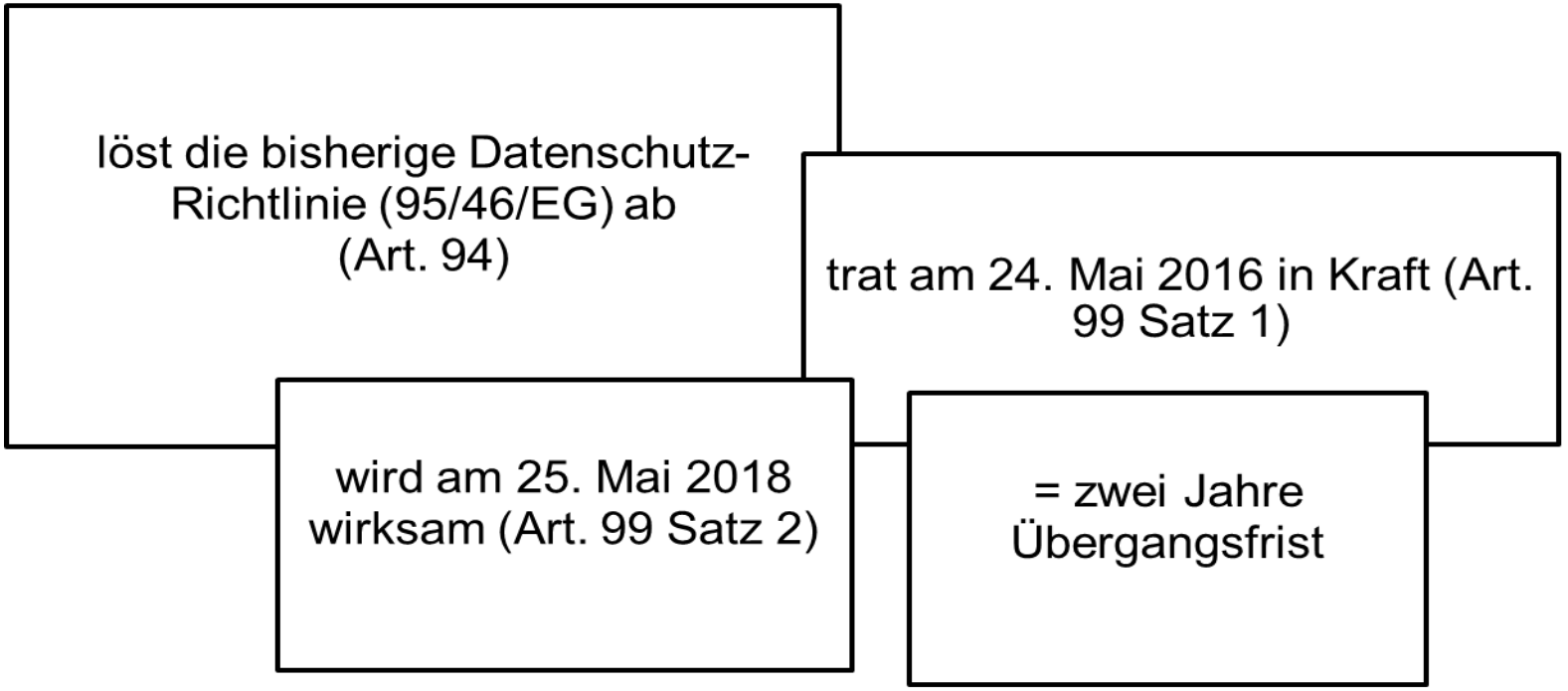
# DATENSCHUTZ 2018
# - NEUE REGELUNGEN -

