Datenschutz nach der EU-Datenschutz-Grundverordnung

Workshop

Agenda

Ihre Referenten

Susann Harder

- Rechtsanwältin seit 2012
- Partnerin bei ECOVIS seit 2015
- Externe Datenschutzbeauftragte

Axel Keller, LL.M.

- Rechtsanwalt seit 2003
- Partner bei ECOVIS seit 2007
- Externer Datenschutzbeauftragter

Die Workshopunterlagen und diverse weitere Informationen finden Sie auf unserer Website:

www.ecovis.com/datenschutzberater/

Entwicklung der EU-DSGVO II

Was es 1995 **gab**	**Was es 1995 nicht gab**

• Umsetzung der Datenschutzrichtlinie 95/46/EG in nationales Recht
• In Deutschland: Bundesdatenschutz-gesetz
• Eigenständige und unabhängige Datenschutzaufsichtsbehörden
• Unterschiedliche Bußgeldbestimmungen und -höhen
	• Smartphones
	  • 15. August 1996: Nokia 9000 Communicator (VK: 2.700 D-Mark)
	  • 2002: erstes Blackberry Smartphone
	  • 9. Januar 2007: Vorstellung iPhone (Absatz von 270.000 Stück am ersten Verkaufstag)
	• Google (4. September 1998 gegründet)
	• Facebook (4. Februar 2004 gegründet)
	• Tablets, Big Data

Entwicklung der EU-DSGVO II

Erneuerung erforderlich

– **Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG**

Datenschutz-Grundverordnung (EU-DSGVO)

- **Ziele**:
  - **Harmonisierung des Rechtsrahmens für den Datenschutz in Europa**
  - **Europaweite Koordination des Datenschutzes**
  - **Europaweite Koordinierung der Datenschutzaufsichtsbehörden**

→ Gilt ab dem 25. Mai 2018

Entwicklung der EU-DSGVO III

Datenschutz-Grundverordnung (EU-DSGVO)

Wird Datenschutz jetzt so richtig „sexy“?

Bringt das dem Einzelnen tatsächlich etwas?

Für wen machen wir das eigentlich – wirklich für den Kunden?

Ist das alles wirklich sinnvoll?

Zahlen Sie eigentlich gerne Steuern…?!

Entwicklung der EU-DSGVO IV

Sachlicher Anwendungsbereich

- **Ganz / teilweise automatisierte Verarbeitung personenbezogener Daten**
  - Jede Verarbeitung mittels EDV, d. h. PC, Netzwerk mit Server, Notebook, Smartphone, Tablet, Videokameras, Kopierer…

- **Nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen**
  - Digitale Sammlungen personenbezogener Daten
  - Auch analoge, manuelle Sammlungen (Akten), wenn gleichartiger innerer oder äußerer Aufbau, und Karteikarten

- **Personenbezogene Daten**
  - Alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche Person** beziehen
  - Bei juristischen Personen: Ansprechpartner als nat. Personen bedenken

- **Ausschließlich persönliche oder familiäre Tätigkeiten nicht umfasst**

Entwicklung der EU-DSGVO V

Persönlicher Anwendungsbereich - Normadressat

- **DSGVO richtet sich an:**
  - die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die
  - allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

- **Das heißt**:
  - (Einzel-) Unternehmen, gleich welcher Rechtsform
  - Verbände
  - Vereine
  - Stiftungen

- **Oder anders:**

Die DSGVO richtet sich an JEDEN, der
außerhalb des rein privaten Bereichs mit personenbezogenen Daten umgeht.

Bedeutung I

- **Stellen bei der Bundesdatenschutzbeauftragten**

  - 2014: 85
  - Anfang 2017: 111
  - Ende 2017: 160
  - eingestellt werden Juristen und IT-Fachleute

- **Zusätzlicher Personalbedarf bei den Landes-DSB**

  - Je nach Bundesland zwischen 24 und 33 Stellen
  - Stand der Bewilligung in den Haushaltsverhandlungen (2017 / 2018):
    - Berlin und Sachsen 0
    - Sachsen-Anhalt 2 / 2 (beantragt 16)
    - Schleswig-Holstein 4
    - Brandenburg 8 (beantragt 15)
    - Rheinland-Pfalz / Schleswig-Holstein 4 (beantragt 10)
    - Bayern (Landesamt für Datenschutzaufsicht) 4 (beantragt 7)
    - Bayern (Bayerischer Landesdatenschutzbeauftragter) 3 / 3

Kein Grund zur Sorge?

