



# Datenschutz nach der EU-Datenschutz-Grundverordnung

18. Informationsforum für Versicherungs-, Finanzanlagen- und Immobiliendarlehensvermittler

# 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



**Den Vortrag und diverse weitere  
Informationen finden Sie auf unserer Website:**

**[www.ecovis.com/datenschutzberater/](http://www.ecovis.com/datenschutzberater/)**

# Agenda

1. Ein neues Datenschutzrecht? Musste das wirklich sein?! F. 5
2. Und was bedeutet das jetzt für mich? F. 11
3. Ändert sich denn überhaupt etwas? F. 16
4. Was muss ich denn dann jetzt machen? F. 22

# 1. Ein neues Datenschutzrecht? Musste das wirklich sein?!



# Entwicklung der EU-DSGVO

## Was es 1995 **gab**

- Umsetzung der Datenschutzrichtlinie 95/46/EG in nationales Recht
- In Deutschland: Bundesdatenschutzgesetz
- Eigenständige und unabhängige Datenschutzaufsichtsbehörden
- Unterschiedliche Bußgeldbestimmungen und -höhen

## Was es 1995 **nicht gab**

- 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

Erneuerung erforderlich !

Datenschutz-Grundverordnung (EU-DSGVO)

=

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



Ziele:

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

**Gilt ab 25. Mai 2018 !**

# Entwicklung der EU-DSGVO

## 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...?!**



# Anwendung der EU-DSGVO

## 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** (Verantwortlicher)

- (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.**

# Anwendung der EU-DSGVO

## Sachlicher Anwendungsbereich

- Personenbezogene Daten
  - Alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche Person** beziehen
  - Bei juristischen Personen – B2B-Geschäft: Ansprechpartner als nat. Personen bedenken
- **Ganz / teilweise automatisierte** Verarbeitung personenbezogener Daten
  - Jede Verarbeitung mittels EDV, d. h. PC, Netzwerk mit Server, Notebook, Smartphone, Tablet, Videokameras, Kopierer etc.
- 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
- Ausschließlich persönliche oder familiäre Tätigkeiten nicht umfasst

## 2. Und was bedeutet das jetzt für mich?



# Personalaufstockung

- **Stellen Bundes-Datenschutzbeauftragte**



- **Personalbedarf Landes-Datenschutzbeauftragte**

- Je nach Bundesland zwischen 24 und 33 Stellen
- Stand der Bewilligung in den Haushaltsverhandlungen (2017 / 2018):
  - 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

# Personalaufstockung

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)

Bürgerbeauftragte dem Landtag zugeordnet ist.

### Doppeltes Personal, doppelte Kosten


14 Stellen sollen neu geschaffen werden, zehn für Beamte und vier für Angestellte. Bisher sind dort 16 Posten besetzt. Die Ausgaben für das Personal verdoppeln sich

Mecklenburg-Vorpommern verstärkt den Datenschutz. Die Behörde des Datenschutz-Beauftragten Heinz Müller soll deutlich aufgestockt werden und fast doppelt so viel Personal bekommen bisher. Das geht aus den Haushaltsplanungen für das kommende Jahr hervor. Verantwortlich dafür ist die Landtagsverwaltung, da der Datenschutz-Beauftragte wie der

# Bedeutung

## Datenschutz – bislang kein Thema?

- 14. November 2016 – Datenschutz-Sonderprüfung
  - Aktion in 10 Bundesländern (BY, **MV**, BE, HH, NI, NRW, ST, HB, RP, SL)
  - Prüfung in 500 zufällig ausgewählten Unternehmen
- 25 Fragen, detaillierte Stellungnahme zur Inanspruchnahme von Dienstleistungen von Unternehmen außerhalb der EU
  - Fernwartung, Reisemanagement, CRM, Marketing, Bewerbermanagement, Ticketing, QM- / Compliance-Systeme
  - Externe Speicherlösungen (Dropbox)
  - Kollaborationsplattformen (Doodle)
  - Chat- / Messaging-Systeme (WhatsApp, Threema)
  - Videokonferenzsysteme (Skype)
- **Hätten Sie´s gewusst?**
  - EU-U.S. Privacy Shield, binding corporate rules
  - Oder liegen Ihnen wirksame Einwilligungserklärungen aller Beteiligten vor...?



