



# Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer

Dr. Arne Schümann  
Referentin Wettbewerbsrecht

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 1



## Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer

### Gliederung

1. Datenschutz - Warum und wieso?
2. Grundlagen Datenschutz
  - Allgemein
  - Grundlagen Datenschutzgrundverordnung
3. Was ist zu tun? – Allgemein
4. Einzelne Problemstellungen
- (5. Datensicherheit)
6. Zusammenfassung

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 2

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

1. Datenschutz – Warum und Wieso?

IHK DRESDEN

Art. 1 DS-GVO „Ziele der DS-GVO“

(1) Diese Verordnung enthält Vorschriften zum **Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.**

(2) Diese Verordnung **schützt die Grundrechte und Grundfreiheiten natürlicher Personen** und insbesondere deren Recht auf Schutz personenbezogener Daten.

(3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 3

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

1. Datenschutz – Warum und Wieso?

IHK DRESDEN

Das Recht auf **informationelle Selbstbestimmung** resultiert aus Art. 1 (Menschenwürde) und Art. 2 (Freiheit zur persönlicher Entfaltung) GG

↓

- Datenschutz ist der Schutz personenbezogener Daten bei deren Erhebung, Verarbeitung und Nutzung!
- Datenschutz ist die Sicherung der Freiheit des Datenverkehrs

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 4

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

1. Datenschutz – Warum und Wieso?

IHK DRESDEN

Was sind personenbezogene Daten?

↓

Art. 4 I DS-GVO/ § 46 I BDSG-neu

„personenbezogene Daten“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 5

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

1. Datenschutz – Warum und Wieso?

IHK DRESDEN

Was sind besonders schutzbedürftige personenbezogene Daten?

↓

„Giftschrankdaten“, Art. 4 Nr. 13, 14, 15 DS-GVO/§ 46 Nr. 14 BDSG-neu sind Daten, die aus sensiblen Lebensbereichen stammen: (z.B.)

- Angaben über rassische und ethnische Herkunft
- Politische Meinungen
- Religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeiten
- Gesundheit
- Sexualleben

**Diese Daten dürfen nur aufgrund besonderer Umstände erhoben werden und müssen gesondert geschützt werden!**  
**Art. 9 DS-GVO/ § 48 BDSG-neu**

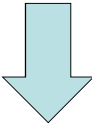
19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 6

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
 1. Datenschutz – warum und wieso

IHK DRESDEN

Warum sollte ich mich damit beschäftigen?

Der Haftungsrahmen wurde erheblich erweitert




Die Bußgelder für Verstöße gegen die Grundprinzipien wurden massiv erhöht. Die Strafe kann **bis zu 20. Mio € oder 4 % des weltweiten Jahresumsatzes** betragen!

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 7

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
 2. Grundlagen Datenschutz - Allgemein

IHK DRESDEN

Verbot mit Erlaubnisvorbehalt, Art- 6 DS-GVO



Erhebung, Nutzung oder Verarbeitung ist nur dann zulässig, wenn eine Rechtsvorschrift (DS-GVO, BDSG, andere Gesetze) das vorsieht, oder eine Einwilligung vorliegt!

AG ist verpflichtet z.B. Geburtstag und Krankenkasse wg. Sozialversicherungspflicht zu erfassen.

Onlinehändler braucht Lieferanschrift zur Erfüllung des Vertrags und will die Daten darüber hinaus für personalisierte Werbung nutzen → Einwilligung

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 8

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
 2. Grundlagen Datenschutz – Allgemein

IHK DRESDEN

Die Verpflichtung zum Datengeheimnis § 53 BDSG-neu

↓

Wer mit Datenverarbeitung beschäftigt ist, ist verpflichtet personenbezogene Daten nicht unbefugt zu erheben, zu verarbeiten oder zu nutzen.

d.h. Verpflichtung auf Datengeheimnis von Mitarbeitern  
 d.h. diese besteht auch nach Beendigung der Tätigkeit fort

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 9

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
 2. Grundlagen Datenschutz - Allgemein