Bedeutung II

Stand: 27.04.2017 19:54 Uhr - Lesezeit: ca.2 Min.

MV stockt Datenschutz-Behörde auf

von Stefan Ludmann, NDR 1 Radio MV

Immer mehr zu tun für die Datenschützer: Das Land will das Personal nun aufstocken. (Archivbild)

Mecklenburg-Vorpommern verstärkt den Datenschutz. Die Behörde des Datenschutz-Beauftragten Heinz Müller [illegible] werden und fast doppelt so viel Personal be[illegible]or [illegible]. Das geht aus [illegible] Haushaltsplanungen für das kommende Jahr hervor. Verantwortlich dafür ist die Landtagsverwaltung, da der Datenschutz-Beauftragte wie der Bürgerbeauftragte dem Landtag zugeordnet ist.

Dop[illegible]

14 Stellen sollen neu geschaffen werden, zehn [illegible] vier für Angestellte. Bisher [illegible]. Die Ausgaben für das Personal verdoppeln sich

Bedeutung III

Datenschutz – bislang kein Thema?!

- **14. November 2016 – Datenschutz-Sonderprüfung**
  - abgestimmte Aktion in 10 Bundesländern
    - Bayern, **Mecklenburg-Vorpommern**, Berlin, Hamburg, Niedersachsen, NRW und Sachsen-Anhalt, Bremen, Rheinland-Pfalz, Saarland
  - Prüfung in 500 zufällig ausgewählten Unternehmen

- 25 Fragen, detaillierte Stellungnahme zur Inanspruchnahme von Dienstleistungen von Unternehmen außerhalb der EU angefordert
  - Fernwartung, Reisemanagement, CRM, Marketing, Bewerbermanagement, QM- / Compliance-Systeme, Ticketing
  - Externe Speicherlösungen (Dropbox)
  - Kollaborationsplattformen (Doodle)
  - Chat- / Messaging-Systeme (WhatsApp, Threema)
  - Videokonferenzsysteme (Skype)

Bußgeld: künftig bis 20 Mio. €

- **Hätten Sie´s gewusst?**
  - EU-U.S. Privacy Shield, binding corporate rules
  - Oder liegen Ihnen wirksame Einwilligungserklärungen aller Beteiligten vor…?

Bedeutung IV

An
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach

oder per Fax an 0981 / 53 98 1300
per E-Mail an poststelle@lda.bayern.de
(per E-Mail bitte nur als pdf-Dateianhang)

Das Petze-Formular…

EU-U.S. Privacy Shield

Formular für die Einreichung von Beschwerden

Zur Bearbeitung Ihrer Beschwerde sollten Sie dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) die folgenden Angaben zukommen lassen. Sie können dafür dieses Formular nutzen oder

II. Angaben zum Sachverhalt

1. **Welches Unternehmen hat Ihre Daten in die USA übermittelt?**
   (Bitte geben Sie, soweit bekannt, die Kontaktdaten dieses Unternehmens an):
   Klicken Sie hier, um Text einzugeben.

2. **An welches US-Unternehmen sind Ihre personenbezogenen Daten übermittelt worden?**
   (Bitte geben Sie, soweit bekannt, die Kontaktdaten diese Unternehmens an):
   Klicken Sie hier, um Text einzugeben.