Wirtschaft. Mach es in Brandenburg. IHK Potsdam

# ALLGEMEINE GRUNDLAGEN

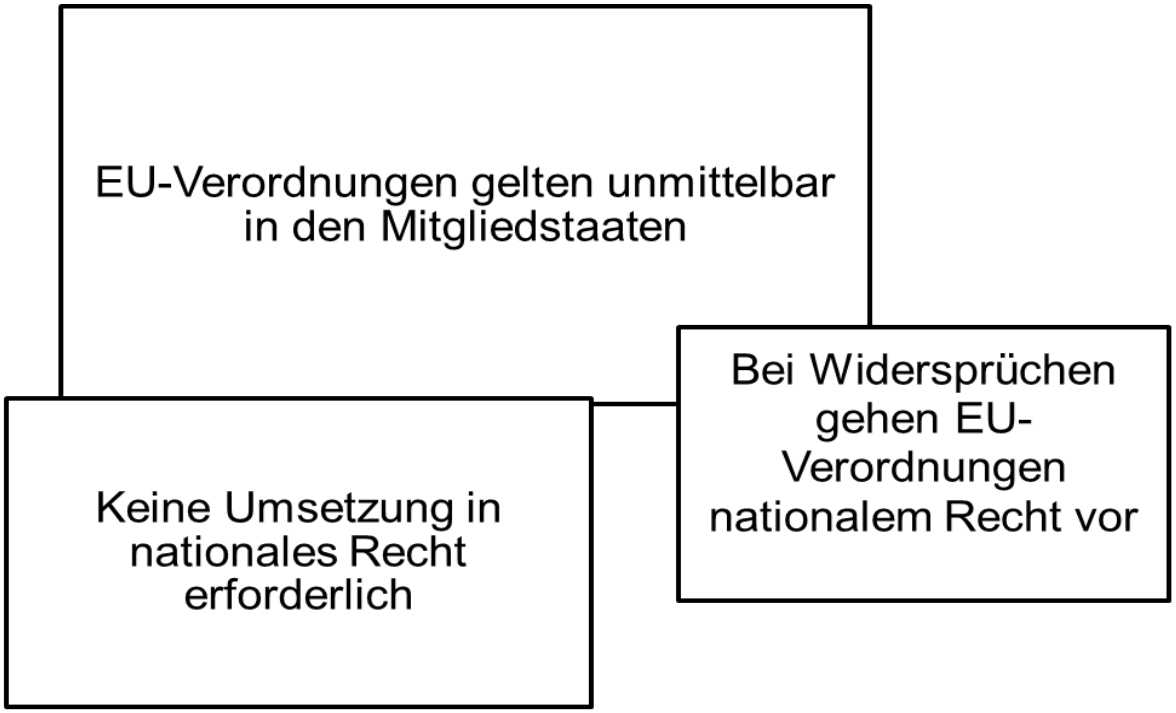
## Die DS-GVO …



# ALLGEMEINE GRUNDLAGEN

## Die DS-GVO – Rechtswirkungen ...

**BDSG**
**LDSG**



# ALLGEMEINE GRUNDLAGEN

## Die DS-GVO – Rechtswirkungen, aber …

DS-GVO enthält zahlreiche Öffnungsklauseln für die nationalen Gesetzgeber

- in einigen Bereichen verpflichtend (z. B. Art. 51 – Festlegung der Aufsichtsbehörde)
- in einigen Bereichen optional (z. B.: Art. 88 – Beschäftigtendatenschutz)

Konkretisierung und Umsetzung durch

- BDSG-neu (für Behörden und andere öffentliche Stellen des Bundes und für Unternehmen)
- BbgDSG-neu (für öffentliche Stellen des Landes Brandenburg)
- Anpassung spezialgesetzlicher Bestimmungen auf Bundes- und Landes-ebene (z. B. Sozialrecht, Polizei- und Sicherheitsgesetze, Steuerrecht usw.)

# ALLGEMEINE GRUNDLAGEN

## Problem: Auslegung der DS-GVO

Keine gefestigte Interpretations- bzw. Auslegungshilfen:

- EuGH-Rechtsprechung bezieht sich auf Richtlinie 95/46/EG
- Stellungnahmen/Orientierungshilfen des Europäischen Datenschutzausschusses müssen erst noch formuliert werden
- Kommentierungen aus der Literatur existieren noch nicht

- Unternehmen werden sich anfangs einer großen Rechtsunsicherheit bei der Auslegung der EU-DS-GVO stellen müssen.

# ALLGEMEINE GRUNDLAGEN

## Hilfsmittel zur Auslegung der DS-GVO

Erwägungsgründe zur DS-GVO

Englische Originalversion

Guidelines der Artikel 29 Datenschutzgruppe der Europäischen Kommission

ab 25. Mai 2018 des Europäischen Datenschutzausschusses

(Art. 68 ff. DS-GVO)

# ALLGEMEINE GRUNDLAGEN

## Hilfsmittel zur Auslegung der DS-GVO

Kurzpapiere (Auslegungshinweise der deutschen Datenschutzaufsichts-behörden für die Praxis) –

http://www.lda.brandenburg.de/sixcms/detail.php/bb1.c.523474.de

- Kurzpapier Nr. 3: Verarbeitung personenbezogener Daten für Werbung
- Kurzpapier Nr. 4: Datenübermittlung an Drittländer
- Kurzpapier Nr. 6: Auskunftsrecht der betroffenen Personen
- Kurzpapier Nr. 8: Maßnahmenplan für Unternehmen
- Kurzpapier Nr. 10: Informationspflichten bei Dritt- und Direkterhebung
- Kurzpapier Nr. 11: Recht auf Löschung/„Recht auf Vergessenwerden“

# WAS BEDEUTET DATENSCHUTZ?

Der Begriff ist irreführend!