IHK DRESDEN

Grundsätze der Datenverarbeitung Art. 5 DS-GVO, § 47 BDSG-neu

<b>Rechtmäßigkeit</b> Die Datenverarbeitung muss ...	auf rechtmäßige Weise in einer für den Betroffenen nachvollziehbaren Art und Weise erfolgen.
<b>Zweckbindung</b> Die Datenverarbeitung muss ...	aufgrund festgelegter, eindeutiger und rechtmäßiger Zwecke erfolgen. Keine Weiterverarbeitung.
<b>Transparenz/Rechenschaftspflicht</b>	Der Betroffene muss informiert werden und der Verarbeiter muss Rechenschaft ablegen können.
<b>Datenminimierung</b> Die Datenverarbeitung muss ...	auf das notwendige Maß beschränkt sein.

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 10

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
2. Grundlagen Datenschutz - Allgemein

IHK DRESDEN

Grundsätze der Datenverarbeitung Art. 5 DS-GVO, § 47 BDSG-neu

<b>Richtigkeit</b> Die Daten müssen ...	sachlich richtig und aktuell sein und Maßnahmen zur Löschung und Berichtigung bereitgehalten werden.
<b>Speicherbegrenzung</b>	Die Speicherung der Daten ist nur solange zulässig, wie es für den Verarbeitungszweck erforderlich ist.
<b>Integrität und Vertraulichkeit</b>	Es müssen angemessene und geeignete technische und organisatorische Datensicherungsmaßnahmen vorhanden sein.

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 11

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
2. Grundlagen Datenschutz – DS-GVO


IHK DRESDEN

**Aufbau Datenschutzgrundverordnung**

- Kap. I Allgemeine Bestimmungen Art. 1-4 (EG 1-37)
- Kap. II Grundsätze Art. 5-11 (EG 38-57)
- Kap. III Rechte der betroffenen Person Art. 12-23 (EG 58-73)
- Kap. IV Verantwortlicher und Auftragsverarbeiter Art. 24-43 (EG 74-100)
- Kap. V Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen Art. 44-50 (EG 101-116)
- Kap. VI Vorschriften für besondere Verarbeitungssituationen Art. 51-59 (EG 117-129)
- Kap. VII Rechtsbehelfe, Haftung und Sanktionen Art. 60-76 (EG 130-140)
- Kap. VIII Unabhängigkeit der Aufsichtsbehörden Art. 77-84 (EG 141-152)
- Kap. IX Zusammenarbeit und Kohärenz Art. 85-91 (EG 153-165)
- Kap. X Delegierte Rechtsakte und Durchführungsrechtsakte Art. 92-93 (EG 166-170)
- Kap. XI Schlussbestimmungen Art. 94-99 (EG 171-173)

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 12

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
2. Grundlagen Datenschutz – DS-GVO



Wann gilt DS-GVO?

Ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten und die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder werden sollen (Sachlicher Geltungsbereich Art. 2 I DS-GVO)

⇒ d.h. immer bei Umgang mit personenbezogenen Daten


Wo gilt DS-GVO?

Räumlicher Geltungsbereich erweitert (es gilt Niederlassungs- und Marktortprinzip)

⇒ d.h. auch nicht EU/EWR-Unternehmen umfasst

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 13

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
2. Grundlagen DS-GVO



**Nachweis-/Dokumentationspflicht, Art. 24 I DS-GVO**

Der **Verantwortliche setzt** unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen** um, um **sicherzustellen und den Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls **überprüft und aktualisiert**. [...]

↓

Datenschutz ist Chefsache! Eine Übertragung der Verantwortlichkeit auf den DSB ist nicht möglich!

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 14

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
2. Grundlagen – DS-GVO

IHK DRESDEN

**Privacy by Design & Default, Art. 25 DS-GVO**

Schon im Entwicklungsprozess sind durch Technisch Operative Maßnahmen (TOM) die Grundprinzipien zu beachten.