Änderungen zum BDSG I

Rechtsgrundsätze der EU-DSGVO

- **Verbot mit Erlaubnisvorbehalt (Art. 6)**
  - Der Umgang mit personenbezogenen Daten ist verboten, es sei denn, ich habe eine Erlaubnis (gesetzliche Norm oder Einwilligung des Betroffenen)
- **Transparenzgebot (Art. 5 Abs. 1)**
  - Der Betroffene ist durch mich umfassend zu informieren (bspw. über Umfang und Zweck der Datenerhebung und seine Rechte).
- **Zweckbindung (Art. 5 Abs. 1)**
  - Ich darf die Daten nur zu dem Zweck verwenden, zu dem ich sie erhoben habe. (Beispiel: Darf ich Werbung an meine Kundendatei senden?)

Änderungen zum BDSG II

Rechtsgrundsätze der EU-DSGVO

- **Datensparsamkeit, Datenminimierung (Art. 25 Abs. 2)**
  - Ich darf nur diejenigen Daten erheben und behalten, die für den Zweck erforderlich sind.
- **Technische und organisatorische Maßnahmen zum Schutz der Daten (Art. 25 Abs. 1)**
  - Ich muss Maßnahmen zur Umsetzung der Datenschutzgrundsätze treffen. (Pseudonymisierung, Anonymisierung, Berechtigungs-, Zugriffs- und Zutrittskonzepte, Lese- und Zugriffsprotokollierung, Wiederanlaufplan etc.)
- **Es kommen neu hinzu:**
  - Nachweisbarkeit, „Rechenschaftspflicht“
  - Risikobewertungen, Bildung von Risikoklassen nach Art der Daten, Eintrittswahrscheinlichkeit eines Schadens und dessen Höhe („Risiko-Folgen-Abschätzung“)

BayLDA → Bayerisches Landesamt für Datenschutzaufsicht

Anforderungen an die Datenverarbeitung

Rechenschaftspflicht

Artikel 5: Grundsätze für die Vera

(1) Personenbezogene Daten müsse
a) ... auf rechtmäßige Weise ... („Rechtma ... arbeitung nach Treu und Glauben, Transparenz“)
b) ... für festgelegte, eindeutige und leg ... ecke
c) ... auf das notwendige Maß beschrä ... Daten
d) ... sachlich richtig ... („Richtigkeit“)
e) ... erforderlich ... („Speicherbegre ... ng“) [und m
f) ... angemessener Sicherheit ... („In ... grität und Ver
[verarbeitet werden.]

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

Wie prüfen wir:

Zeig mal !!

(„Beweislastumkehr“)

Thomas Kranig, Präsident des Bayerischen Landesamts für Datenschutzaufsicht, 23. März 2017

Änderungen zum BDSG III

Bußgelder I

- **LIBE-Ausschuss (Ausschuss für bürgerliche Freiheiten, Justiz und Inneres) des Europaparlaments am 11.06.2015:**

Ein Kernpunkt der Reform ist die Einführung „starker Sanktionen“ bei Datenschutzverstößen, die „wehtun sollen“.

- **Höhe**
  - bis zu € 10.000.000 oder
  - bis zu 2% des gesamten, weltweit erzielten Jahresumsatzes
  - je nachdem, welcher der Beträge höher ist

- **Bei Verstößen der Verantwortlichen und der Auftragsdatenverarbeiter gegen die Pflichten aus Art. 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43**
  - IT-Sicherheitsmanagement
  - Zusammenarbeit mit der Aufsichtsbehörde
  - Alle Vorschriften zur Auftragsdatenverarbeitung
  - Datenschutz-Folgeabschätzung (neu!)
  - Datenpannen

Änderungen zum BDSG IV

Bußgelder II

- **Höhe**
  - bis zu € 20.000.000 oder
  - bis zu 4% des gesamten, weltweit erzielten Jahresumsatzes
  - je nachdem, welcher der Beträge höher ist

- **Bei Verstößen gegen**
  - Grundsätze für die Verarbeitung, einschließlich Einwilligung
  - Rechte der betroffenen Personen
  - Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation
  - Alle Pflichten gemäß den Rechtsvorschriften der Mitgliedsstaaten, die aufgrund Öffnungsklausel erlassen wurden (bspw. Bestellung eines Datenschutzbeauftragten)
  - Nichtbefolgen einer Anweisung der Aufsichtsbehörde
  - Nichtgewährung des Zugangs für die Aufsichtsbehörde

Änderungen zum BDSG VI

Bußgelder III

→ Neue Faustregel der Aufsichtsbehörden: Faktor 66,6?