Bußgeld:  
künftig bis  
20 Mio. €

# Beschwerdeformular

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](mailto: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

Formular für die Einreichung von Beschwerden zum EU-U.S. Privacy Shield

BayLDA

## 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 dieses Unternehmens an):  
Klicken Sie hier, um Text einzugeben.

### 3. Ändert sich denn überhaupt etwas?





# Änderungen zum BDSG

## Rechtsgrundsätze der EU-DSGVO

- **Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO)**

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 DSGVO)**

Der Betroffene ist durch mich umfassend zu informieren (bspw. über Umfang und Zweck der Datenerhebung und seine Rechte).

- **Zweckbindung (Art. 5 Abs. 1 DSGVO)**

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

## Rechtsgrundsätze der EU-DSGVO

- **Datensparsamkeit, Datenminimierung (Art. 25 Abs. 2 DSGVO)**

Ich darf nur diejenigen Daten erheben und behalten, die für den Zweck erforderlich sind.

- **Technische, organisatorische Maßnahmen zum Schutz d. Daten (Art. 25 Abs. 1 DSGVO)**

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“)

# Änderungen zum BDSG

## Rechenschaftspflicht



Bayerisches Landesamt für  
Datenschutzaufsicht



### Anforderungen an die Datenverarbeitung

#### Rechenschaftspflicht

##### Artikel 5: Grundsätze für die Verarbeitung

- (1) Personenbezogene Daten müssen:
  - a) ... auf rechtmäßige Weise ... („Rechtmäßigkeit und Glaubhaftigkeit, Transparenz“)
  - b) ... für festgelegte, eindeutige und legitime Zwecke
  - c) ... auf das notwendige Maß beschränkt
  - d) ... sachlich richtig ... („Richtigkeit“)
  - e) ... erforderlich ... („Speicherbegrenzung“)
  - f) ... angemessener Sicherheit ... („Integrität und Vertraulichkeit“)[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

## Bußgelder

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**“.*

# Änderungen zum BDSG

## Bußgelder nach Art. 83 Abs. 4a) DSGVO

- **Höhe**
  - bis zu € 10.000.000 oder
  - bis zu 2% des gesamten, weltweit erzielten Jahresumsatzes
  - je nachdem, welcher der Beträge höher ist
- **Bei Verstößen gegen**
  - die Pflichten aus Art. 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42, 43
  - IT-Sicherheitsmanagement
  - Zusammenarbeit mit der Aufsichtsbehörde
  - Alle Vorschriften zur Auftragsdatenverarbeitung
  - Datenschutz-Folgeabschätzung (neu!)
  - Datenpannen

