Datenschutz in der Steuerkanzlei

Dirk Munker, Dipl. Staatswissenschaftler (Univ.), Datenschutz-Auditor (TÜV)

Inhalt

Chronologie Datenschutz in Deutschland

30.09.1970	1. Hessisches Datenschutzgesetz
01.02.1977	1. Bundesdatenschutzgesetz (in Kraft ab 1978)
…….	
25.05.2016	In-Kraft-Treten der EU-Datenschutz-Grundverordnung (DS-GVO)
25.05.2018	EU-weite Geltung der DSGVO
25.05.2018	BDSG „neu“
??	E-Privacy-Verordnung (bislang nur Entwurf EU-Kommission!)

Erwägungsgründe u. a.

Stärkung und Präzisierung der Rechte der betroffenen Personen

Verschärfung der Auflagen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden

Gleiche Befugnisse der Mitgliedstaaten bei Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung

EU-Datenschutz-Grundverordnung

Vorrang EU-Verordnung vor nationalem Recht

EU-Verordnung hat grds. Anwendungsvorrang vor jedem nationalen

Gesetz → kein Umsetzungsgesetz im nationalen Recht erforderlich, in VO vorgesehen → nationale Regelungen möglich

Ausgestaltungspflicht durch nationalen Gesetzgeber, sofern durch VO angeordnet

Datenschutz zwischen 2 Stühlen:

BDSG-alt bis 24.05.2018

DSGVO und BDSG-neu ab 25.05.2018

Inhalt

Datenschutzprobleme der Vergangenheit und der Gegenwart

- Gehackte Steuerkanzlei zahlt EUR 100.000,00 Lösegeld in 2008
- 2014 - Aktentonne einer Thüringer Kanzlei steht auf dem Gehsteig
- Zahlreiche erpresste Kanzleien in den vergangenen Jahren (Locky, Golden Eye …), oftmals mehrere Tage Ausfall
- Abmahnungen wegen Kontaktformular (fehlender Hinweis in den Datenschutzhinweisen) und fehlender Webseitenverschlüsselung
- Angriffe werden vermehrt durch Social Networking vorbereitet

Fakten

- Datenschutz wird (zu) oft vernachlässigt
- Gefährdungspotenzial steigt durch moderne Technik

  → jederzeitige Verfügbarkeit von Daten, leichtes Erstellen von Profilen und Querverbindungen

- Beachtung gesetzlich vorgeschrieben im Bundesdatenschutzgesetz und zukünftig in der EU-Datenschutz-Grundverordnung
- Bußgeld bis zu 10/20 Millionen € bzw. 2 %/4 % des weltweiten Jahresumsatzes
- Datenschutz nicht nur lästige Pflicht/auch Vorteile

  → fördert klare Arbeitsanweisungen, bringt Image- und Vertrauensgewinn nach innen und außen, Schadensprävention

Was bedeutet Datenschutz?

Artikel 1 DSGVO

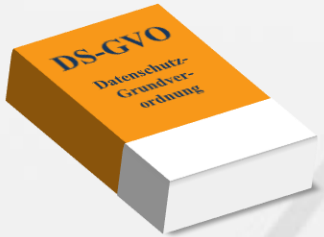
Schutzzweck

Nicht Schutz der Daten, sondern Schutz der Person = „Betroffener“ bzw. „natürliche Person“

Artikel 2 DSGVO

Schutzgut

Gilt für personenbezogene Daten:
gilt nicht im persönlichen oder familiären Bereich.



Was bedeutet Datenschutz?

- „Datenschutz“ als Gesamtheit der in verschiedenen Gesetzen zum Schutz des Individuums vorhandenen Regelungen zum Schutz der Privatsphäre.

  → Schutz vor unberechtigten Zugriffen in einer zunehmend automatisierten und computerisierten Welt.

- Schutz des Einzelnen vor einer Beeinträchtigung des Persönlichkeitsrechts!

  → **Kein „gläserner Mensch“!**

Artikel 1 Abs. 1 Grundgesetz:

„Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist die Verpflichtung aller staatlichen Gewalt.“

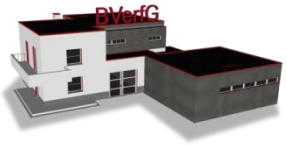
Artikel 2 Abs. 1 Grundgesetz:

„Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“

Volkszählungsurteil vom 15.12.1983:

„Grundrecht auf informationelle Selbstbestimmung“

- Schutz der Privatsphäre
- Kenntnis darüber, welche Daten wo gespeichert sind



Urteil des Bundesverfassungsgerichts vom 27.02.2008

Grundrecht auf digitale Intimsphäre

- Schutz der Daten in IT-Systemen sowie deren Vertraulichkeit und Integrität

Datenschutz hat Verfassungsrang!

Charta der Grundrechte der Europäischen Union

Schutz personenbezogener Daten

- Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Wo ist der Datenschutz geregelt?

EU Datenschutz-Grundverordnung

Bundesdatenschutzgesetz

Kirchen-Datenschutzgesetze

Landes-Datenschutzgesetze

BDSG, LDSG und Kirchen-DSG sind sog. Auffanggesetze und greifen nur, wenn die speziellen gesetzlichen Regelungen nicht greifen → DSGVO hat stets Vorrang.

Spezielle gesetzliche Regelungen:

BGB, HGB, UWG, StBerG, WPO, BRAO, AO, StGB, SGB, TMG etc.

Was sind personenbezogene Daten?

Alle Einzelangaben, die sich auf bestimmte o. bestimmbare natürliche Person beziehen

Persönliche Verhältnisse

Name, Anschrift, Geburtsdatum, Familienstand, Anzahl der Kinder	Zeugnisse / berufl. Bewertungen
Aussehen, Fingerabdruck, Iris	Kontonummer / Bankverbindung
Telefonnummer (priv. u. berufl.)	Hobbys
Arbeitgeber und Beruf	...

Was sind personenbezogene Daten?

Alle Einzelangaben, die sich auf bestimmte o. bestimmbare natürliche Person beziehen