...durch Technik, Art. 25 I

- Abwägung Stand der Technik vs. Kosten
- Risiko vs. Eintrittswahrscheinlichkeit

...durch Voreinstellungen, Art. 25 II

Datenschutzfreundliche Voreinstellungen



Dokumentation und Nachweispflichten


19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 15

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
2. Grundlagen – DS-GVO

IHK DRESDEN

**Datenschutzfolgenabschätzung, Art. 35 DS-GVO**

(1) 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.[...]



d.h. dezidierte Auseinandersetzung mit dem Risiko der eigenen Datenverarbeitungsvorgänge und Dokumentation

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 16




**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
2. Grundlagen DS-GVO

IHK DRESDEN

**Joint Controllership, Art. 26 I DS-GVO**

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



Gemeinsame Haftung

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 17


**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
2. Grundlagen DS-GVO

IHK DRESDEN

**Auftragsdatenverarbeitung, Art. 28 I DS-GVO**

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

- Keinen weiteren ohne Genehmigung
- Konkrete Bestimmungen für den schriftlichen Vertrag gefordert
- Zertifizierung möglich
- Standardvertragsklauseln (bisher nur für Übermittlung in Drittländer)



Ggf. selbst Haftung als Verantwortlicher,  
mindestens Schadensersatzpflicht

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 18

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
2. Grundlagen DS-GVO

IHK DRESDEN

**Informationspflichten, Art. 12-14 DS-GVO**

Art. 12  
geeignete Maßnahmen zur Informationsvermittlung zur Verarbeitung in **präziser, transparenter, verständlicher und leicht zugänglicher** Form in einer **klaren und einfachen Sprache**

Art. 13  
enthalten detaillierte Bestimmungen, welche Informationen bei der Datenerhebung beim Betroffenen künftig gegeben werden müssen.

Art. 14  
detaillierte Informationspflichten entsprechend Art. 13, wenn die Daten nicht beim Betroffenen selbst erhoben wurden


19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 19

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
2. Grundlagen DS-GVO

IHK DRESDEN

**Betroffenenrechte, Art. 15-21, 34 DS-GVO**


- Informationsrechte, Art. 12-14, 34
- Auskunftsrecht, Art. 15
- Berichtigung, Art. 16
- **Recht auf „Vergessenwerden“, Art. 17**
- Einschränkung der Verarbeitung, Art. 18
- Mitteilungspflicht bei Berichtigung oder Löschung, Art. 19
- **Recht auf „Datenübertragbarkeit, Art. 20**
- Widerspruchsrecht, Art. 21
- Recht nicht einer ausschließlich automatischen Entscheidung unterworfen zu sein
- Recht auf Widerruf einer Einwilligung (Art. 7 Abs. 3)




**Erheblicher Anpassungsbedarf**

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 20

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
3. Was ist zu tun? - Allgemein




„Ein Datenschutzmanagement ist zur Umsetzung der DS-GVO notwendig – natürlich abhängig von der Größe des Unternehmens, der personenbezogenen Daten, die verarbeitet werden und der Menge und der Qualität der Daten. Zumindest muss aber auch in kleineren und mittleren Unternehmen ein Mindestmaß an Dokumentation vorhanden sein.“  
Annette Karstedt-Meierriecks, DIHK



Insbesondere, da **zusätzlich** eine Verbandsklage aufgrund § 2 II Nr. 11 UKlaG durch Verbraucherverbände bei Verstößen möglich ist.

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 21

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
3. Was ist zu tun? - Allgemein



**Entwicklung einer Datenschutz-Compliance  
(Organisatorische Ausgestaltung durch Geschäftsführung)**

1. Datenschutzziele ermitteln und festlegen
2. Datenschutz-Governance-Struktur schaffen (Verantwortlichkeiten festlegen und verteilen)
3. Dokumentation der Ergebnisse in einer *Datenschutzleitlinie*

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 22

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

3. Was ist zu tun? - Allgemein

IHK DRESDEN

**Was ist zu tun? – Allgemein**

- Bestandsaufnahme (Welche Prozesse, Daten habe/erhebe/speichere ich, oder übermittle ich)
- GAP-Analyse (Soll-Vergleich des Istzustandes)
- Konzepte zur wirksamen Umsetzung der Betroffenenrechte entwickeln
- Risikoanalyse
- Datenschutzmanagementsystem entwickeln (DSFA)
- Einbindung des DSB
- Schulung der MA/Sensibilisierung
- Bestehende Verträge/Vereinbarungen prüfen (AuftragsdatenV, Betriebsvereinbarungen, etc.)
- Einwilligungsmanagement
- Dokumentation