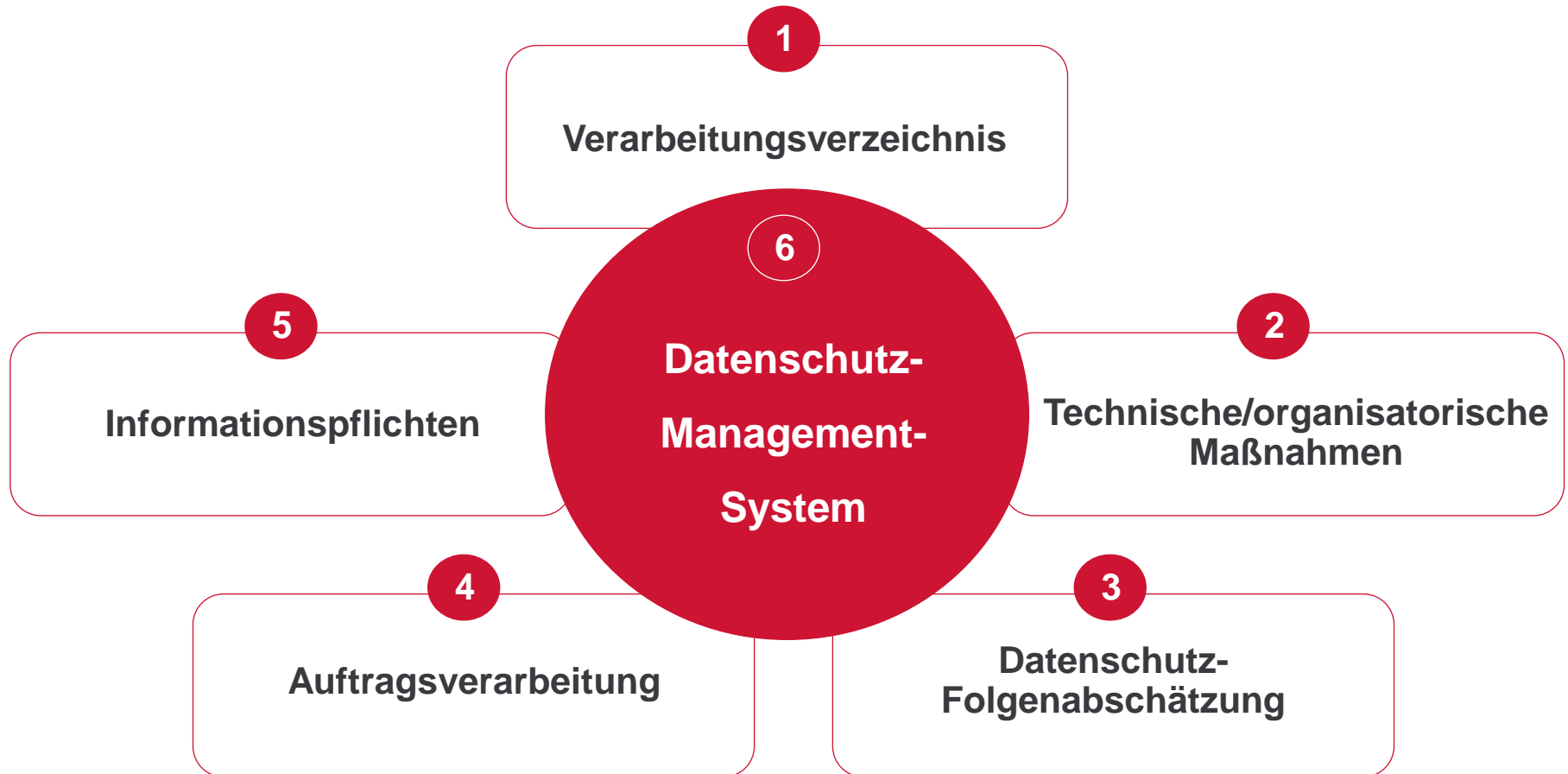
## Bußgelder nach Art. 83 Abs. 5 DSGVO

- **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 Verarbeitung, Einwilligung
  - Rechte der betroffenen Personen
  - Übermittlung personenbezogener Daten an Empfänger im Drittland/internat. Organisation
  - Alle Pflichten gem. den Rechtsvorschriften d. Mitgliedsstaaten, die aufgrund Öffnungsklausel erlassen wurden (bspw. Bestellung eines DSB)
  - Nichtbefolgen d. Anweisung d. Aufsichtsbehörde
  - Nichtgewährung des Zugangs für die Aufsichtsbehörde

## 4. Was muss ich denn dann jetzt machen?



# Datenschutz-Management-System (DSMS) mit seinen Bausteinen



# DSMS mit seinen Bausteinen

## 1. Verarbeitungsverzeichnis

- Das Verarbeitungsverzeichnis dient dem Nachweis der Einhaltung der DSGVO
- Sämtliche Verarbeitungen personenbezogener Daten werden hier dokumentiert

**Verarbeitungen** sind automatische oder nichtautomatische Verfahren bzw. Vorgänge im Zusammenhang mit personenbezogenen Daten (Erheben, Erfassen, Ordnen, Speichern, Anpassen, Verändern, Verwenden, Offenlegen, Übermitteln, Abfragen, Lösen, Verknüpfen etc.).