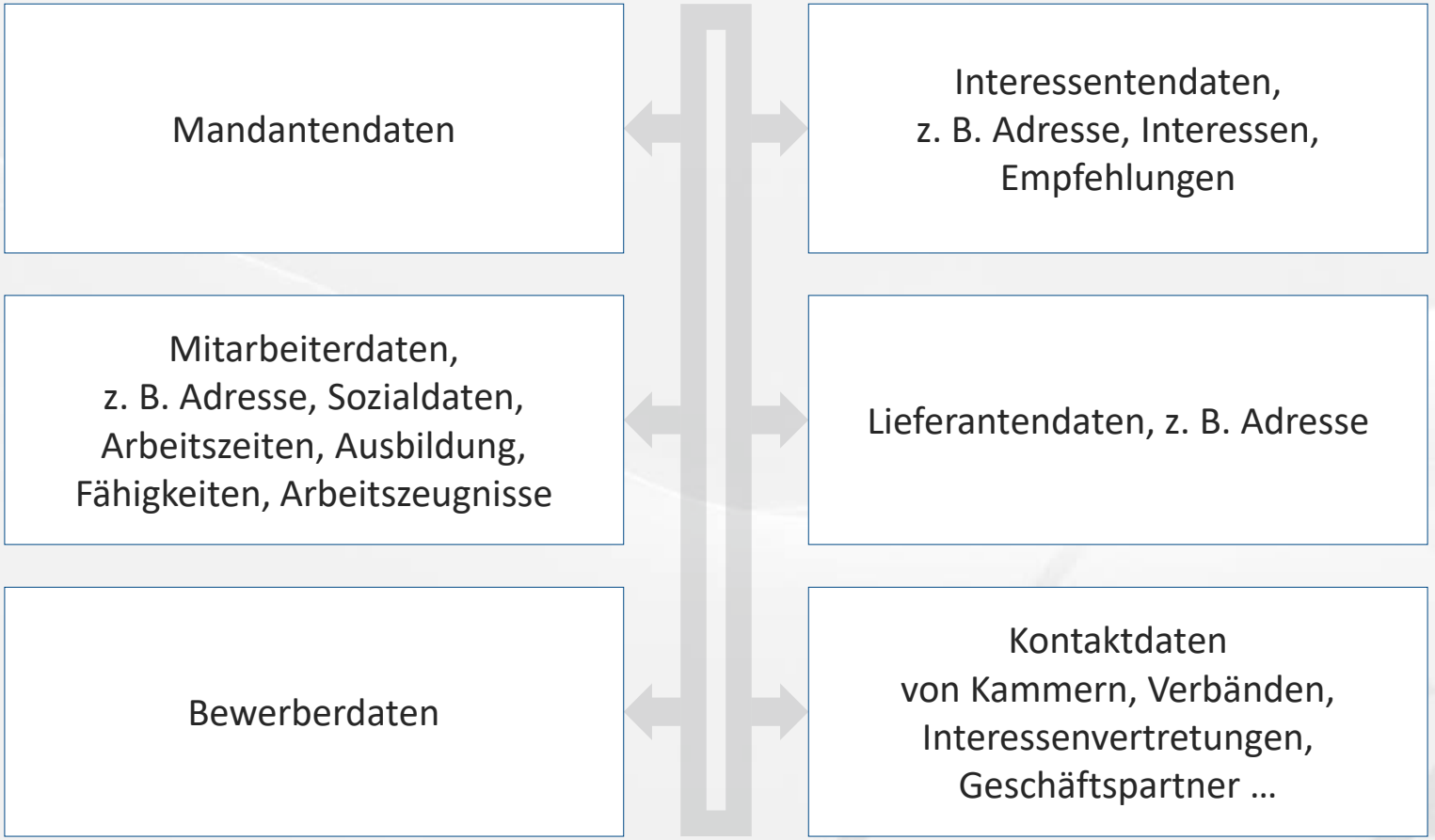
Sachliche Verhältnisse

Einkommen , Vermögen	Vertragsbeziehungen
Kfz-Typ	Führen von Telefonaten, Schreiben von E-Mails,
Steuern, Versicherungen	Umfang der Internet-Nutzung
Grundbesitz	...

„Besondere Arten“ personenbezogener Daten

- Rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit
- Verarbeitung von genetischen/biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

Welche personenbezogenen Daten gibt es in der Kanzlei?



- Berufsträger nach § 57 Abs. 1 StBerG
  (ggf. auch § 43 Abs. 1 Satz 2 WPO oder § 43a Abs. 2 Satz 1 BRAO)
- Gehilfen nach § 62 StBerG
  (ggf. auch § 50 WPO oder § 2 Abs. 4 BORA i. V. m. § 43a Abs. 2 Satz 1 BRAO)
- § 203 Strafgesetzbuch (StGB)
  - Berufsträger nach § 203 Abs. 1 Nr. 3 StGB
  - Gehilfen nach § 203 Abs. 3 Satz 2 StGB

    „Wer unbefugt ein fremdes Geheimnis … offenbart … wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.“
- **Gilt nur für Mandantendaten!**

Art. 29 DSGVO

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten…

§ 88 TKG (Telekommunikationsgesetz)

Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

§ 17 UWG (Gesetz gegen den unlauteren Wettbewerb)

Verrat von Geschäfts- oder Betriebsgeheimnissen

§ 35 SGB I (Sozialdatenschutz bzw. erweiterter Sozialdatenschutz)

Personalabteilung bzw. Mitarbeiter die mit Leistungsträgern im Sinne der SGB kommunizieren (§ 78 SGB X: Personen oder Stellen, die nicht in § 35 des Ersten Buches genannt und denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck verarbeiten oder nutzen, zu dem sie ihnen befugt übermittelt worden sind. Die Dritten haben die Daten in demselben Umfang geheim zu halten wie die in § 35 des Ersten Buches genannten Stellen).

- **Grundsatz:**

  Personenbezogene Daten dürfen **gar nicht** erhoben, verarbeitet oder genutzt werden, es sei denn…

- **Nach DSG-VO erlaubt:**
  - Einwilligung,
  - Erfüllung eines Vertrags,
  - rechtliche Verpflichtung,
  - lebenswichtige Interessen schützen,
  - Wahrnehmung einer Aufgabe … im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt,
  - Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten