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 23

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

4. Einzelne Problemstellungen

IHK DRESDEN

**Benötige ich einen betrieblichen Datenschutzbeauftragten?**

Die gesetzliche Pflicht trifft gemäß Art. 37 DSGVO künftig ein Unternehmen:

- wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten besteht

§ 38 BDSG-neu

- behält Schwellenwert bei (10 Personen ständig mit der automatisierten Datenverarbeitung beschäftigt) bei
- Daten die einer DSFA unterliegen
- bei geschäftsmäßiger Übermittlung (auch anonymisierter) /Markt- und Meinungsforschung

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 24

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
4. Einzelne Problemstellungen

IHK DRESDEN

**Wie setze ich die Anforderungen zu Informationspflichten um?**

Überprüfung und Anpassung der Datenschutzbelehrung !

- Rechtsgrundlage angeben, wenn Art. 6 f DS-GVO auch noch die besonderen Interessen
- Bei Übermittlung in Drittland, das und wie angemessenes Schutzniveau erreicht wird (Art. 44 – 49 DS-GVO)
- Information über die Rechte Betroffener erweitern (Vergessenwerden/Übertragbarkeit)
- Recht auf Beschwerde bei Aufsichtsbehörde mit Kontakt
- Hinweis auf automatisierte Entscheidungsfindung (Art. 22 DS-GVO)
- Zweckbestimmung anpassen, ggf. konkretisiert erweitern → an Zweckbindung denken
- Bei Übertragung/Übermittlung informieren an wen und wozu
- **Widerspruchsrecht „in einer von anderen Informationen getrennten Form“ (Art. 21 IV)**

**TIPP!** Wegen unklarer Rechtsprechung:  
Bei Vorhalten von Kontaktformular gesondert auf Datenschutzbelehrung verlinken und ggf. wenn Einwilligung nötig die weiteren Voraussetzungen nach Art. 7 DS-GVO erfüllen

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 25

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
4. Einzelne Problemstellungen

IHK DRESDEN

**Wie muss eine ausreichende Einwilligung aussehen? (Art. 7 DSGVO/ § 51 BDSG-neu)?**

Gemäß Art. 7 DSGVO muss eine wirksame Einwilligung (auch weiterhin)

- auf der **freien Entscheidung** des Betroffenen beruhen → benötigt wird eine „eindeutige und bestätigende Handlung“,  
 → d.h. keine vorgekreuzten Formulare, Formulierungen beachten
- dem **Betroffenen alle nötigen Informationen** über die Datenverarbeitung bieten,
- nicht zwingend mehr schriftlich erfolgen (**Achtung: Beweiszwecke!**)
- Hinweise zum Widerspruchs- und Widerrufsrecht enthalten.

→ Beachte: **Kopplungsverbot**  
(z. B. Abhängigkeit von Vertragsabschluss)

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 26

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
4. Einzelne Problemstellungen

IHK DRESDEN

**Darf ich automatisierte Entscheidungen herbeiführen?** Art. 22 DS-GVO

- Betroffener hat Anspruch darauf, dass keine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung ergeht, die rechtliche Wirkung entfaltet, oder sie in ähnlicher Weise beeinträchtigt!
- Grundsätzlich keine automatisierten Entscheidungen
- Ausnahmen:
  - wenn Rechtsvorschriften die Entscheidung für zulässig erklären und für ausreichende Interessenabwägung sorgen
  - wenn die Entscheidung für den Abschluss eines Vertrages *erforderlich* ist
  - wenn eine ausdrückliche Einwilligung vorliegt
- Der Verantwortliche muss bei den beiden letzten dafür sorgen, dass ausreichende Interessenwahrung stattfindet (mindestens: Recht auf Einwirkung durch eine Person, Recht auf Darlegung des eigenen Standpunktes und Recht auf Anfechtung der Entscheidung)

↓

**weiterhin möglich, aber nicht bei Kindern!**

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 27

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
4. Einzelne Problemstellungen

IHK DRESDEN

**Was ist eine Datenschutzfolgenabschätzung (DSFA) und wann muss sie durchgeführt werden?**

Art. 32 DS-GVO fordert vom Verantwortlichen eine Risikoabwägung, die die Folgen einer geplanten Datenverarbeitung ermitteln soll.