- Übermittlung personenbezogener Daten in die USA
  - Adobe (Acrobat Reader) € 8.000
  - Unilever € 11.000
  - Punica € 9.000

- Keinen Datenschutzbeauftragten bestellt / Fragen nach Krankheitsgrund
  - Drogerie Müller € 137.500

- Ankauf von Listen mit Daten und datenschutzwidrige Nutzung
  - DEBEKA € 1,3 Mio. Bußgeld zzgl. € 600.000,00 Zustiftung

- Videoüberwachung der Mitarbeiter
  - Lidl € 1,46 Mio.
    (Einzelbußgelder zwischen € 10.000 und € 310.000)

Änderungen zum BDSG VII

Informationspflichten des Verantwortlichen, §§ 12ff. DSGVO

- **Differenzierung nach Ort der Erhebung**
  - Erhebung bei dem Betroffenen
  - Erhebung bei Dritten

- **Inhalt** (unter Anderem)
  - Name und Kontaktdaten des Verantwortlichen, Kontaktdaten des Datenschutzbeauftragten, Zwecke der Datenverarbeitung, Kategorien der erhobenen Daten, Empfänger oder Kategorien von Empfängern dieser Daten, Dauer der Speicherung, ggfls. Berechtigte Interessen des Verantwortlichen für die Datenverarbeitung
  - Bestehen der Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Möglichkeit des Widerrufs der Einwilligung, Bestehen des Beschwerderechts bei der Aufsichtsbehörde)
  - Quelle, aus der die personenbezogenen Daten stammen
  - beabsichtigte Zweckänderung

Abmahnung bei unzureichender Datenschutzerklärung?!

- **Insbesondere nach § 3a UWG – Informationspflichten sind Marktverhaltensregelungen**

Maßnahmen I

I. **Sensibilisierung von Geschäftsleitung und Mitarbeitern (Schulungen etc.)**

II. **Start eines Projekts zur Einführung der DSGVO**

Datenschutzbeauftragter notwendig?

1. Bestandsaufnahme, Analyse des Ist-Zustands

   a. Ist eine DS-Dokumentation vorhanden? (Verfahrensverzeichnis, Vorabkontrollen, Datenschutzkonzept, IT-Sicherheitskonzept, Arbeits- / Prozessanweisungen)

   b. Welche Rechtsgrundlagen sind einschlägig?

   c. Datenschutzorganisation vorhanden? (technische / organisatorische Maßnahmen)

   d. Welche Dienstleister werden genutzt? Sind darunter Auftrags(daten)verarbeiter?

   e. Gibt es eine Betriebsvereinbarung mit Regelungen zum Arbeitnehmerdatenschutz?

Maßnahmen II

Der Datenschutzbeauftragte I

- **Bestellung zwingend notwendig, wenn (alternativ)**

  - **mindestens 10 Personen** im Unternehmen ständig mit automatisierter Datenverarbeitung beschäftigt sind
  - Verarbeitungen erfolgen, die eine **Datenschutzfolgenabschätzung erforderlich** machen
  - Datenverarbeitung durch **Behörde / öffentliche Stelle** (Ausnahme: Rechtsprechung) erfolgt
  - **Kerntätigkeit** in umfangreicher, regelmäßiger und **systematischer Beobachtung** von Personen besteht (Auskunfteien, Detekteien, Versicherungen)
  - **Kerntätigkeit** in umfangreicher Verarbeitung **besonderer Kategorien von Daten** besteht
    - Rassische und ethnische Herkunft, Politische Meinungen, Religiöse oder weltanschauliche Überzeugungen / **Gewerkschaftszugehörigkeit**
    - **Genetische Daten / Biometrische Daten / Gesundheitsdaten**
    - Daten zum Sexualleben / zur sexuellen Orientierung