Es geht nicht um den Schutz der Daten!

**Schutz des Betroffenen**

vor der missbräuchlichen Verwendung der
über seine Person gespeicherten Daten

# HIGHLIGHTS DER DS-GVO

1. Ausweitung des Anwendungsbereiches
   - alle Verarbeitungen, die sich an EU-Bürger richten (Aufenthalt in der EU ist ausreichend)

2. Neue Begriffsdefinitionen
   - Umfassender Verarbeitungsbegriff - Aufhebung Dreiklang
   - Auftragsverarbeiter
   - Einwilligung
   - besondere Arten von Daten (biometrische Daten u. genetische Daten)

3. Verarbeitung zu anderen Zwecken als den ursprünglichen Erhebungszwecken
   - Grundsatz der Zweckbindung bleibt erhalten
   - aber: nur, wenn „mit ursprünglichem Zweck vereinbar“

# HIGHLIGHTS DER DS-GVO

4. Einwilligung und Widerruf
   - Anforderungen an informierte, freiwillige Einwilligung erhöht
   - Anforderungen an Widerruf für Betroffenen herabgesetzt
   - Widerrufsrecht erweitert
   - Kopplungsverbot verschärft
   - Informations- und Auskunftspflichten erweitert
   - Datenportabilität
   - Löschpflicht erweitert

5. Auftragsverhältnis
   - Auftragsverarbeiter wird stärker in die Pflicht genommen
   - Dokumentation der Verarbeitungstätigkeiten

6. Datenschutzfolgenabschätzung
   - für besonders risikobehaftete DV
   - aber: Pflicht zur Meldung der Verfahren bei der Aufsichtsbehörde entfällt

# HIGHLIGHTS DER DS-GVO

7. Meldepflicht bei Datenpannen
   - Jeder Vorfall, der ein „Risiko“ für den Betroffenen darstellt
   - Innerhalb von 72 h
   - Auch der Betroffene muss informiert werden

8. Rechenschaftspflicht
   - Datenschutzmanagement notwendig
   - abhängig von der Größe des Unternehmens
   - aber: auch in kleineren und mittleren Unternehmen Mindestmaß an Dokumentation
   - empfindliche Bußgelder

# PRINZIPIEN DER DATENVERARBEITUNG

Verbotsprinzip mit Erlaubnisvorbehalt

Erwägungsgrund 40:

Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden, […]

# PRINZIPIEN ZUR DATENVERARBEITUNG – ART. 5 DS-GVO

| | |
|---|---|
| Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz | • Verarbeitung auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für den Betroffenen nachvollziehbaren Weise |
| Zweckbindung | • Erhebung nur für festgelegte, eindeutige und rechtmäßige Zwecke und Verbot der Weiterverarbeitung in einer mit diesen Zwecken nicht zu vereinbarenden Weise |
| Datenminimierung | • Beschränkung auf das für den Zweck der Verarbeitung angemessene und sachlich relevante sowie notwendige Maß |
| Richtigkeit | • Sachlich richtige und aktuelle Daten, Maßnahmen zur unverzüglichen Löschung oder Berichtigung |
| Speicherbegrenzung | • Speicherung mit Personenbezug nur so lange, wie es für die Verarbeitungszwecke erforderlich ist |
| Integrität und Vertraulichkeit | • Geeignete TOM zum angemessenen Schutz der Daten, insb. Vor unbefugter oder unrechtmäßiger Verarbeitung, zufälligem Verlust, ... |

# PERSONENBEZOGENE DATEN

Schutzgegenstand: personenbezogene Daten

personenbezogene Daten = alle Informationen, die sich auf eine identifizierte oder identifizierbare natürlichen Person beziehen