- nötig, wenn ein hohes oder sehr hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht
- das Risiko ist durch angemessene technische und organisatorische Maßnahmen zu reduzieren
- Dabei ist zu berücksichtigen:
  - Stand der Technik,
  - Implementierungskosten und
  - Art, Umfang, Umstände
  - Zweck der Verarbeitung,
  - Eintrittswahrscheinlichkeit und
  - Schwere des Risikos

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 28

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

4. Einzelne Problemstellungen

**Wie führe ich eine DSFA durch?**

1. Welche Datenverarbeitungsverfahren führe ich wozu durch → systematische Beschreibung → Notwendigkeit und Verhältnismäßigkeit der Verarbeitung
2. Risikobestimmung und -bewertung → (sog. Schwellenwertanalyse) [ISO/CNIL]
  - Schutzbedarfsfeststellung → habe ich Daten, die besonderen Schutzes bedürfen?
  - Schadensgröße → wäre eine Datenmissbrauch von geringer, mittlerer oder schwerer Auswirkung? Wirtschaftlicher/gesellschaftlicher Ruin?
  - Einordnung in Risikoskala
4. Risikominimierung → technische/organisatorische Maßnahmen
5. Dokumentation

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 29

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

4. Einzelne Problemstellungen

**Wie führe ich eine DSFA durch?**

Lt. Art. 29 Gruppe immer durchzuführen, wenn die folgenden Maßnahmen durchgeführt werden:

- Scoring und Auswertung, automatisierte Entscheidungen
- Systematische Beobachtung
- Sensible Daten, schutzbedürftige Personen betroffen
- Datenverarbeitung im großen Umfang, Datenabgleich
- wenn Dienstleistung nur mit vorheriger Datenverarbeitung in Anspruch genommen werden kann

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 30

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

4. Einzelne Problemstellungen

IHK DRESDEN

**Was muss ich bei der Auftragsdatenverarbeitung beachten?**

1. Unterscheidung Auftragsverarbeiter oder Joint Controller?
2. Sorgfältige Auswahl des Auftragsverarbeiters! → Garantien für Rechtskonformität und Wahrung der Rechte der Betroffenen
3. Mind. Regelungen nach Art. 28 III DS-GVO vertraglich fixieren
4. Weisungen an den Auftragsverarbeiter dokumentieren
5. Unterauftragnehmer ausschließen, mind. gesonderte Genehmigung [allgemeine Genehmigung] fordern → Vertragsklauseln bzw. AGB beachten, wenn Unterauftragnehmer, dann Auftragsverarbeiter dazu verpflichten, die gleichen Datenschutzverpflichtungen aufzulegen

↓

Auch bestehende Verträge sollten angepasst werden! DS-GVO gilt grundsätzlich für die ab dem 25.5.2018 durchgeführten Datenverarbeitungsprozesse!

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 31

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

4. Einzelne Problemstellungen

IHK DRESDEN

**Darf ich Daten ins Ausland übermitteln?**

Ja, aber:  
zu beachten sind Art. 44 ff. DS-GVO → „adäquates Schutzniveau“

Nur dann zulässig, wenn

- ein Angemessenheitsbeschluss der Kommission vorliegt (Art. 44)  
(bisher: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, [US – Privacy-Shield, Beschluss 01.08.2016])
- das Unternehmen geeignete Garantien bietet, einschließlich verbindlicher interner Datenschutzvorschriften (z.B. Zertifizierung möglich, Art. 45,46)
- oder eine Ausnahme greift (Art. 49)
  - Einwilligung
  - Zur Erfüllung eines Vertrages erforderlich
  - Öffentliches Interesse
  - Geltendmachung, Ausübung, Verteidigung von Rechtsansprüchen
  - Lebenswichtige Interessen
  - Öffentliches Register