Maßnahmen III

Der Datenschutzbeauftragte II

- **Kerntätigkeit** besteht in umfangreicher Verarbeitung **besonderer Kategorien von Daten**

  - **Genetische / Biometrische / Gesundheitsdaten**
  - Beispielsweise Krankenhäuser, (Gen-)Labors, Familienberatungsstellen, Dienstleister im biometrischen ID-Management, Anbieter von Erotikartikeln

  - **Niedergelassene Ärzte?**

    - Erwägungsgrund 91 der DSGVO

„Die Verarbeitung personenbezogener Daten sollte **nicht** als umfangreich gelten, wenn die Verarbeitung personenbezogener Daten von Patienten oder von Mandanten betrifft und durch einen **einzelnen Arzt**, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.“

  - **Alle „Mehrarzteinrichtungen“ müssen künftig zwingend einen DSB bestellen!**

Maßnahmen IV

Der Datenschutzbeauftragte III

- **Umfang der Aufgaben kann unabhängig von bestehender Pflicht die Bestellung sinnvoll machen**

- **Interner oder externer Datenschutzbeauftragter?**

  - Benennung eines internen DSB möglich, wenn geeignet und unabhängig
  - Ausgeschlossen: Inhaber, Geschäftsführer, Prokurist, Personalleiter, Leiter IT, Administratoren, Mitarbeiter EDV, Vertriebsleiter, Ehepartner

- **Vorteile des externen Datenschutzbeauftragten**

  - keine Fehlzeiten
  - kein Sonderkündigungsschutz
  - vorhandene Fachkunde und Zuverlässigkeit
  - Vertretung ist sichergestellt (4-Augen-Prinzip)
  - keine Haftungsprivilegierung („gefahrgeneigte Tätigkeit“)
  - Bestehender Versicherungsschutz

Maßnahmen V

I. **Sensibilisierung von Geschäftsleitung und Mitarbeitern (Schulungen etc.)**

II. **Start eines Projekts zur Einführung der DSGVO**

Datenschutzbeauftragter notwendig!

1. Bestandsaufnahme, Analyse des Ist-Zustands

   a. Ist eine DS-Dokumentation vorhanden? (Verfahrensverzeichnis, Vorabkontrollen, Datenschutzkonzept, IT-Sicherheitskonzept, Arbeits- / Prozessanweisungen)

   b. Welche Rechtsgrundlagen sind einschlägig?

   c. Datenschutzorganisation vorhanden? (technische / organisatorische Maßnahmen)

   d. Welche Dienstleister werden genutzt? Sind darunter Auftrags(daten)verarbeiter?

   e. Gibt es eine Betriebsvereinbarung mit Regelungen zum Arbeitnehmerdatenschutz?