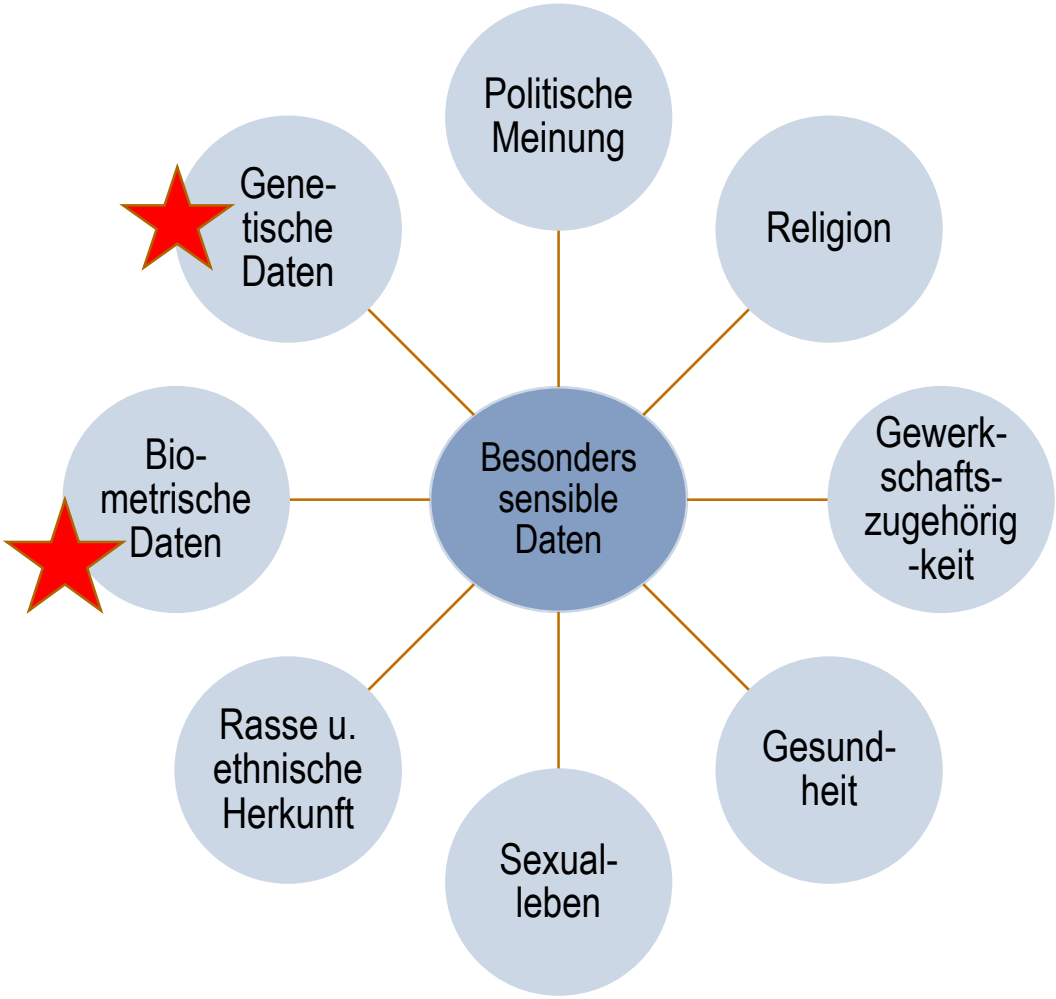
Sie sind in jeder Erscheinungsform geschützt:
d.h. auch die – ohne Computer – erhobenen Daten oder die auf Papier geschriebenen Daten (also z. B. auch Akten) stellen eine geschützte Datenerhebung dar

# PERSONENBEZOGENE DATEN

| Persönliche Verhältnisse | | Sachliche Verhältnisse |
|---|---|---|
| Name,<br>Anschrift,<br>Familienstand,<br>Geburtsdatum,<br>Staatsangehörigkeit,<br>Beruf,<br>Konfession,<br>Krankheiten u.a. |  | Einkommen,<br>Eigentumsverhältnisse,<br>Kfz-Kennzeichen,<br>Steuern,<br>Versicherungen,<br>… |

**Einzelangaben:** Name, Ausweisnummer, Telefon, E-Mail-Adresse

# PERSONENBEZOGENE DATEN



# ALLGEMEINE GRUNDLAGEN

Erlaubnistatbestände (Art. 6)

grundsätzlich jegliche Verarbeitung personenbezogener Daten verboten, es sein denn, es liegt mind. einer der nachfolgenden Erlaubnistatbestände vor:

- Einwilligung des Betroffenen (Art. 7)
- Vertragsverhältnis mit Betroffenem
- Rechtliche Verpflichtung des Verantwortlichen
- Schutz lebenswichtiger Interessen des Betroffenen / eines Anderen
- Wahrnehmung einer Aufgabe im öffentlichen Interesse / Ausübung öffentlicher Gewalt
- Berechtigtes Interesse des Verantwortlichen oder eines Dritten

# DS-GVO GESETZLICHE ERLAUBNISTATBESTÄNDE

Art. 6 Abs. 1 lit b) Vertrag

Die Verarbeitung ist zur Erfüllung eines Vertrages mit der betroffenen Person oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Anfrage der betroffenen Personen erfolgen, erforderlich.

Zur Erfüllung des Vertrages erforderlich: Name, Anschrift, Telefon-Nr.