    erforderlich, sofern nicht Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

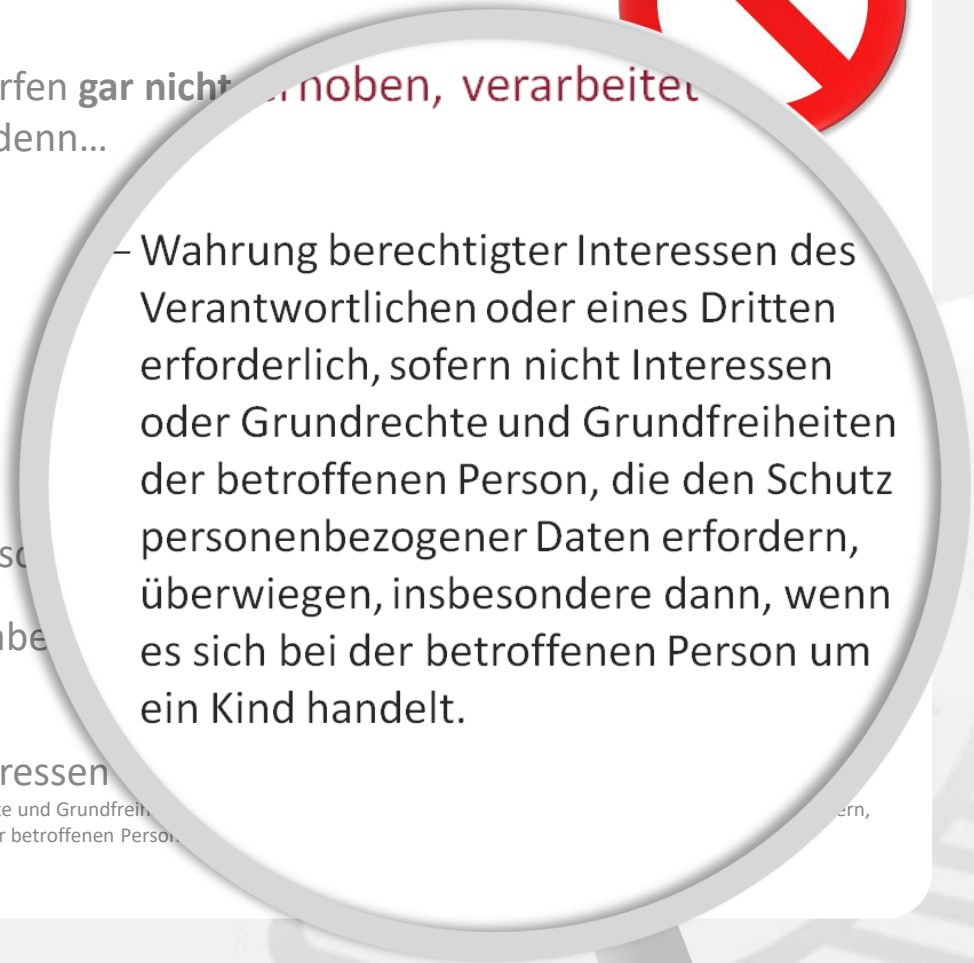
Verbot mit Erlaubnisvorbehalt

- **Grundsatz:**

  Personenbezogene Daten dürfen **gar nicht** [illegible] noben, verarbeitet oder genutzt werden, es sei denn…

- **Nach DSG-VO erlaubt:**
  - Einwilligung,
  - Erfüllung eines Vertrags,
  - rechtliche Verpflichtung,
  - lebenswichtige Interessen s[illegible]
  - Wahrnehmung einer Aufgabe [illegible] öffentlicher Gewalt,
  - Wahrung berechtigter Interessen

    erforderlich, sofern nicht Interessen oder Grundrechte und Grundfrei[illegible] überwiegen, insbesondere dann, wenn es sich bei der betroffenen Perso[illegible] [illegible]ern,



Häufige Rechtsgrundlagen in der Kanzlei

Erhebung, Verarbeitung und Nutzung von

Mandantendaten, Daten von Geschäftspartnern und Daten von Kommunikationspartnern auf Grundlage von Art. 6, Art. 21 und EG 45 ff. DSGVO

Mitarbeiterdaten auf der Grundlage von Art. 88 und EG 155 DSGVO, § 26 BDSG 2018, ggf. auch durch Einwilligung (z. B. Fotos auf der Homepage)

Art. 5 DSGVO (Grundsätze für die Verarbeitung personenbezogener Daten)

- Rechtmäßigkeit,
- Verarbeitung nach Treu und Glauben,
- Transparenz,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung,
- Integrität,
- Vertraulichkeit

Bedrohungen und mögliche Schwachstellen

- Angriffe können sich gegen Nutzer, Systeme, Anwendungen und Netze richten.
- Eine große Rolle spielt der „Faktor Mensch“,
  - Fahrlässigkeit, ggf. durch Unwissen oder mangelnde Sensibilisierung
  - Vorsatz
- Höhere Gewalt
- organisatorische Mängel
- technisches Versagen

Beispiel: Risiken bei der Datensicherung

- Wenig oder gar keine Zeit
- unregelmäßige Sicherungszyklen
- veraltete und zu wenige Datenträger
- Unverschlüsselte Datenträger werden ausgelagert.
- Datensicherung nicht erfolgt.
- Rücksicherung wird nicht getestet.
- Sicherung nicht komplett
- kein Sicherungskonzept
- Beschlagnahmeschutz bei Auslagerung?

Inhalt

Der Zusammenhang zwischen Datenschutz und Datensicherheit

Datenschutz

Schutz des Persönlichkeitrechts

Art. 32 DSGVO

Datensicherheit

Verfügbarkeit

Vertraulichkeit

Integrität

Verbindlichkeit

Art. 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)

- **Zu berücksichtigen:**
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfangs, Umstände und der Zwecke der Verarbeitung
  - Eintrittswahrscheinlichkeit
  - Risiken für die Rechte und Freiheiten natürlicher Personen

Art. 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)

- **Zu ergreifen sind:**
  - geeignete technische und organisatorische Maßnahmen
  - Datenschutzkonforme Voreinstellungen, u. a. bei
    - Umfang der Verarbeitung
    - Speicherfrist
    - Zugänglichkeit
- **Zertifizierung nach Art. 42 als möglicher Nachweis**

Art. 32 DSGVO (Sicherheit der Verarbeitung)

Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung … Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ... geeignete technische und organisatorische Maßnahmen,

- Pseudonymisierung und Verschlüsselung
- Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit der Systeme und Dienste
- Verfügbarkeit der personenbezogenen Daten und rasche Wiederherstellung
- regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
- Berücksichtigung der Risiken bei der Beurteilung des Schutzniveaus

Art. 5 Abs. 2 DSGVO (Grundsätze für die Verarbeitung personenbezogener Daten):

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

Art. 24 Abs. 2 DSGVO (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.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

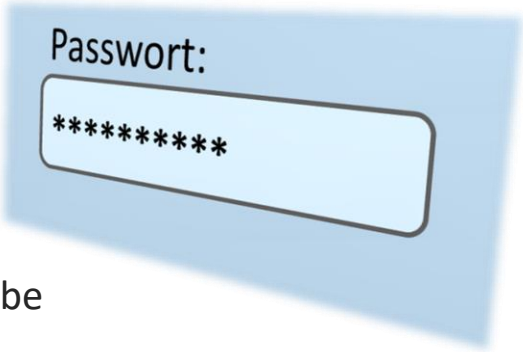
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	**Zutrittskontrolle**
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Zutrittskontrolle

Einbruchschutz wie Zaun, Türen, Fenster, Rollladen	Schlüsselausgabeliste	Begleitung des Wartungspersonal
Alarmanlage	zeitgesteuerte Schlösser	Reinigungskräfte
Videoüberwachung	Verpflichtung des Wartungspersonals	Heimarbeitsplätze

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Zugangskontrolle



- Passwortkomplexität, -länge, -wechsel

  → **Wie gestaltet man ein sicheres Passwort?**

- Sperrung des Accounts bei mehrfacher Falscheingabe
- Mehrfachauthentifizierung
- Protokollierung der Anmeldungen und Anmeldeversuche
- Schloss (Kensingtonschloss)
- BIOS-Passwort, Bitlocker
- Bildschirmschoner mit Time-Out und Passwortschutz

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Zugriffskontrolle

- Rollen-/Rechtekonzept

  → **Vergabe der Berechtigung durch die Kanzleileitung, nicht durch die IT**

- Besonderer Schutz für Systemdaten und Protokolle

  → Stichwort: Kontrolle Privatnutzung

- regelmäßige Überprüfung der Berechtigungen
- Protokollierung der Zugriffe und Zugriffsversuche
- Umgang mit USB-Sticks und Festplatten
- Verbot privater Datenträger
- Entsorgung von Papier und Datenträgern

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Trennungskontrolle

- Getrennte Speicherung, Veränderung, Löschung, Übermittlung
- interne Mandantenfähigkeit/Zweckbindung
- Funktionstrennung (Produktion/Test)
- organisatorische Trennung der Datenbestände nach Zuständigkeit
- Trennen von Bearbeitungs- und Publikumszonen!
- Softwareseitige Trennung von Daten (Mandantendaten, Mitarbeiterdaten, Lieferantendaten) auf unterschiedlichen Laufwerken oder Systemen
- feste Zuordnung verantwortlicher Mitarbeiter und deren Handlungsspielräume (Nutzungsrechte und Freigaben im Netzwerk, Stellenbeschreibung der einzelnen Mitarbeiter), Aufteilung nach Tätigkeitsbereichen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Pseudonymisierung

„Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können,

- sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und
- technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.

