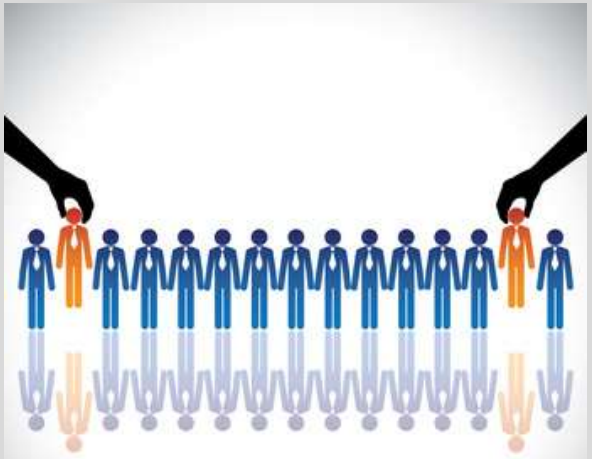
MUNKER Datenschutz

Die EU-DSGVO und die verschärften Regelungen Auftrags(daten)verarbeitung



MUNKER Datenschutz

Dirk Munker

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

Datenschutzbeauftragter des LSWB

Mehr als 12 Jahre Erfahrung im Datenschutz, darunter u.a.:

- Datenschutz in Steuerkanzleien
- Medizinischer Datenschutz
- Datenschutz in KMU
- Datenschutz im Personalwesen
- Datenschutz bei Finanzdienstleistern…

LSWB kanzleiplus

BvD e.V. Datenschutzbeauftragter nach Verbandskriterien verpflichtet Nr.: 100265

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

TÜVRheinland ZERTIFIZIERT
Geprüfte Qualifikation
Gültig bis: 10.05.2018
www.tuv.com
ID 0000040134

MUNKER Datenschutz

Chronologie Datenschutz in Deutschland

- 30.09.1970 1. Hessisches Datenschutzgesetz
- 01.02.1977 1. Bundesdatenschutzgesetz (in Kraft ab 1978)
- …….
- 14.04.2016 Beschluss der EU-Datenschutz-Grundverordnung (EU-Parlament)
- 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!)

MUNKER Datenschutz

EU-Datenschutz-Grundverordnung

- Erwägungsgründe u. a.
  - Stärkung und Präzisierung der Rechte der betroffenen Personen,
  - Verschärfung der Auflagen,
  - gleiche Befugnisse der Mitgliedstaaten,
  - gleiche Sanktionen im Falle der Verletzung der DS-GVO.

- Vorrang einer EU-Verordnung vor nationalem Recht
  - Eine EU-Verordnung hat grds. Anwendungsvorrang vor jedem nationalen Gesetz,
  - Sofern in VO vorgesehen, dann nationale Regelungen möglich.

- Ausgestaltungspflicht durch nationalen Gesetzgeber, sofern durch VO angeordnet.