Maßnahmen VI

2. Handlungsbedarf feststellen

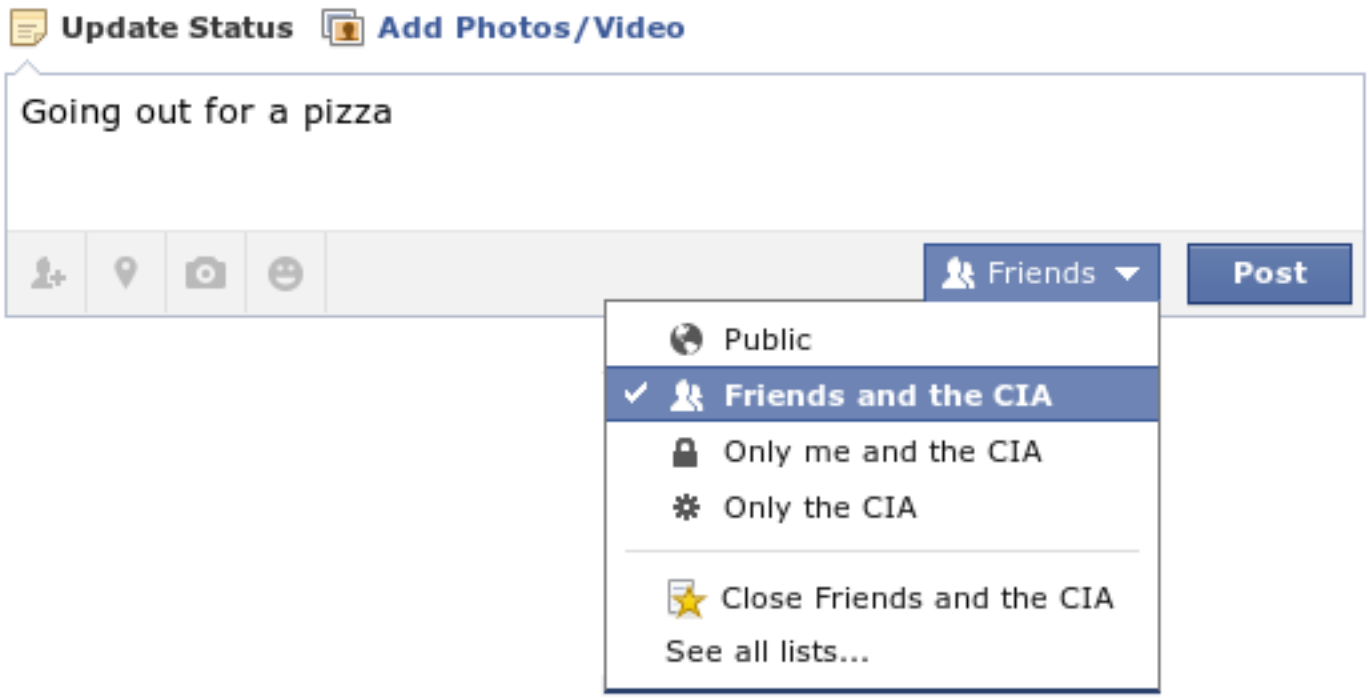
a. Rechtmäßigkeit der Datenverarbeitung nach DSGVO prüfen

b. Gesonderte Prüfung, ob zulässigerweise Minderjährigendaten verarbeitet werden

c. Prüfung aller Verträge mit Dienstleistern, die personenbezogene Daten verarbeiten

d. Prüfung jedes Datenverarbeitungsprozesses auf
- Datenschutz durch Technikgestaltung (privacy by design) und
- Datenschutz durch Voreinstellungen (privacy by default)
- Notwendigkeit einer Datenschutzfolgenabschätzung (Schwellwertanalyse)

Datenschutz durch Voreinstellungen (privacy by default)