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 32



**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
4. Einzelne Problemstellungen

IHK DRESDEN

**Was ist mit der Verwendung von Cookies?**

1. DS-GVO enthält keine Bestimmung zu Cookies → Cookie-Richtlinie nicht umgesetzt → bisher nach dt. Rechtsprechung ausreichend, für Erstellung von Nutzungsprofilen bei Verwendung von Pseudonymen zu Zwecken der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien → bisher Banner, ok, und Hinweis auf Widerspruch in der Datenschutzbelehrung (Opt-Out) → Rechtsprechung EuGH 2018?
2. DS-GVO gilt grundsätzlich, d.h. Datenerhebung nur mit Einwilligung oder ggf. Art. 6 f DS-GVO „berechtigte Interessen“  
**Abwägung!** → **zulässig wohl Steigerung Benutzerfreundlichkeit** (EU-Privacy-Verordnung abzuwarten → Browsereinstellungen)

Datenschutzbelehrung überprüfen und anpassen (wer erhebt, speichert und nutzt, aus welchem Grund und Widerrufsrecht hat, s.o.) vor Einwilligung.  
Ggf. Banner mit ok zum anklicken, mit zwingender Kenntnisnahme der Datenschutzbelehrung, Kästchen nicht vorgehakt

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 33

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
4. Einzelne Problemstellungen

IHK DRESDEN

**Was ist ein Verzeichnisse und benötige ich das?  
(Art. 30 DS-GVO/ § 70 BDSG-neu)**

Verantwortlicher und Auftragsverarbeiter sind verpflichtet ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in ihre Zuständigkeit fallen.  
Ausnahme Art. 30 VI:  
→ gilt nicht für Unternehmen, die **weniger als 250 Mitarbeiter** beschäftigen,  
- sofern die Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen beinhaltet  
- die Verarbeitung nicht nur gelegentlich erfolgt  
- oder nicht die Verarbeitung sensibler Daten

Inhalt:  
Namen und Kontaktdaten, Zwecke der Verarbeitung, Kategorien von Empfängern bei Offenlegung, Kategorien betroffener Personen und personenbezogener Daten, Verwendung von Profiling, Kategorien von Übermittlungen an Drittstaat, internationale Organisation, Rechtsgrundlage, Löschrufen bzw. Überprüfungsfristen, Allgemeine Beschreibung TOMs

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 34

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

4. Einzelne Problemstellungen

IHK DRESDEN

**Welche Meldepflichten nach DS-GVO bestehen wann?**

1. Meldepflicht bei der Aufsichtsbehörde, wenn eine Verletzung des Schutzes personenbezogener Daten (Art. 33 I DS-GVO/ § 65 BDSG-neu)
  - es sei denn kein Risiko für Rechte und Freiheiten von natürlichen Personen (DSFA-Nachweis)
  - Frist unverzüglich mindestens binnen 72 Stunden nach Bekanntwerden (Nachmeldung möglich), Dokumentation der Verletzung
  - Inhalt:
    - Was (Art der Verletzung),
    - Wer (Kategorien und ungefähre Anzahl der betroffenen Personen bzw. Datensätzen)
    - Wozu (wahrscheinliche Folgen)
    - Wie vorgehen (ergriffene/vorgeschlagene Maßnahmen zur Behebung der Verletzung, ggf. Maßnahmen zur Abmilderung)
2. Meldepflicht gegenüber betroffener Person, wenn hohes Risiko für dessen Rechte und Freiheiten, unverzüglich (Art. 34 DS-GVO/§ 66 BDSG-neu)