MUNKER Datenschutz

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

MUNKER Datenschutz

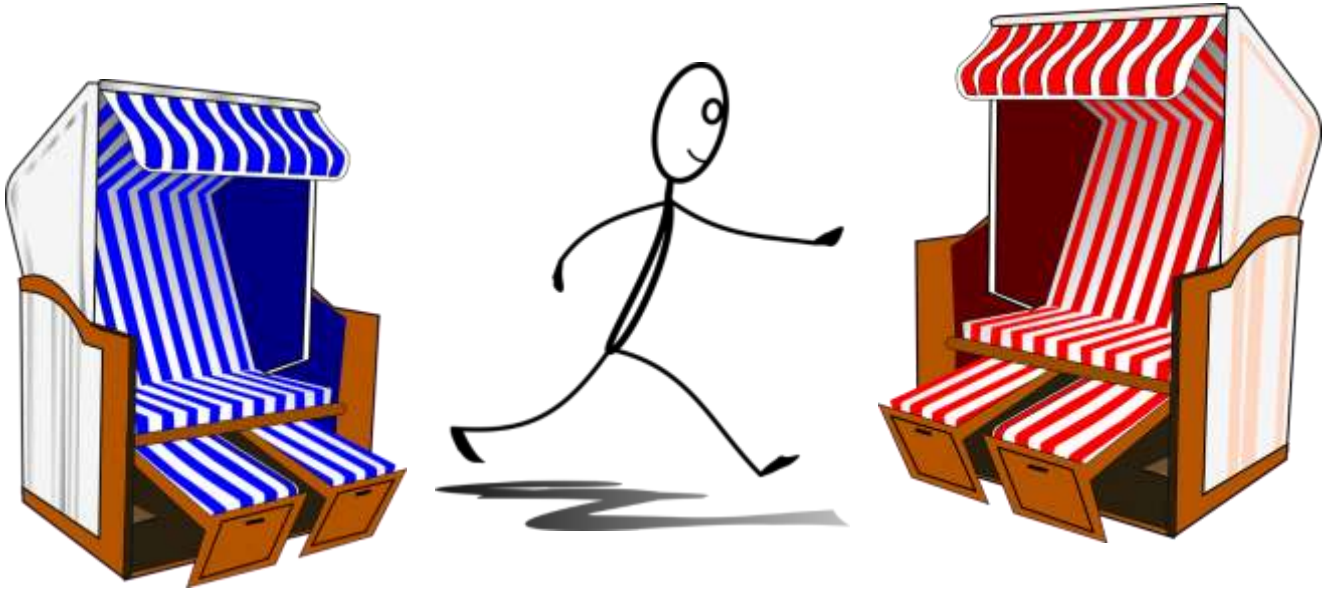
EU-Datenschutz-Grundverordnung

- wird über die Aufsichtsbehörde voraussichtlich wesentlich strenger exekutiert als das bisher der Fall war
- beinhaltet eine Meldepflicht von Datenschutzpannen (innerhalb von 72 Stunden an die Aufsichtsbehörde) und eine Beweislastumkehr
- beinhaltet eine Meldepflicht des Datenschutzbeauftragten
- setzt wesentlich mehr an Dokumentation voraus als das BDSG
- tritt am 25. Mai 2018 EU-weit in Kraft

MUNKER Datenschutz

EU-Datenschutz-Grundverordnung

- Datenschutz zwischen 2 Stühlen:



BDSG-alt bis 24.05.2018

DS-GVO, und BDSG-neu ab 25.05.2018

MUNKER Datenschutz

Grundsätze der DSGVO

Art. 5 DSGVO, Abs. 1 (Grundsätze für die Verarbeitung personenbezogener Daten):

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

MUNKER Datenschutz

Rechenschaftspflicht

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).“

MUNKER Datenschutz

Datenschutz + datenschutzfreundliche Voreinstellungen

EW 78 und Art. 25 DS-GVO: 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.

Datenminimierung hinsichtlich

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

MUNKER Datenschutz

Datenschutzfreundliche Voreinstellungen

Art. 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), Absatz 3:

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

-> Datenschutzzertifikat? ISO 27001? …?

MUNKER Datenschutz

Technische und organisatorische Maßnahmen

Art. 32 DSGVO (Sicherheit der Verarbeitung):

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“.

MUNKER Datenschutz

Technische und organisatorische Maßnahmen nach DS-GVO

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

MUNKER Datenschutz

Technische und organisatorische Maßnahmen nach DS-GVO

Artikel 32 Sicherheit der Verarbeitung

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

MUNKER Datenschutz

Technische und organisatorische Maßnahmen nach DS-GVO

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

MUNKER Datenschutz

Datenverarbeitung im Auftrag -> Auftragsverarbeitung

- 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 zu Erfüllung weiterer eigener Aufgaben oder Funktonen benötigt. Damit handelt es sich um eine Übermittlung an „Dritte“ und die Haftung gegenüber dem Dateneigentümer geht an den Funktionsnehmer über!

- Ist die herkömmliche Abgrenzung zur „Funktionsübertragung“ jetzt obsolet?

  Bei Verstoß des Auftragnehmers gegen die DS-GVO oder andere datenschutzrechtliche Regelungen -> Mithaftung!

