach § 42a BDSG

- Begrenzt auf bestimmte Datenkategorien (§ 42a Satz 1 BDSG)
- Unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt
- Es drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen
- Unverzügliche Meldung an Aufsichtsbehörde/betroffene Personen

Künftig: Art. 33 und 34 DSGVO

- Keine Begrenzung auf bestimmte Datenkategorien („Verletzung des Schutzes personenbezogener Daten“)
- Meldepflicht an Aufsichtsbehörde entfällt, wenn Verletzung „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“
- Meldung an Aufsichtsbehörde binnen 72 Stunden
- Benachrichtigung der betroffenen Personen kann in bestimmten Fällen entfallen

II. Spezielle Punkte

11. Bestellung von Datenschutzbeauftragten

a) **Bestellverpflichtung** für

- öffentliche Stellen,
- nichtöffentliche Stellen (10-Personen-Grenze)
- Verantwortliche wie Auftragsverarbeiter
- bei bestimmten Kerntätigkeiten (umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen / Verarbeitung von Datenkategorien nach Art. 9 u. 10 DSGVO)

b) Auswahl anhand beruflicher Qualifikation und Fachkunde

c) **Pflicht zur Mitteilung der Kontaktdaten an Aufsichtsbehörde** + Veröffentlichungspflicht (Art. 37 Abs. 7 DSGVO)

II. Spezielle Punkte

11. Bestellung von Datenschutzbeauftragten

- a) Pflicht des Verantwortlichen/Auftragsverarbeiters, den Datenschutzbeauftragten **ordnungsgemäß und frühzeitig** einzubinden (Art. 38 Abs. 1 DSGVO)
- b) Pflicht des Verantwortlichen/Auftragsverarbeiters zur Bereitstellung von Ressourcen/keine Erteilung von Weisungen
- c) **Aufgaben des Datenschutzbeauftragten:**
 - Unterrichtung und Beratung des Verantwortlichen/Auftragsverarbeiters
 - Überwachung der Einhaltung von Datenschutzvorschriften
 - Sensibilisierung und Schulung der Mitarbeiter
 - Beratung/Überwachung bei Datenschutz-Folgenabschätzungen
 - Kontaktstelle für Aufsichtsbehörde

III. Zusammenfassung

1. Ab **25.05.2018** gilt die DSGVO und das BDSG-neu. Möglich bleibt die Neufassung des LDSG.
2. Einige **wesentliche Punkte** betreffen das Folgende:
 - a) Verantwortliche müssen die Einhaltung datenschutzrechtlicher Grundsätze nachweisen können (**Rechenschaftspflicht**), Art. 5 Abs. 2 DSGVO.
 - b) Insbesondere Verträge zur Auftragsverarbeitung, Betriebs- und Dienstvereinbarungen sowie Einwilligungserklärungen sind auf ihre Konformität mit den Anforderungen der DSGVO zu **prüfen und ggf. anzupassen**.
 - c) **Rechte betroffener Personen** wurden inhaltlich erweitert. Antragsgemäße Maßnahmen sind fristgemäß zu ergreifen.
 - d) Bei den **Meldepflichten** ist eine Risikoabschätzung vorzunehmen.