In der Regel nicht erforderlich: E-Mail-Adresse, Geburtsdatum, Kaufinteressen, Teilnahmeinteressen, Kontodaten, Fotos, …

# DS-GVO GESETZLICHE ERLAUBNISTATBESTÄNDE

Art. 6 Abs. 1 lit c) rechtliche Verpflichtung

Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung, der der Verarbeitende unterliegt, erforderlich.

Beispiel: Erhebung der Religionszugehörigkeit im Beschäftigungsverhältnis wegen der Kirchensteuer

# DS-GVO GESETZLICHE ERLAUBNISTATBESTÄNDE

Art. 6 Abs. 1 lit f) berechtigtes Interesse

Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, und die Interessen der betroffenen Person überwiegen die Interessen nicht, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

# DS-GVO BERECHTIGTES INTERESSE

Art. 6 Abs. 1 lit f) berechtigtes Interesse

- Grundsätzlich jedes von der Rechtsordnung gebilligte wirtschaftliche oder ideelle Interesse.
- Dieses ist mit den Interessen der betroffenen Personen abzuwägen.

  Maßstab: vernünftige Erwartungen der betroffenen Personen.

# DS-GVO BERECHTIGTES INTERESSE

Beispiele berechtigten Interesses

- Erwägungsgrund 47:

  Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht. Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.

- Werbung (wenn maßgebliche und angemessene Beziehung)?
- Geschäftsübergabe / Unternehmensnachfolge?
- Bonitätsabfragen?

# DS-GVO ZWECKÄNDERUNG

Art. 6 Abs. 4 DS- GVO Zweckänderung

- Daten dürfen mit einer anderen Zweckbestimmung verarbeitet werden, wenn dieser geänderte Zweck mit dem ursprünglichen Zweck der Erhebung vereinbar ist.

- Maßstab für die Beurteilung ist wiederum die vernünftige Erwartung der betroffenen Person.

- Prüfung genau dokumentieren
  - Jede Verbindung zwischen den Zwecken
  - Zusammenhang der Erhebung
  - Art der personenbezogenen Daten (besonders sensible Daten?)
  - Mögliche Folgen der Weiterverarbeitung für betroffene Person

# DS-GVO GESETZLICHE ERLAUBNISTATBESTÄNDE

Art. 6 Abs. 1 lit. a) Einwilligung

Einwilligung = *Jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.*

# DS-GVO EINWILLIGUNG

## Einwilligung - Informiertheit und Eindeutigkeit

- Informiertheit erfordert, dass mindestens Angaben zu dem Verantwortlichen sowie zu den verfolgten Zwecken erfolgen. Blankoeinwilligungen genügen nicht
- Eindeutigkeit: Einverständnis in die DV muss klar zum Ausdruck kommen (Ende von Op-Out, Stillschweigen, vorangekreuzten Kästchen etc.)
- Durch weitreichende Informations- und Dokumentationspflichten können komplexe Datenschutzhinweise entstehen, die auch in AGB zulässig sind, soweit sie besonders hervorgehoben sind.

# DS-GVO EINWILLIGUNG

## Einwilligung - Freiwilligkeit

- Freiwilligkeit erfordert, dass die Einwilligung auf dem uneingeschränkten freien Willen der betroffenen Person beruhen muss.

  → Kopplungsverbot

- Einwilligung kann jederzeit widerrufen werden, Art. 7 Abs. 3 DS-GVO

- Nach den Erwägungsgründen gilt eine Einwilligung als dann nicht freiwillig abgegeben, wenn zwischen den Parteien ein klares Ungleichgewicht besteht und deshalb unwahrscheinlich ist, dass die Einwilligung ohne Zwang abgegeben wurde

# DS-GVO EINWILLIGUNG

## Einwilligung - Form

- DS-GVO sieht keine bestimmte Form vor
- Kann schriftlich, elektronisch oder mündlich erfolgen
- Aber: Datenverarbeiter unterliegen der Nachweispflicht aus Art. 5 DS-GVO
- Daher Empfehlung: in der Praxis Einwilligungen in Schriftform (Textform) oder auf andere bewährte Weise (double opt-in)
- Hinweis auf Widerrufsmöglichkeit

- Gelten bislang eingeholte Einwilligungen fort?
  - Erwägungsgrund 171 sofern diese ihrer Art nach den Bedingungen der DS-GVO entsprechen

# DS-GVO EINWILLIGUNG

## Einwilligung - Sonstiges

- Bei Kindern, die das 16. Lebensjahr noch nicht vollendet haben, müssen die Erziehungsberechtigten einwilligen (Art. 8 DS-GVO)

# DS-GVO EINWILLIGUNG

Achtung bei E-Mail Werbung

Trennung in

- Datenschutzrechtliche Einwilligung
- Wettbewerbsrechtliche Einwilligung

Ändert sich auch durch DS-GVO nicht!