Pseudonymisierung

Datenminimierung wirksam umsetzen

Risiken für die betroffenen Personen senken

Verantwortliche und Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	**Weitergabekontrolle**
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Weitergabekontrolle

- Wo erfolgt welche Übermittlung?
- An wen darf übermittelt werden?
- Wie und womit wird übermittelt?
- Wer darf übermitteln?
- Archivierung der Übermittlung
- Postein- und -ausgangsbuch
- Verschlüsselung, auch E-Mail-Verschlüsselung

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Eingabekontrolle

Protokollierung der Zugriffe auf das System und im System	(revisionssichere) Archivierung von Daten und Dokumenten
Protokollierung der Administrationstätigkeiten	Stellenbeschreibungen, Dienstanweisungen, Geschäftsverteilungsplan
Protokollierung der Vergabe von Berechtigungen	ggf. QM-Handbuch

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	**Verfügbarkeitskontrolle**
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Verfügbarkeitskontrolle

- Feuerlöscher (Serverraum CO2-Löscher!)
- unterbrechungsfreie Stromversorgung
- Notstromaggregat
- Klimaanlage im Serverraum
- getrennte Aufbewahrung von Sicherungsdatenträgern

Verfügbarkeitskontrolle

kanzleiweit einheitliches Virenprogramm

regelmäßige Virenprüfungen

Firewall, Virenschutz

keine Nutzung privater Software auf Kanzleirechnern

regelmäßige Aktualisierung des Virenprogramms

Verfügbarkeitskontrolle

Notfallplan

Papier-Ersatzverfahren prüfen und vorbereiten (Erreichbarkeit der Mandanten?)

Vereinbarungen mit IT-Dienstleister und Lieferanten über Reaktionszeiten

Verhaltensvorschriften (Alarmpläne)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Rasche Wiederherstellbarkeit

- Datensicherung
  - Datensicherungsverfahren (Zeitpunkte, Umfang, Aufbewahrungsdauer)
  - Tages-, Monats-, Halbjahres- und Jahressicherungen
  - sichere Lagerung
  - Überprüfung der Sicherungsläufe
  - Übungen zur Datenwiederherstellung
- Notfallplan
- Vertrag mit IT-Dienstleister

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	**Datenschutz-Management**
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Datenschutz-Management

planen

organisieren

Gesetzliche und betriebliche Anforderungen des Datenschutzes systematisch

kontrollieren

steuern

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Organisatorischer und technischer Prozess der Reaktion auf erkannte oder vermutete Datenschutzpannen

Schulung der Mitarbeiter → Erkennen der Panne + Schaden begrenzen

Abwägung der Risiken für den Betroffenen

Meldung an Aufsichtsbehörde innerhalb von 72 Stunden,
Ausnahme: Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für Rechte und Freiheiten natürlicher Personen.

- Art der Verletzung des Schutzes personenbezogener Daten (Kategorien, Zahl der Betroffenen)
- Namen und die Kontaktdaten des Datenschutzbeauftragten (oder einer sonstigen Anlaufstelle)
- Beschreibung der wahrscheinlichen Folgen
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen
- gegebenenfalls Maßnahmen zur Abmilderung der nachteiligen Auswirkungen.

Organisatorischer und technischer Pro… …auf erkannte oder vermutete…

Schulung der Mitarbei…

Abwägung der Risi…

Meldung an Aufsi… Ausnahme: Verletz… sichtlich nicht zu ei… …en.

- Art der Verletzung des Schutzes pers…
- Namen und die Kontaktdaten des Date…
- Beschreibung der wahrscheinlichen Folge…
- Beschreibung der ergriffenen oder vorgeschlag…
- gegebenenfalls Maßnahmen zur Abmilderung der n…

Risiko für Rechte…

- Art der Verletzung des Schutzes personenbezogener Daten (Kategorien, Zahl der Betroffenen)
- Namen und die Kontaktdaten des Datenschutzbeauftragten (oder einer sonstigen Anlaufstelle)
- Beschreibung der wahrscheinlichen Folgen
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen
- gegebenenfalls Maßnahmen zur Abmilderung der nachteiligen Auswirkungen.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Datenschutzfreundliche Voreinstellungen

EW 78 und Art. 25 DSGVO

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.

Datenschutzfreundliche Voreinstellungen

EW 78 und Art. 25 DSGVO

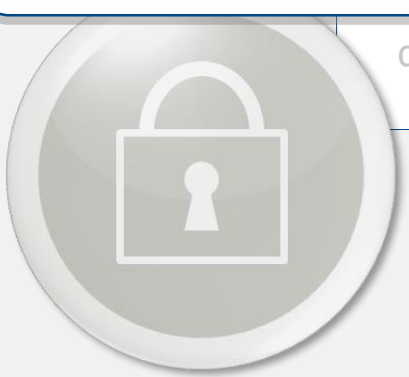
Interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des

HINWEIS

Datenminimierung hinsichtlich

- Menge der erhobenen personenbezogenen Daten
- Umfang ihrer Verarbeitung
- Speicherfrist
- Zugänglichkeit

default) Genüge tun.



1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)	Zutrittskontrolle
	Zugangskontrolle
	Zugriffskontrolle
	Trennungskontrolle
	Pseudonymisierung
2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)	Weitergabekontrolle
	Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle
	rasche Wiederherstellbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management
	Incident-Response-Management
	datenschutzfreundliche Voreinstellungen
	Auftragskontrolle

Auftragsdatenverarbeitung im BDSG-alt,

- Weisungsabhängig!
- Auftraggeber haftet dem Dateneigentümer (Betroffenen) gegenüber!

Funktionsübertragung, wenn der Auftragnehmer nicht nur Daten verarbeitende Hilfsfunktionen weisungsabhängig erfüllt, sondern die übergebenen Daten zur Erfüllung weiterer eigener Aufgaben oder Funktonen benötigt.

- Übermittlung an „Dritte“
- Haftung gegenüber dem Dateneigentümer geht an den Funktionsnehmer über!

Ist die herkömmliche Abgrenzung zur „Funktionsübertragung“ jetzt obsolet?

Datenverarbeitung im Auftrag → Auftragsverarbeitung

Auftragsdatenverarbeitung im BDSG-alt,

- Weisungsabhängig!
- Auftraggeber haftet dem Dateneigentümer (Betroffenen) gegenüber!