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 35

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

4. Einzelne Problemstellungen

IHK DRESDEN

**Was sind die konkreten Konsequenzen für einen Verstoß?**

Bis 10 Mio. EUR / 2% d. weltweiten Jahresumsatz nach Art. 83 Abs. 4 DSGVO



- Einwilligung von Kindern (Art. 8 DSGVO)
- ADV (Art. 29 DSGVO)
- Unzureichende Dokumentation (Art. 30 DSGVO)
- Zusammenarbeit mit der Aufsichtsbehörde (Art. 31 DSGVO)
- neu: Unzureichende Technisch Organisatorische Maßnahmen
- Meldung von Datenschutzverstößen an Aufsicht + betroffene Personen (Art. 33,34 DSGVO)
- Nicht durchgeführte Datenschutz-Folgenabschätzung bzw. Konsultation der Aufsicht (Art. 35, 36 DSGVO)
- Benennung, Stellung und Aufgaben des DSB (Art. 37, 38, 39 DSGVO)
- Pflichten der Überwachungs- und Zertifizierungsstellen (Art. 41,42,43 DSGVO)

Bis 20 Mio. / 4% d. weltweiten Jahresumsatzes

- Verstöße gegen Grundsätze nach Art. 5 DSGVO
- Verstoß gegen Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO)
- Verarbeitung ohne Einwilligung (Art. 7 DSGVO)
- Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO)
- Verstöße bei Beachtung der Rechte betroffener Personen (Art. 12-22 DSGVO)
- Verstöße bei Drittlandsübermittlungen (Art. 44-49 DSGVO)

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 36

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
5. Datensicherheit [Exkurs]

Sicherheit der Verarbeitung – muss durch den Verantwortlichen gewährleistet werden  
Art. 32 DS-GVO

Unter Berücksichtigung

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände und Zwecke der Verarbeitung
- Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Beispiele für derartige Maßnahmen:

- Pseudonymisierung und Verschlüsselung
- Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste
  - Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Notfall schnell wiederherzustellen
  - Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (z.B. Penetrationstests)

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 37

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**  
5. Datensicherheit [Exkurs]





Anforderungen nach § 64 BDSG-neu

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übertragungskontrolle
- Eingabekontrolle
- Wiederherstellbarkeit
- Zuverlässigkeit
- Datenintegrität
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennbarkeit

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 38

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

**5. Datensicherheit [Exkurs- Einfache Ansätze, Quelle: Dataarea GmbH]**



Sicherheit durch:

- „clean desk policy“
- Lösungsfristen und ordnungsgemäße Entsorgung
- Keine Datenerhebung ohne Grund, keine Herausgabe
- Sichere Passwörter/Passwortrhythmen
- Computer ausschalten/ Ruheposition

Datenminimierung durch

- Einschränkung Personenkreis,
- Einschränkung der Erhebung → nur vom Zweck umfasste Daten
- Automatische Sperr- und Löschroutinen


Verfügbarkeit sichern durch

- Sicherheitskopien (Löschrhythmen nicht vergessen)
- Äußere Einflüsse vermeiden, bzw. eindämmen (Schadsoftware, Hochwasser/Feuer/Blitz)
- Hard-/Software aktualisieren
- Reparaturstrategien
- Vertretungsregelungen schaffen

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 39

**Die Datenschutzgrundverordnung und ihre Folgen für Unternehmer**

**6. Zusammenfassung**



1. Die Datenschutzgrundverordnung geht jeden an und muss bis zum 25.5.2018 umgesetzt werden!
2. Die Umsetzung ist **kein Hexenwerk!**
3. strukturiertes Vorgehen:
  - Bestandsaufnahme der Datenverarbeitungsvorgänge, Handlungsbedarf feststellen
  - Sensibilisierung
  - Verträge checken
  - Entwickeln von Sicherungssystemen (teilweise einfachster Art, teilweise mit IT-seitiger Unterstützung)
  - Anpassung der Datenschutzbelehrung an die eigene Situation und das eigene entwickelte System zur Durchsetzung der Betroffenenrechte
4. Dokumentation

19.02.2018 GB HDV/Referat Recht, Dr. Arne Schümann 40

**Die Datenschutzgrundverordnung und ihre Folgen  
für Unternehmer**  
6. Zusammenfassung



Dr. Arne Schümann  
Referentin Wettbewerbsrecht

IHK Dresden  
Geschäftsbereich Handel / Dienstleistungen / Verkehr  
Referat Recht  
Telefon:0351 2802-194  
Fax:0351 2802-7194  
E-Mail: [schumann.arne@dresden.ihk.de](mailto:schumann.arne@dresden.ihk.de)