- Einwilligung nach UWG
  - Freiwilligkeit
  - Informiertheit
  - Ausdrücklichkeit
- Unzulässige Werbung = Eingriff in das allgemeine Persönlichkeitsrecht bzw. das Recht am eingerichteten und ausgeübten Gewerbebetrieb

# BEISPIEL EINWILLIGUNG

## Achtung bei E-Mail Werbung

Werbliche Ansprache über E-Mail Adresse (§ 7 Abs. 2 Nr. 3 UWG)

*„eine unzumutbare Belästigung ist stets anzunehmen ... Bei Werbung unter Verwendung elektronischer Post, ohne dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegt.“*

# BEISPIEL EINWILLIGUNG

## Achtung bei E-Mail Werbung

### Bestandskundenmarketing (§ 7 Abs. 3 UWG)

Voraussetzungen:

(1) E-Mail Adresse wurde im Zusammenhang mit abgeschlossenem Vertrag erlangt

(2) Direktwerbung für eigene ähnliche Produkte

- Enge Auslegung, vgl. OLG Jena Urt. V. 21.04.2010 – 2 U 88/10
- „die Ähnlichkeit muss sich auf die bereits gekauften Waren beziehen und dem gleichen typischen Verwendungszweck oder Bedarf des Kunden entsprechen; ggf. ist es noch zulässig, Zubehör oder Ergänzungswaren zu bewerben...“

(3) Kein Widerspruch des Kunden

(4) „klarer und deutlicher“ Hinweis auf Widerspruchsrecht bei Erhebung

# RECHTE DES BETROFFENEN

Datenschutzgrundverordnung stärkt die Rechte der Betroffenen

**Welche Rechte hat der Betroffene?**

- *Informationsrecht*
- *Auskunfts- und Widerspruchsrecht*
- *Recht auf Berichtigung, Löschung und Einschränkung*

- **Recht auf Datenübertragbarkeit/Datenportabilität**
- **Recht auf Vergessenwerden**
- **Beschwerderecht (bei den Aufsichtsbehörden)**

# RECHTE DES BETROFFENEN

**Die zur Verfügung gestellte schriftliche Information muss**

- *leicht zugänglich und verständlich*
- *in klarer einfacher Sprache sowie*
- *transparent sein (was – warum – wo – durch wen getan wird)*

**Es müssen Informationen gegeben werden**

- *zur Rechtsgrundlage für die Datenverarbeitung*
- *zu Speicherdauer und Löschfristen*
- *zu den Rechten der von der DV betroffenen Person (Widerruf,…)*
- *zum Datentransfer in Länder außerhalb der EU*
- *zum Auftragsverarbeiter*

# RECHTE DES BETROFFENEN

**Achtung: die betroffene Person hat**

- *Anspruch auf eine „Kopie“ der gespeicherten Informationen*
- *Anspruch auf Antwort innerhalb von ein bis drei Monaten*
- *Recht des Verantwortlichen mutwillige Anfragen abzuwehren oder Vergütung zu verlangen (Beweislast für Mutwillen liegt beim Verantwortlichen)*

**Wann besteht keine Informationspflicht?**

- *Wenn der Betroffene bereits über die Informationen verfügt*
- *Wenn die Speicherung oder Offenlegung ausdrücklich durch Rechtsvorschrift geregelt ist*
- *Wenn die Informationen öffentlich zugänglich sind*
- *Wenn die Mitteilung sich als unmöglich erweist bzw. einen unverhältnismäßigen Aufwand erfordert*
- *Bei geheimhaltungspflichtigen Daten*

# DATENSCHUTZMANAGEMENT

## Regelungen zum Datenschutzmanagement

- Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten
- Art. 30 DSGVO Verzeichnis aller Verarbeitungstätigkeiten
- Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen
- Art. 35 DSGVO Risiko-Folgenabschätzung

# DATENSCHUTZMANAGEMENT

## Was verlangt ein DSMS

- Datenschutzrichtlinie
- Datenschutzorganisation und Verantwortlichkeiten
- Sensibilisierung der Mitarbeiter
- Durchführung von Kontrollen
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutz-Folgenabschätzung
- Vertragsmanagement
- Prozess zur Wahrnehmung von Betroffenenrechten
- Prozess zur Meldung von Datenschutzverstößen

# VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

- Verfahren, in denen personenbezogene Daten verarbeitet werden, sind zu identifizieren und in einer Verarbeitungsübersicht zu erfassen

- „Verarbeitung“ in Art. 4 DS-GVO beschrieben z.B.:
  - Erheben, Erfassen, Speichern, Organisieren, Ordnen, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Übermitteln, Verbreiten, Bereitstellen, Abgleich, Verknüpfung, Einschränken, Löschen etc.