MERKE

Bei Verstoß des Auftragnehmers gegen die DSGVO oder andere datenschutzrechtliche Regelungen → Mithaftung!

Erfüllung weiterer eigener Aufgaben oder Funktionen benötigt.

- Übermittlung an „Dritte“
- Haftung gegenüber dem Dateneigentümer geht an den Funktionsnehmer über!

Ist die herkömmliche Abgrenzung zur „Funktionsübertragung“ jetzt obsolet?

Beispiele für Datenverarbeitung im Auftrag

Lohnbuchhaltungsbüros, Datenerfassungsbüros, Rechenzentren, Copyshops	Entsorger (IT/TK) und Entsorger Papier
externe Dienstleister EDV und TK mit „Remote-Zugriff“, Server, Aktivkomponenten, Datenbanken, Wartungsverträge, Softwarepflege, etc.	Internet-Service-Provider, Internet und E-Mail-Dienste
externe Dienstleister Peripherie IT/TK, Faxgeräte, Drucker, Multifunktionsgeräte, Scanner, Kopiergeräte, etc.	Application-Service-Provider (Fremdsoftware als Dienstleistung), z. B. Softwareanbieter, Systempartner

Auftragsverarbeitung nach Art. 28 DSGVO

Sorgfältige Auswahl der Auftragnehmer, hinreichende Garantien!

Kriterien für die Auswahl der Auftragnehmer: geeignete technische und organisatorische Maßnahmen

detaillierte Regelungen der Auftragsverhältnisse (schriftlich oder elektronisch)

detaillierte Regelungen der Unterauftragsverhältnisse, Einsatz und Wechsel von Subunternehmen nur mit schriftlicher Genehmigung

Detaillierte Regelungen der Auftragsverhältnisse

- Weisung des Verantwortlichen
- Verpflichtung der Mitarbeiter zur Vertraulichkeit
- Maßnahmen nach Art. 32 (Sicherheit der Verarbeitung, TOMs)
- Regelungen zu Subdienstleistern

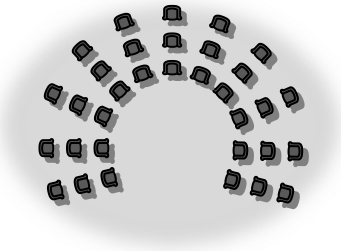
- Unterstützung des Auftraggebers bei der Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte betroffener Person
- Unterstützung des Verantwortlichen bei Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten:
  - Meldung von Datenschutzpannen,
  - Benachrichtigung der Betroffenen,
  - Datenschutz-Folgenabschätzung.

Detaillierte Regelungen der Auftragsverhältnisse

- Löschung oder Rückgabe von Daten nach Beendigung
- Unterstützung des Verantwortlichen bei Überprüfungen — einschließlich Inspektionen
- unverzügliche Information, falls eine Weisung des Verantwortlichen gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt

Kontrolle der Auftragsverhältnisse

Kontrolle der Unterauftragnehmer (z. B. durch den DSB)	Selbstauskünfte?
Zertifizierung?	Grundsätzlich wird eine jährliche Kontrolle empfohlen!
Genehmigte Verhaltensregel?	Notwendigkeit von Vor-Ort-Audits?



960. Sitzung des Bundesrats am 22. September 2017:

„Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“:

§ 203 c) Abs. 3 wird wie folgt geändert:

Die in den Absätzen 1 und 2 Genannten*) dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

*) u. a. Steuerberater

§ 203 Strafgesetzbuch - Neue Rechtliche Situation

960. Sitzung des Bundesrats am 22. September 2017:

„Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“:

HINWEIS

Lösung:

Verpflichtung der Dienstleister auf die Verschwiegenheit nach § 203 StGB! (Subunternehmer nicht vergessen!)

Die in den Absätzen 1 und 2 Genannten*) dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

*) u. a. Steuerberater

Auftragskontrolle bei Berufsgeheimnisträgern

Sämtliche Auftragsverarbeiter und Subunternehmen sind als **„Mitwirkende“** auf § 203 Strafgesetzbuch zu verpflichten!

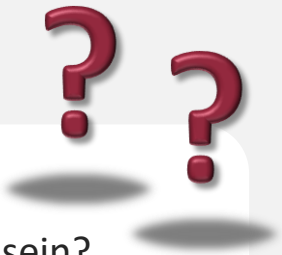
Verpflichtung ist erforderlich!

Bei Berufsgeheimnisträgern wird die jährliche Kontrolle der Auftragsverarbeiter dringend empfohlen!

Pflichten des Auftragnehmers

- Arbeiten nach Weisung des Auftraggebers
- Hinweispflichten bei Verstößen
- Benennung des Datenschutzbeauftragten
- Nachweis der Sicherungsmaßnahmen (technisch-organisatorische Maßnahmen), ggf. auch durch Zertifikate oder Auditberichte
- (Führung des Verzeichnisses der Verarbeitungstätigkeiten beim Auftragsverarbeiter)

Die Steuerkanzlei als Auftragsverarbeiter?



- Kann eine Steuerkanzlei Auftragsdatenverarbeiter eines Mandanten sein?
- Hierzu gab es in der Vergangenheit unterschiedliche Auffassungen.
- Einhellige Meinung Bundessteuerberaterkammer und Mehrzahl der Datenschutzaufsichtsbehörden in der Welt BDSG-alt:

  Nein, da die freiberufliche, eigenverantwortliche Tätigkeit die enge Weisungsgebundenheit im Sinne des § 11 BDSG nicht zulässt.

- **DSGVO und BDSG-neu → ???**

Zusammenfassung Auftragsverarbeitung

Wechsel von Subunternehmer nur mit Genehmigung

Elektronische Form des Vertrages zur Auftragsverarbeitung möglich

Verpflichtung nach § 203 StGB beachten!

Nachweis der Garantien: Zertifikate oder genehmigte Verhaltensregeln, ggf. auch Audits vor Ort

Regelmäßige (jährliche) Kontrolle der Auftragsverarbeiter

Inhalt

- Notwendigkeit der Bestellung nach Art. 37 DSGVO
- oder § 38 BDSG-neu
  - mehr als neun Personen bei automatisierter Datenverarbeitung
  - mindestens 20 Personen bei Datenverarbeitung auf andere Weise
- oder freiwillig gemäß Art. 37 Abs. 4 Satz 1 DSGVO

- Voraussetzungen nach Art. 37 DSGVO
  - berufliche Qualifikation
    - Fachwissen
    - Fähigkeiten

Die Rechte des Datenschutzbeauftragten

Frühzeitige und ordnungsgemäße Einbindung	Geheimhaltung und Vertraulichkeit, deshalb Zeugnisverweigerungs-recht und Beschlagnahmeverbot für Unterlagen und Akten des DSB
Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen	Weisungsfreiheit
Teilnahme an Fort- und Weiterbildungsmaßnahmen auf Kosten der verantwortlichen Stelle	Benachteiligungsverbot, Kündigungsschutz auch weiterhin naheliegend (interner Datenschutzbeauftragter)

Die Benennung zum Datenschutzbeauftragten

Empfehlung: schriftlich mit Verweis auf Aufgaben

Befristung ist strittig (Kommentare BDSG-alt: bei wichtigen Grund oder externem DSB, 2 oder 3 Jahre?)