- Das Verzeichnis ist, auf Anfrage, der Aufsichtsbehörde zur Verfügung zu stellen (Art. 30 Abs. 4 DSGVO)

**Das Verarbeitungsverzeichnis ist künftig das zentrale Element einer ordnungsgemäßen Datenschutzdokumentation!**



# DSMS mit seinen Bausteinen

Also fast jede  
Organisation

## 1. Verarbeitungsverzeichnis

- Jeder Verantwortliche erstellt und führt ein Verzeichnis der Verarbeitungstätigkeiten, wenn (alternativ)
  - Über 250 Mitarbeiter beschäftigt werden
  - Die Verarbeitungen ein Risiko für Rechte und Freiheiten der betroffenen Personen bergen
  - **Die Verarbeitung nicht nur gelegentlich erfolgt**
  - Die Verarbeitung besonderer Datenkategorien gem. Art. 9 Abs. 1 DSGVO oder strafrechtlicher Verurteilungen gem. Art. 10 DSGVO einschließt
- Das Verzeichnis enthält nach Art. 30 Abs. 1 DSGVO mindestens folgende Angaben:
  - Namen und Kontaktdaten des Verantwortlichen und ggf. des gemeinsam mit ihm Verantwortlichen und des Datenschutzbeauftragten
  - Zwecke der Verarbeitung
  - Beschreibung der Kategorien betroffener Personen , personenbezogener Daten, Empfänger und Fristen zur Löschung dieser
  - Ggf. Übermittlungen an ein Drittland oder eine internat. Organisation
  - Allgemeine Beschreibung der techn./org. Maßnahmen gem. Art. 32 Abs. 1 DSGVO zur Pseudonymisierung, Verschlüsselung, Sicherstellung, Wiederherstellung und Prüfung der Verarbeitungen

# DSMS mit seinen Bausteinen

## 2. Technische und organisatorische Maßnahmen

- Dienen der Vorbeugung, Minimierung und Behebung von Mängeln und Risiken bei der Verarbeitung personenbezogener Daten
- Technische und organisatorische Maßnahmen nach Art. 30 Abs. 1 DSGVO:
  - Pseudonymisierung und Verschlüsselung personenbezogener Daten
  - Gewährleistung von Integrität, Vertraulichkeit, Verfügbarkeit, Belastbarkeit der Systeme und Dienste
  - Wiederherstellung der Verfügbarkeit personenbezogener Daten nach technischen oder physischen Zwischenfällen
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluation der Wirksamkeit der Maßnahmen
- Technische und organisatorische Maßnahmen müssen anhand des Art. 5 Abs. 2 DSGVO dokumentiert werden (Rechenschaftspflicht)

# DSMS mit seinen Bausteinen

## Beispiele für techn./org. Maßnahmen

### Pseudonymisierung

- Festlegung der durch Pseudonymisierung zu ersetzenden identifizierbaren Daten
- Definition der Pseudonymisierungsregel, zufällige Erzeugung der Zuordnungstabellen

### Verschlüsselung

- Schlüssel können für die Dauer des Kommunikationsvorgangs oder mittel- bis langfristig eingesetzt werden
- Festlegung zur Auswahl geeigneter kryptografischer Verfahren

### Maßnahmen zur Gewährleistung von Integrität und Vertraulichkeit der Systeme und Dienste

- Formulierung von Sicherheitsleitlinien
- Zugriffskontrolle und sicherer Umgang mit Speichermedien

### Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste

- Sicherheitskopien von Daten, Prozesszuständen, Transaktionshistorien...
- Schutz vor äußeren Einflüssen

### Wiederherstellung bei Zwischenfällen

- Notfallkonzept, -handbuch erstellen

### Überprüfung, Bewertung, Evaluierung der Wirksamkeit der Maßnahmen

- Audits, Zertifizierungen, externe Prüfungen

### Weitere Maßnahmen:

- Einschränkung der Nutzungsrechte
- Protokollierung von Zugriffen
- Transparenz- und Rechenschaftspflicht durch weitreichende Dokumentation