Maßnahmen VI

2. Handlungsbedarf feststellen

a. Rechtmäßigkeit der Datenverarbeitung nach DSGVO prüfen

b. Gesonderte Prüfung, ob zulässigerweise Minderjährigendaten verarbeitet werden

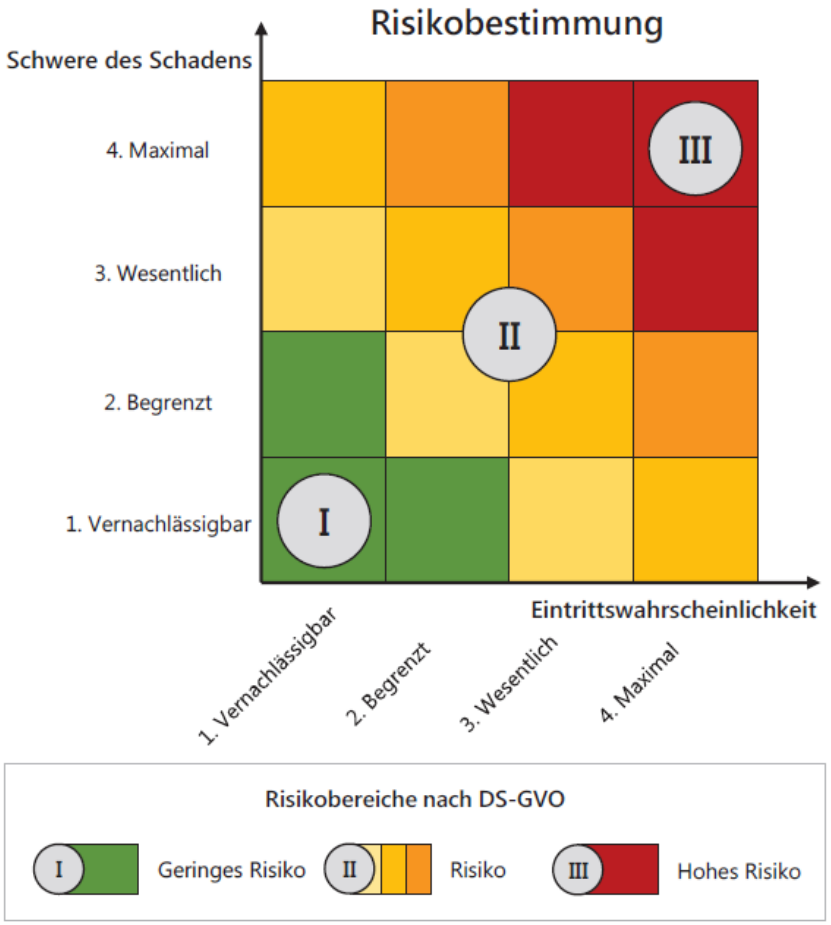
c. Prüfung aller Verträge mit Dienstleistern, die personenbezogene Daten verarbeiten

d. Prüfung jedes Datenverarbeitungsprozesses auf
- Datenschutz durch Technikgestaltung (privacy by design) und
- Datenschutz durch Voreinstellungen (privacy by default)
- Notwendigkeit einer Datenschutzfolgenabschätzung (Schwellwertanalyse)

Maßnahmen VII

- **Notwendigkeit einer Datenschutzfolgenabschätzung (Schwellwertanalyse)**

  - Eine Idee:



Maßnahmen VIII

2. Handlungsbedarf feststellen

e. Einrichtung einer Datenschutzfolgenabschätzung für betroffene DV-Prozesse (Datenschutzrisikobewertung)

f. Festlegung von Prozessen / Verfahren zur Abstimmung zwischen DSB und Aufsichtsbehörde

g. Umsetzung der Informationspflichten gegenüber den Betroffenen / Einrichtung Prozess für Reaktion auf weitere Betroffenenrechte (Berichtigung, Löschung, Auskunft)

h. Prozess zur laufenden Dokumentation aller Datenschutzmaßnahmen einschließlich der Überprüfung der Datensicherheit einrichten

Maßnahmen IX

3. **Umsetzung**

   a. **Verfahrensverzeichnis** erstellen / Datenschutz-Management-System installieren (in Art. 24 und 32 DSGVO ausdrücklich verlangt)

   b. Organisationspflicht im Sinne eines PDCA (Plan-Do-Check-Act) – Zyklus gesetzlich normiert

- **Ergänzende Praxishinweise**

  - Orientierung an Standards (VdS 10010, VdS 3473, ISO 27001/-2, DIN 66399, BSI-Grundschutz und BSI-Standards) empfehlenswert („Sorgfalt des ordentlichen Kaufmanns“)
  - QM-Team einbeziehen, wenn vorhanden
  - QM-Prozesse anpassen, ggfls. neu aufsetzen („Umgang mit Datenleck“)
  - Wirtschaftsprüfer einbeziehen, falls vorhanden (IT-Sonderprüfung; Verlässlichkeit, Validität und Vollständigkeit der Daten!)
  - (mittel- / langfristig) Datenschutzaudit / -zertifizierung erwägen
  - Informationssicherheits-Managementsystem (ISMS) notwendig?

Vielen Dank!

ECOVIS GM Rechtsanwälte PartG mbB

Am Campus 1 - 11, 18182 Rostock-Bentwisch
Tel.: +49 (0)381 649-210
eMail: dsb-nord@ecovis.com

Internet: www.ecovis.com/datenschutzberater