Unterstellung, Berichterstattung

Aufgaben des Datenschutzbeauftragten

Unterrichtung und Beratung

- des Verantwortlichen oder
- des Auftragsverarbeiters und
- der Beschäftigten

Überwachung der Einhaltung der DSGVO, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten

Überwachung der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten

Überwachung der Strategien zur Sensibilisierung und Schulung der beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen

Aufgaben des Datenschutzbeauftragten

Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung

Zusammenarbeit mit der Aufsichtsbehörde

Tätigkeit als Anlaufstelle für die Aufsichtsbehörde

Aufgaben des Datenschutzbeauftragten

Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung

HINWEIS

Datenschutzbeauftragter trägt bei Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er Art, Umfang, Umstände und Zwecke der Verarbeitung berücksichtigt.

Tätigkeit als Anlaufstelle für die Aufsichtsbehörde

Vorteile:

- Kennt die Kanzlei und ist in den internen Ablauf eingebunden.

Nachteile:

- Zeitaufwand geht zu Lasten seiner eigentlichen Tätigkeit,
- Gefahr der „Betriebsblindheit“,
- ggf. Interessenkollisionen:
  - Inhaber, Vorstand oder Geschäftsführer,
  - Leiter EDV, Systemadministrator,
  - Leiter Personal,
  - ggf. Geldwäschebeauftragter.

Vorteile:

- Spezialkenntnisse sind bereits vorhanden, d. h. keine Fortbildungsmaßnahmen,
- besitzt breit gefächerte Kenntnis (Synergieeffekte), oftmals auch branchenspezifische Kenntnisse.

Nachteile:

- ist nicht ohne weiteres in den Kanzleiablauf eingebunden,
- kennt die Kanzlei anfangs nicht.

Meldung/Veröffentlichung des Datenschutzbeauftragten

Meldung der Kontaktdaten des Datenschutzbeauftragten
an die Aufsichtsbehörde zum Stichtag 25.05.2018

Internetauftritt → Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten im Rahmen des Datenschutzhinweises

Information nach Artikel 13 → Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten

Inhalt

Betroffenenrechte

- Informationspflicht bei Datenerhebung (Art. 13, Art. 14)
- Auskunftsrecht inkl. Kopie der Daten (Art. 15)
- Berichtigung, Korrekturbegehren (Art. 16)
- Löschung, Löschungsbegehren (Art. 17)
- Einschränkung (Art. 18)
- Mitteilungspflicht bei Berichtigung, Löschung, Einschränkung der Verarbeitung (Art. 19)
- Datenübertragbarkeit (Art. 20)
- Widerspruch, Widerruf (Art. 21)
- Profiling (Art. 22)

Betroffenenrechte

- Informationspflicht bei Datenerhebung (Art. 13, Art. 14)
- Auskunftsrecht inkl. Kopie der Daten (Art. 15)

HINWEIS

Alle Maßnahmen sollen unter Berücksichtigung der wirtschaftlichen Verhältnismäßigkeit getroffen werden.

- Mitteilungspflicht bei Berichtigung, Löschung, Einschränkung der Verarbeitung (Art. 19)
- Datenübertragbarkeit (Art. 20)
- Widerspruch, Widerruf (Art. 21)
- Profiling (Art. 22)

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche … Folgendes mit:

- den Namen und die Kontaktdaten des Verantwortlichen …;
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten; (heißt: wenn vorhanden, dann mitteilen!)
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung …
- wenn die Verarbeitung auf … beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln,
- **das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der EU-Kommission**

  oder … einen

  Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

- Zusätzlich … stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung …:
- die Dauer, für die die personenbezogenen Daten gespeichert werden …;
- das Bestehen eines Rechts auf Auskunft … Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie
- Recht auf Datenübertragbarkeit;
- das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- 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;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling … 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.

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

- Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten …, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen … zur Verfügung.

Informationspflicht in der Steuerkanzlei

- Im Rahmen des Steuerberatungsvertrages
- Internetauftritt
- jede weitere Verarbeitung personenbezogener Daten
- im Rahmen des Arbeitsverhältnisses

Inhalt

Das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 beim Verantwortlichen

Ausnahmen für Unternehmen mit weniger als 250 Mitarbeiter, sofern keine kritische Datenverarbeitung

Gibt es eine Unternehmen ohne kritische Verarbeitung?

Auf welcher Grundlage soll sonst die Risikobewertung erfolgen?

Das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 beim Verantwortlichen

- Namen und die Kontaktdaten des Verantwortlichen
- Datenschutzbeauftragter
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern
- Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation
- Fristen für die Löschung der verschiedenen Datenkategorie
- Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1

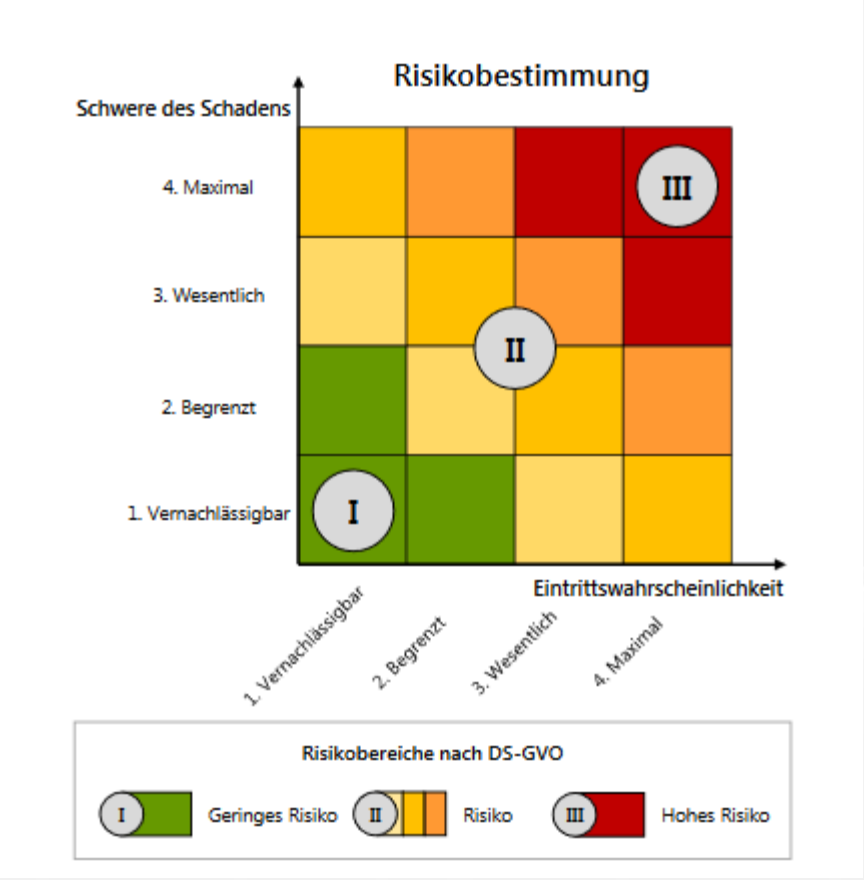
Risikobewertung im Verzeichnis der Verarbeitungstätigkeiten

Eintrittswahrscheinlichkeit – Risiko für den Betroffenen

ggf. Zusammenfassung in Kategorien

hohes Risiko → Datenschutz-Folgenabschätzung

Risikobewertung im Verzeichnis der Verarbeitungstätigkeiten



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

Inhalt

Hohes Risiko durch

- Verwendung neuer Technologien
- Art, Umfang, Umstände und Zwecke der Verarbeitung

Datenschutz-Folgenabschätzung, insbesondere bei

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten
- umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (Videoüberwachung).