# DSMS mit seinen Bausteinen

## Sonderproblem: Kommunikation über unverschlüsselte E-Mail

- Schreiben der Aufsichtsbehörde Hamburg vom 08. Januar 2018

*„Die Versendung von unverschlüsselten E-Mails, die personenbezogene Daten enthalten, insbesondere für Angehörige von Berufsgruppen, die auch einer strafrechtlich sanktionierten Schweigepflicht nach § 203 StGB unterliegen, ist nach alledem nicht nur bedenklich, sondern stellt auch ein ungeeignetes Kommunikationsmittel dar.“*

*„Die Versendung von unverschlüsselten E-Mails, die personenbezogene Daten enthalten, insbesondere für Angehörige von Berufsgruppen, die auch einer strafrechtlich sanktionierten Schweigepflicht nach § 203 StGB unterliegen, ist nach alledem nicht nur bedenklich, sondern stellt auch ein ungeeignetes Kommunikationsmittel dar. [...] Daher scheidet auch die elektronische Übertragung sensibler personenbezogener Daten ohne Verschlüsselung etwa per Mail aus, auch wenn der Betroffene explizit um die Übersendung per Mail bittet.“*

# DSMS mit seinen Bausteinen

## Sonderproblem: Kommunikation über unverschlüsselte E-Mail

- Schreiben der Aufsichtsbehörde Hamburg vom 08. Januar 2018

*„Die Versendung von unverschlüsselten E-Mails, die personenbezogene Daten enthalten, insbesondere für Angehörige von Berufsgruppen, die auch einer strafrechtlich sanktionierten Schweigepflicht nach § 203 StGB unterliegen, ist nach alledem nicht nur bedenklich, sondern stellt auch ein ungeeignetes Kommunikationsmittel dar.“*

*„Die Versendung von unverschlüsselten E-Mails, die personenbezogene Daten enthalten, insbesondere für Angehörige von Berufsgruppen, die auch einer strafrechtlich sanktionierten Schweigepflicht nach § 203 StGB unterliegen, ist nach alledem nicht nur bedenklich, sondern stellt auch ein ungeeignetes Kommunikationsmittel dar. [...] Daher scheidet auch die elektronische Übertragung sensibler personenbezogener Daten ohne Verschlüsselung etwa per Mail aus, auch wenn der Betroffene explizit um die Übersendung per Mail bittet.“*

- Ob ein Kunde in die unverschlüsselte Kommunikation tatsächlich nicht einwilligen kann, ist nicht abschließend geklärt

# DSMS mit seinen Bausteinen

## Sonderproblem: Kommunikation über unverschlüsselte E-Mail

- Versicherungsvermittler unterliegen (im Bereich der Personenversicherungen KV, Unfall, LV) dem Anwendungsbereich des § 203 StGB!

**„Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als **Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung** anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.“**

- BGH (Urt. v. 10. Februar 2010):
  - „Angehöriger“ ist jede Person, die aufgrund ihrer Funktion mit Geheimnissen des Versicherungsnehmers in Berührung kommen kann. Damit sind alle in den Kreis der Geheimnisträger einbezogen, die mit der Anbahnung, Abwicklung oder Verwaltung solcher Versicherungsverträge befasst sind. Hierzu gehört **vor allem** ein selbständiger Versicherungsvertreter.