MUNKER Datenschutz

Beispiele für Datenverarbeitung im Auftrag

- Rechenzentren, Copyshops.
- Externe Dienstleister EDV und TK mit „Remote-Zugriff“ (Server, Aktivkomponenten, Datenbanken, Wartungsverträge, Softwarepflege, Wartung TK-Anlagen etc.).
- Externe Dienstleister Peripherie IT/TK (Faxgeräte, Drucker, Multifunktionsgeräte, Scanner, Kopiergeräte, etc.).
- Entsorger (IT / TK) und Entsorger Papier.
- Internet-Service-Provider (Internet und E-Mail-Dienste).

MUNKER Datenschutz

Auftragsverarbeitung nach Art. 28 DS-GVO

- Sorgfältige Auswahl der Auftragnehmer. Hinreichende Garantien!
- Kriterien für die Auswahl der Auftragnehmer: geeignete technische und organisatorische Maßnahmen.
- Detaillierte Regelungen der Unterauftragsverhältnisse. Einsatz und Wechsel von Subunternehmen nur mit schriftlicher Genehmigung.
- Detaillierte Regelungen der Auftragsverhältnisse (schriftlich oder elektronisch).

MUNKER Datenschutz

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 der betroffenen Person .

MUNKER Datenschutz

Detaillierte Regelungen der Auftragsverhältnisse

- Unterstützung des Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten:
  - Meldung von Datenschutzpannen,
  - Benachrichtigung der Betroffenen,
  - Datenschutz-Folgenabschätzung.
- Löschung oder Rückgabe von Daten nach Beendigung.
- Unterstützung des Verantwortlichen bei Überprüfungen — einschließlich Inspektionen.
- Unverzügliche Information, falls eine Weisung des Verantwortlichen gegen die DS-GVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

MUNKER Datenschutz

Kontrolle der Auftragsverhältnisse

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

MUNKER Datenschutz

§ 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“ -> Veröffentlichung im Bundesgesetzblatt am 09.11.2017:

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

  Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen.

  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.

- **Lösung:**

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

MUNKER Datenschutz

Die Steuerkanzlei als Auftragsverarbeiter?

- Kann eine Steuerberaterkanzlei Auftragsdatenverarbeiter eines Mandanten sein?

- Hierzu gab es in der Vergangenheit unterschiedliche Auffassungen:

  Einhellige Meinung Bundessteuerberaterkammer und Bayerisches Landesamt für Datenschutzaufsicht in der „Welt BDSG-alt“:

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

- **DS-GVO und BDSG-neu -> ???**

  -> Aus unserer Sicht gibt es keinen Grund diese Auffassung zu ändern!

MUNKER Datenschutz

Zusammenfassung Auftragsverarbeitung

- Wechsel von Subunternehmer nur mit Genehmigung.
- Elektronische Form des Vertrages zur Auftragsverarbeitung möglich.
- Ergänzende Verpflichtung nach § 203 StGB beachten!
- Nachweis der Garantien: Zertifikate oder genehmigte Verhaltensregeln, ggf. auch Audits vor Ort.
- Regelmäßige (jährliche) Kontrolle der Auftragsverarbeiter.

MUNKER Datenschutz

Der Datenschutzbeauftragte

- Notwendigkeit der Bestellung nach Art. 37 DS-GVO
- 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 DS-GVO
  - Berufliche Qualifikation
  - Fachwissen
  - Fähigkeiten
- Die Kontaktdaten des DSB müssen ab 25.05.2018 an die Aufsichtsbehörde gemeldet werden!

MUNKER Datenschutz

Aufgaben des Datenschutzbeauftragten

- Unterrichtung und Beratung
  - des Verantwortlichen oder
  - des Auftragsverarbeiters und
  - der Beschäftigten,

- Überwachung der Einhaltung der DS-GVO, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten

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

- (Überwachung der) Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen

MUNKER Datenschutz

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

MUNKER Datenschutz

Wer überwacht die Einhaltung des Datenschutzes?

Der Europäische Datenschutzausschuss

18 Aufsichtsbehörden

MUNKER Datenschutz

Die EU-DSGVO und die verschärften Regelungen Auftrags(daten)verarbeitung