Inhalt:

- systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
- gegebenenfalls … berechtigte Interessen,
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge,
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen,
- Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personen-bezogener 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.

Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch

- die zuständigen Verantwortlichen oder
- die zuständigen Auftragsverarbeiter,

ist bei Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch

MERKE

Verbleibt ein hohes Restrisiko: Konsultation der Datenschutzaufsichtsbehörde zwingend erforderlich!

Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

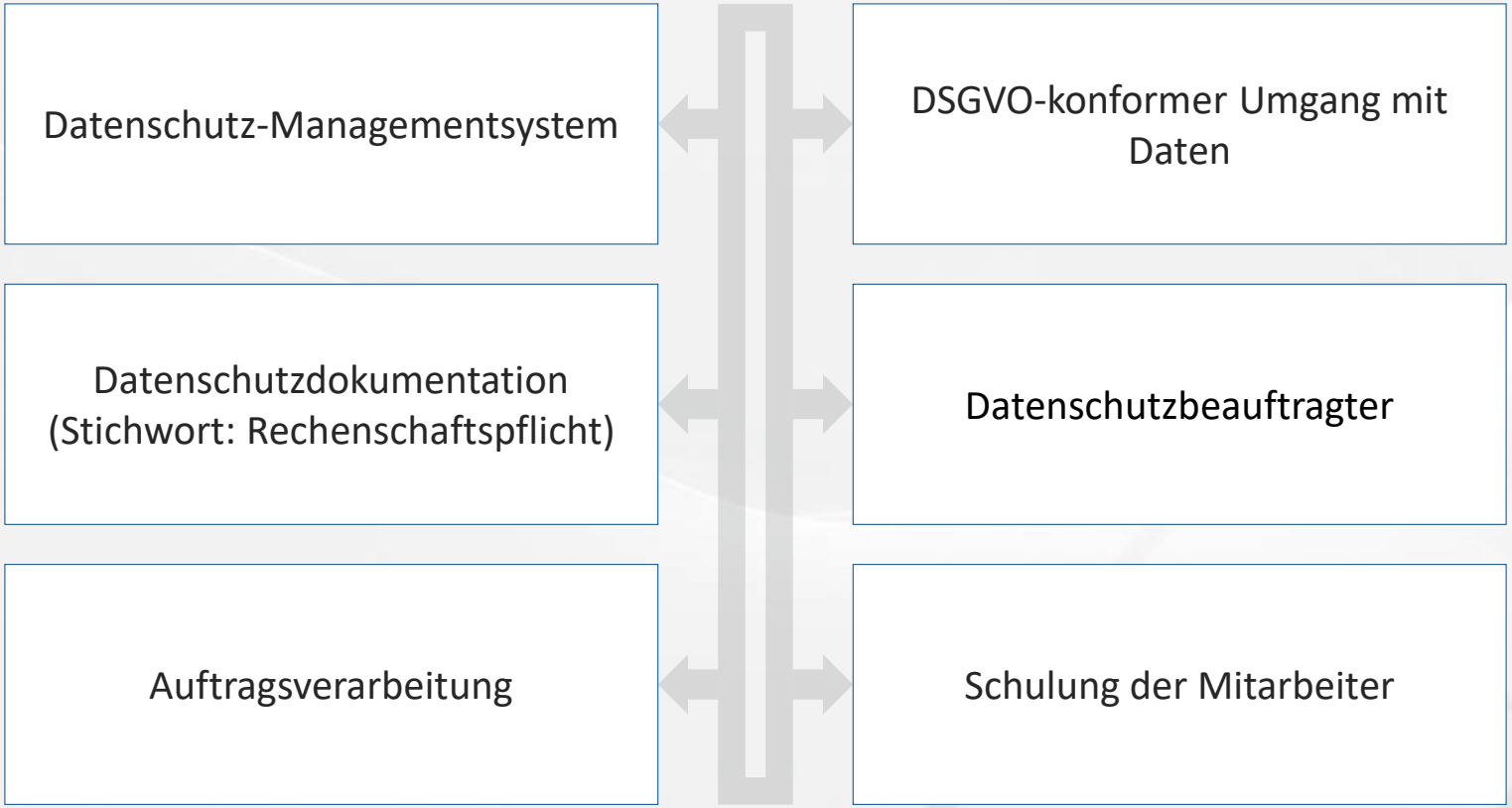
Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch

- die zuständigen Verantwortlichen oder
- die zuständigen Auftragsverarbeiter,

ist bei Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

Inhalt

Handlungsfelder in der Kanzlei

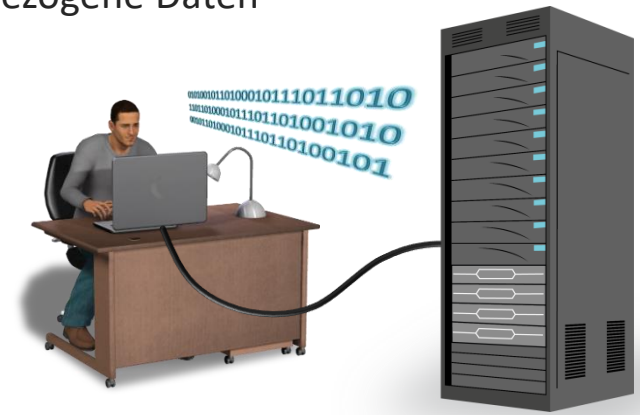


Datenschutz-Managementsystem

Benennung eines Datenschutzbeauftragten (falls mehr als zehn Mitarbeiter personenbezogene Daten verarbeiten)	Prozess zur Meldung an die Aufsichtsbehörde
rechtzeitige Einbindung des Datenschutzbeauftragten	Prozess zur Beantwortung von Anfragen
Meldung der Kontaktdaten des Datenschutzbeauftragten an Aufsichtsbehörde, Veröffentlichung Kontaktdaten	Prozess zur Löschung
Übersicht über die Dienstleister	Prozess zur Verpflichtung auf das Datengeheimnis/auf § 203 StGB
Richtlinien und Anweisungen, ggf. Betriebsvereinbarungen	Umgang mit Beschäftigtendaten (und Bewerbern)