# DSMS mit seinen Bausteinen

## 3. Datenschutz-Folgenabschätzung

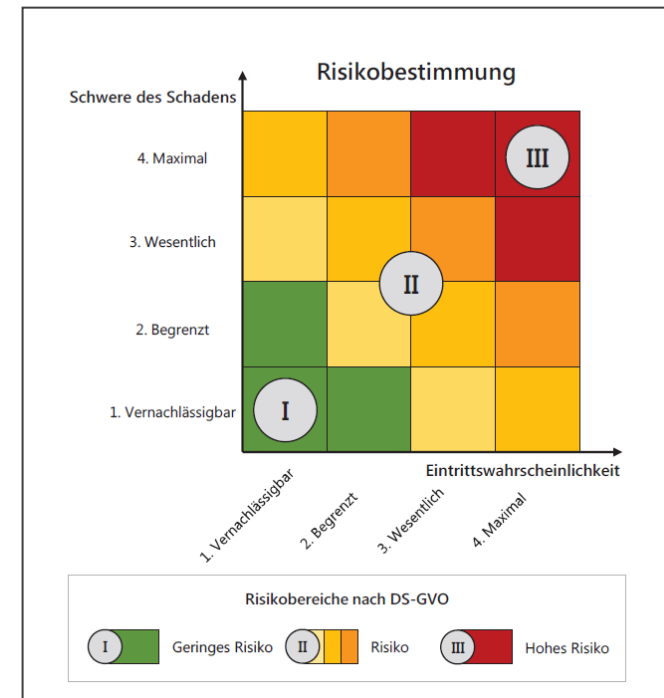
Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine **Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge** für den Schutz personenbezogener Daten durch (Art. 35 Abs. 1 DSGVO)

- Notwendigkeit einer **Datenschutz-Folgenabschätzung** bei besonders hohen Risiken nach Art. 35 Abs. 3 DSGVO:
  - Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient
  - Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 oder Art. 10 DSGVO
  - Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

# DSMS mit seinen Bausteinen

## 3. Datenschutz-Folgenabschätzung

- Eintrittswahrscheinlichkeit und Schwere des Schadens bestimmen (Schwellwertanalyse)
- Die Folgenabschätzung enthält nach Art. 35 Abs. 7 DSGVO:
  - Beschreibung der Verarbeitungsvorgänge und Zwecke der Verarbeitung
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge
  - Bewertung der Risiken für Rechte und Freiheiten der Betroffenen
  - Abhilfemaßnahmen einschließlich Garantien, Sicherheitsvorkehrungen, Verfahren zur Sicherstellung des Datenschutzes





# DSMS mit seinen Bausteinen

## 4. Auftragsverarbeitung

**Auftragsverarbeiter** sind natürliche oder juristische Personen, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

- Jeder Auftragsverarbeiter führt ein **Verzeichnis der Verarbeitungstätigkeiten**, die er im Auftrag eines Verantwortlichen übernommen hat.
- Grundlage der Zusammenarbeit von Verantwortlichen und Auftragsverarbeiter ist ein **Vertrag** mit zwingenden Inhalten:
  - Personenbezogene Daten dürfen vom Auftragsverarbeiter nur auf dokumentierte Weisung des Verantwortlichen verarbeitet werden
  - Verpflichtung der mit der Bearbeitung befassten Personen auf die Vertraulichkeit oder gesetzliche Verschwiegenheitsverpflichtung muss gewährleistet werden
  - Einsatz von Subunternehmern bedarf der Zustimmung des Auftraggebers
  - Sicherheit der Datenverarbeitung (technische und organisatorische Maßnahmen) müssen eingehalten werden
  - Löschung / Rückgabe aller Daten bei Beendigung des Auftrages (wenn keine gesetzliche Aufbewahrungspflicht besteht)

# DSMS mit seinen Bausteinen

## 5. Informationspflichten des Verantwortlichen ggü. Betroffenen (Art. 12ff. DSGVO)

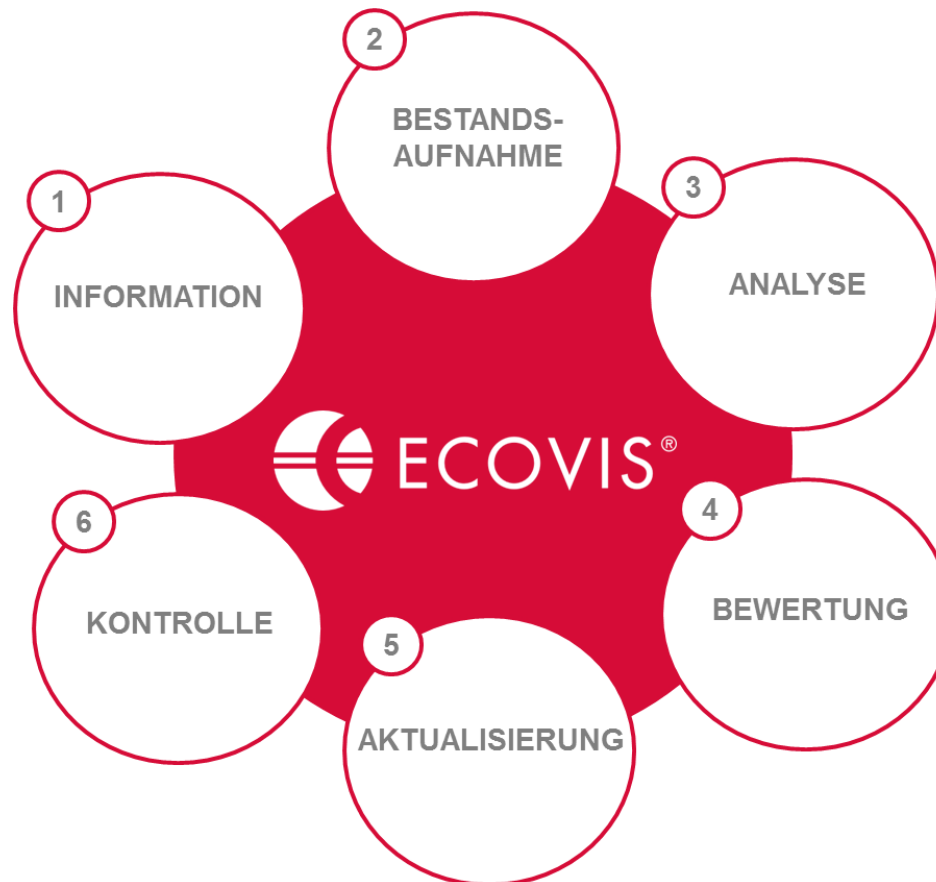
- **Differenzierung nach Ort der Erhebung**
  - Erhebung bei dem Betroffenen
  - Erhebung bei Dritten
- **Inhalt (unter Anderem)**
  - Name und Kontaktdaten des Verantwortlichen, Kontaktdaten des Datenschutzbeauftragten, Zwecke der Datenverarbeitung, Kategorien der erhobenen Daten, Empfänger oder Kategorien 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**

# DSMS mit seinen Bausteinen

## 6. Datenschutz-Management-System



# DSMS mit seinen Bausteinen

## Datenschutzbeauftragter

- **Bestellung eines DSB 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
    - Rassistische und ethnische Herkunft, Politische Meinungen, Religiöse oder weltanschauliche Überzeugungen / **Gewerkschaftszugehörigkeit**
    - **Genetische Daten / Biometrische Daten / Gesundheitsdaten**
    - Daten zum Sexualleben / zur sexuellen Orientierung

# DSMS mit seinen Bausteinen

## Datenschutzbeauftragter

- 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 sind:  
Inhaber, Geschäftsführer, Prokuristen, 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

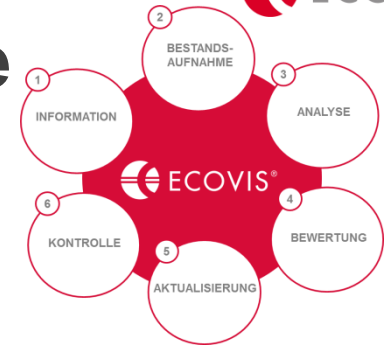
# 1. Information

## Sensibilisierung der Geschäftsführer und Mitarbeiter

- **Information der Fachabteilungen** im Unternehmen über
  - Gesetzliche Vorgaben
  - Ziele des Unternehmens bzgl. dieser Vorgaben
- **Information der Fachbereichsleiter** im Unternehmen über
  - Nähere Projektschritte
  - Beginn der Bestandsaufnahme
  - Wahl der Ansprechpartner für Datenschutzthemen
- **Informationsüberfluss vermeiden** durch
  - Vermittlung von Grundlagenwissen für alle Mitarbeiter
  - Vermittlung von spezifischem Wissen für betroffene/verantwortliche Mitarbeiter
  - Angebot verschiedener Schulungen für verschiedene Personengruppen und Fachabteilungen