Datenschutzdokumentation (Stichwort: „Rechenschaftspflicht“)

- Darstellung aller Prozesse, in den personenbezogene Daten verarbeitet werden
- Risikobewertung mit Schwellwertanalyse
- ggf. Datenschutz-Folgenabschätzung
- Informationsblatt nach Artikel 13
- regelmäßige Berichterstattung des Datenschutzbeauftragten



Handlungsfelder in der Kanzlei

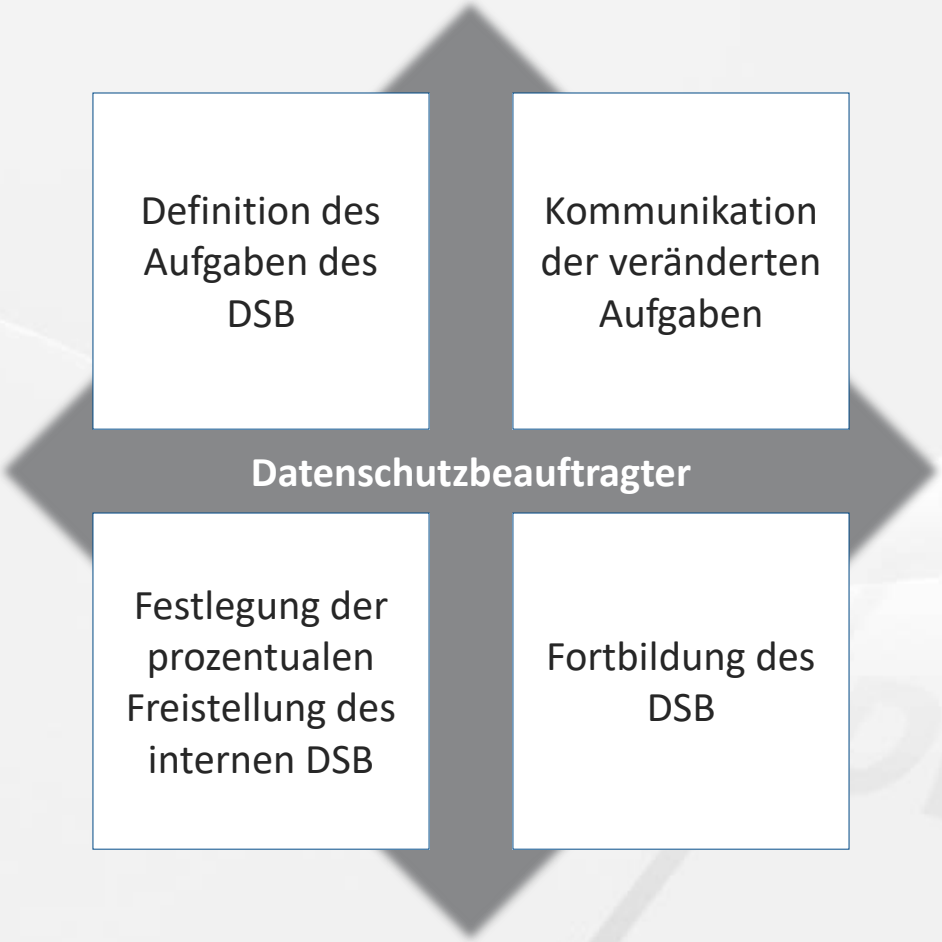
Auftragsverarbeitung

- bestehende Verträge überprüfen
  - ggf. neu schließen
- Eigener Mustervertrag?
  - Zukünftige Einordnung der Leistungen eines Steuerberaters?

DSGVO-konformer Umgang mit Daten

- Fortbildung der Mitarbeiter
- Software DSGVO-konform?
- Auskunftsrechte Betroffener
- Privacy by Design und Privacy by Default
- Recht auf Sperrung, Berichtigung bzw. Löschung

Handlungsfelder in der Kanzlei



Schulung der Mitarbeiter

Sensibilisierung der Mitarbeiter, auch im Hinblick auf alltägliche Risiken (Schadsoftware, Social Networking etc.)

regelmäßige Information der Mitarbeiter über aktuelle Vorfälle und Risiken

Verpflichtung der Mitarbeiter auf das Datengeheimnis

Inhalt

Wer überwacht die Einhaltung des Datenschutzes?

Aufsichts-behörden!

Mandanten?

Betroffene? (Anfragen!)

Mitbewerber?

Verbände? Kammern?

Geschäftsleitung?
Datenschutzbeauftragter!
Jeder Mitarbeiter?

Wer überwacht die Einhaltung des Datenschutzes?

Der Europäische Datenschutzausschuss

18 Aufsichtsbehörden

- Überwachen die Anwendung der DSGVO
- Sensibilisieren und beraten Regierungen, Öffentlichkeit, Verantwortliche und Auftragsverarbeiter
- befassen sich mit Beschwerden
- erstellen eine Liste der Verarbeitungsarten für die eine Datenschutz-Folgenabschätzung durchzuführen ist
- fördern die Ausarbeitung von Verhaltensregeln
- regen die Einführung von Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln und -prüfzeichen an
- …

Inhalt

EU-Datenschutz-Grundverordnung

regelt das Recht auf Schutz persönlicher Daten als Grundrecht innerhalb der EU

… vereinheitlicht weitgehend die derzeit bestehenden 28 nationalen Gesetze innerhalb der EU

… erhöht die Sanktionen bei Vergehen drastisch (bis zu 20 Mio. € bzw. 4 % des weltweiten Umsatzes), Öffnungsklausel für öffentliche Stellen

EU-Datenschutz-Grundverordnung

wird über die Aufsichtsbehörde voraussichtlich wesentlich strenger exekutiert als das bisher der Fall war

beinhaltet eine Meldepflicht (innerhalb von 72 Stunden an Aufsichtsbehörde) und Beweislastumkehr

tritt am 25. Mai 2018 EU-weit in Kraft

setzt wesentlich mehr an Dokumentation voraus als das BDSG

Folgen von Datenschutzverstößen

- Image der Kanzlei nimmt Schaden
- evtl. Informationspflicht nach Art. 33 DSGVO
- ggf. Schadensersatzpflicht gegenüber dem Betroffenen
- für Beschäftigte: arbeitsrechtliche Konsequenzen
- Ordnungswidrigkeit Bußgeld bis zu 10 Mio €/20 Mio € oder 2 %/4 % des weltweiten Jahresumsatzes
- Straftat: Geldstrafe oder Freiheitsstrafe bis zu 3 Jahren.

Vorteile für die Kanzlei

Die Umsetzung eines professionellen Datenschutzkonzepts schafft auch positive Nebeneffekte!

- Ansätze zur Prozessoptimierung
- positive Imagewirkung
- klarer Wettbewerbsvorteil
- Argumentationshilfe für Mandantenbetreuung und Mandantengewinnung

Vielen Dank für Ihre Aufmerksamkeit

Dirk Munker,
Dipl. Staatswissenschaftler (Univ.),
Datenschutz-Auditor (TÜV)