## 2. Bestandsaufnahme und 3. Analyse



### IST-Zustand aufnehmen

- Ist eine **DS-Dokumentation** vorhanden?
  - Verfahrensverzeichnis
  - Vorabkontrollen
  - Datenschutzkonzept
  - IT-Sicherheitskonzept
  - Arbeits-/Prozessanweisungen
- Datenschutzorganisation vorhanden?
  - **Technische Maßnahmen**
  - **organisatorische Maßnahmen**
- Welche **Dienstleister** werden genutzt? Sind darunter Auftrags(daten)verarbeiter?
- Gibt es eine Betriebsvereinbarung mit Regelungen zum **Arbeitnehmerdatenschutz**?
- Welche **Rechtsgrundlagen** sind einschlägig?

# 4. Bewertung

## Handlungsbedarf feststellen

- **Rechtmäßigkeit der Datenverarbeitung** nach DSGVO prüfen (Bewertung der Datenschutzkonformität)
- Gesonderte Prüfung, ob zulässigerweise Minderjüngendaten verarbeitet werden
- Prüfung aller Verträge mit Dienstleistern, die personenbezogene Daten verarbeiten (**Auftragsverarbeitung**)
- Prüfung des Datenverarbeitungsprozesses auf
  - Datenschutz durch Technikgestaltung
  - Datenschutz durch Voreinstellungen
  - Notwendigkeit einer **Datenschutz-Folgenabschätzung** (Art. 35 DSGVO)





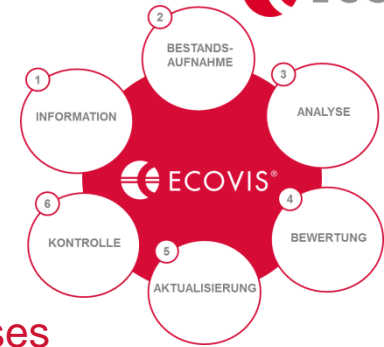
# 4. Bewertung

## Handlungsbedarf feststellen

- Einrichtung einer Datenschutzfolgenabschätzung für betroffene DV-Prozesse (**Datenschutzrisikobewertung**)
- Festlegung von Prozessen / Verfahren zur **Abstimmung** zw. DSB und Aufsichtsbehörde
- **Umsetzung der Informationspflichten** ggü. den Betroffenen / Einrichtung und Prozess für die Reaktion auf weitere Betroffenenrechte (Berichtigung, Löschung, Auskunft)
- Prozess zur laufenden **Dokumentation** aller Datenschutzmaßnahmen einschließlich der Überprüfung der Datensicherheit einrichten



# 5. Aktualisierung und 6. Kontrolle



## Umsetzung – Aktualisierung – Kontrolle

- Umsetzung anhand der Erstellung des **Verarbeitungsverzeichnisses** und der Installation des **Datenschutz-Management-Systems** (in Art. 24 und 32 DSGVO ausdrücklich verlangt)
- Regelmäßige interne und/oder externe Audits, um Mängel und Risiken langfristig auszuschließen bzw. diese kurzfristig zu beheben
- Organisationspflicht im Sinne des PCDA (Plan-Do-Check-Act) – Zyklus gesetzlich normiert
- Orientierung an Standards
  - VdS 10010 (VdS-Richtlinien zur Umsetzung der DSGVO)
  - VdS 3473 (Cyber-Security für kleine und mittlere Unternehmen)
  - ISO 27001/-2 (Informationssicherheit)
  - DIN 66399 (Datenträgervernichtung)
  - BSI-Grundschutz und BSI-Standards (Informationssicherheit)empfehlenswert („Sorgfalt des ordentlichen Kaufmanns“)

# Ergänzende Praxishinweise

- 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](http://www.ecovis.com/datenschutzberater)**