- „Verarbeitungstätigkeit“ = Gesamtheit an Verarbeitungen, mit deren Hilfe eine Zweckbestimmung oder ein Bündel zusammengehöriger Zweckbestimmungen realisiert wird. Sie kann aus einer Vielzahl von DV-Programmen und Dateien bestehen.

# VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

- Die Verpflichtung zu Führung eines Verarbeitungsverzeichnisses ergibt sich aus Art. 30 DS-GVO. Das Verzeichnis dient entsprechend des Erwägungsgrundes 82 zum Nachweis der Einhaltung der Verordnung

- Auch der Auftragsdatenverarbeiter muss ein Verzeichnis führen, das alle Kategorien von Verarbeitungstätigkeiten enthält, die er im Auftrag des Verantwortlichen durchführt

Kein Verzeichnis = Bußgeld
Eigentlich ist die Pflicht, unter gewissen Voraussetzungen ein Verzeichnis über alle relevanten Verarbeitungstätigkeiten führen zu müssen, nicht neu. Allerdings war ein Verstoß dagegen bisher nicht direkt bußgeldbewehrt.

# INHALT DES VERARBEITUNGVERZEICHNISSES

- Name und Kontaktdaten des für die Verarbeitung Verantwortlichen
- Verfahrens- (Prozess-) beschreibung
- Zwecke der Verarbeitung
- Kategorien von betroffenen Personen und personenbezogenen Daten
- Kategorien von Empfängern, an die Daten weitergegeben worden sind oder werden
- Übermittlung von Daten an ein Drittland
- Beauftragter Dienstleister
- Fristen für Löschungen
- Beschreibung der technisch organisatorischen Maßnahmen

# INHALT DES VERARBEITUNGVERZEICHNISSES

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

## Muster 9: Online-Shop – Verzeichnis von Verarbeitungstätigkeiten

**Verantwortlicher:**
Online-Shop Keramik
Hinterer Weg 15
91522 Fallstadt

Tel. 0981/123456-0
E-Mail: keramik@ shop-keramik-fallstadt.de
Web: www.shop-keramik-fallstadt.de

Vorstand: Gerlinde Meier, geb. 21.02.1986

| Verarbeitungstätigkeit | Ansprechpartner | Datum der Einführung | Zwecke der Verarbeitung | Kategorie betroffene Personen | Kategorie von personenbez. Daten | Kategorie von Empfängern | Drittlands-transfer | Löschfristen | Technische/organisatorische Maßnahmen |
|---|---|---|---|---|---|---|---|---|---|
| **Lohnabrechnung (über externen Dienstleister)** | Hans Klausen 0981/123456-1 hans@ shop-keramik-fallstadt.de | 01.01.2018 | • Auszahlung der Löhne/Gehälter<br>• Abfuhr Sozialabgaben u. Steuern | Beschäftigte | • Name und Adressen der Beschäftigten<br>• ggf. Religions-zugehörigkeit<br>• Eindeutige Kennzahlen zur Steuer... | Externes Buchhaltungsbüro | Keine | 10 Jahre (Gesetzliche Aufbewahrungsfrist) | Siehe IT-Sicherheitskonzept |
| **Betrieb der Webseite des Startups (über Hosting-Dienstleister)** | Peter Diercksen 0981/123456-2 peter@ shop-keramik-fallstadt.de | 19.03.2018 | Vertrieb von eigenen Produkten | • Kunden<br>• Webseitenbesucher | • IP-Adressen<br>• Stammdaten der Kunden<br>• E-Mail-Adressen + Passwörter | Keine | Keine | IP-Adresse nach 30 Tagen | Siehe IT-Sicherheitskonzept<br>+ HTTPS-Verschlüsselung<br>+ OWASP-Top10-Schutz<br>+ Patch Management |
| **Kundenverwaltung** | Marie Greiner 0981/123456-3 marie@ shop-keramik-fallstadt.de | 19.03.2018 | Verwaltung der Kundendaten | Kunden | • Stammdaten der Kunden<br>• Kaufhistorien | Keine | Keine | 10 Jahre (Gesetzliche Aufbewahrungsfrist) | Siehe IT-Sicherheitskonzept |
| **Zahlungsabwicklung bei Kunden (über externen Dienstleister)** | Peter Diercksen 0981/123456-2 peter@ shop-keramik-fallstadt.de | 19.03.2018 | Durchführung der Zahlungsverarbeitung | Kunden | • Stammdaten der Kunden<br>• Zahlungsdaten (Bankverbindung) | Keine | Keine | 10 Jahre (Gesetzliche Aufbewahrungsfrist) | Siehe IT-Sicherheitskonzept |
| **Werbemaßnahmen zur Kundengewinnung und -bindung** | Marie Greiner 0981/123456-3 marie@ shop-keramik-fallstadt.de | 20.03.2018 | Marketing zur Kundenakquirierung | • Bestandskunden<br>• potenzielle Neukunden | • E-Mail-Adressen der Kunden<br>• IP-Adressen | Keine | Keine | 10 Jahre (Gesetzliche Aufbewahrungsfrist) | Siehe IT-Sicherheitskonzept |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |

### Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Webplattform bzgl. OWASP-Top10 absichern
- ✓ Automatische Updates aktivieren
- ✓ Standard-Gruppenverwaltung
- ✓ Patch-Management bei CMS berücksichtigen
- ✓ Automati... Updates der Programmiersprache
- ✓ Aktueller...
- ✓ Kundendatenbank absichern
- ✓ Pseudonymisierung/Sperrung/Löschung von Kundendaten)
- ✓ ...mit Standard-Shredder

# VERTRAGS (AUFTRAGS-) MANAGEMENT

## Was ist Auftragsdatenverarbeitung?

Geregelt in Art. 28 DS-GVO

Die Auftragsdatenverarbeitung ist die

- Erhebung
- Verarbeitung
- Oder Nutzung von personenbezogenen Daten

Durch einen Auftragnehmer

- gem. den Weisungen der verantwortlichen Stelle (Auftraggeber)
- Auf Grundlage eines schriftlichen Vertrages

# VERTRAGS (AUFTRAGS-) MANAGEMENT

## Art. 28 DS-GVO verlangt bei ADV den Abschluss von Verträgen

Mindestanforderungen in Art. 28 DS-GVO

Wichtige Nachweispflichten

- zentrales Verzeichnis der Verträge
- turnusmäßige Prüfung der Inhalte
- Prüfung ob Verträge fehlen
- Altverträge auf Neuerungen prüfen

Beispiele typischer Fälle:

- ausgelagerte Callcenter
- Marketingaktionen durch externe Agenturen
- Dienstleisterverträge zur Datenträgerentsorgung
- Externe Lohn- bzw. Gehaltsabrechnung
- Ausgelagerte Rechenzentren
- Ausgelagerte Bewerbungsverfahren

# VERTRAGS (AUFTRAGS-) MANAGEMENT

## Art. 28 DS-GVO verlangt bei ADV den Abschluss von Verträgen

keine Auftragsverarbeitung!

- die Auslagerung von Aufgaben und Funktionen
- externe Inanspruchnahme von Fachleistungen

Beispiele typischer Fälle:

- Transportdienstleistungen von Post- oder Kurierdiensten
- Bewachungsdienste
- Reinigungsdienstleistungen
- Handwerkereinsätze im Unternehmen
- Finanzberatung
- Steuerberatung
- Inkassotätigkeit mit Forderungsübertragung
- Sachverständigen- bzw. Gutachtenbeauftragung

# DATENSCHUTZFOLGENABSCHÄTZUNG

- muss durchgeführt werden, wenn durch die DV voraussichtlich ein hohes Risiko für Rechte und Freiheiten nat. Personen besteht

- Unabhängig vom Risiko ist für besonders sensible Fälle zwingend eine Folgenabschätzung durchzuführen (Art. 35 DS-GVO) z.B. bei automatischer Verarbeitung von Daten, Profilbildungsmaßnahmen oder der systematische Überwachung öffentlich zugängliche Bereiche

- weitere Fälle werden von den Aufsichtsbehörden festgelegt

# MELDEPFLICHTEN BEI DATENPANNEN

- Meldung von Datenschutzverletzungen
  - Anforderungen verschärft
  - jeder (nicht nur bei besonders sensiblen Daten) unbefugte Datenzugriff ist unverzüglich, möglichst binnen 72 Stunden (Art. 33 Abs. 1 DS-GVO), zu melden

Aber:

- Meldepflicht besteht nicht, wenn Datenpanne voraussichtlich nicht zu einem Risiko für die betroffene Person führt
- Problem: Risikoeinschätzung → hierzu werden Hilfestellungen der Aufsichtsbehörden erwartet
- Es ist ein Verfahren zum Umgang mit Datenpannen einzurichten

# MELDEPFLICHTEN BEI DATENPANNEN

- Meldung von Datenschutzverletzungen
  - An den Betroffenen, wenn Risikoabwägung ergibt, dass durch Datenpanne voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht (Art. 34 DS-GVO)
  - Ausnahmen:
  - wenn geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen wurden, durch die die betroffenen Daten für Unbefugte nicht zugänglich sind (z.B. Verschlüsselung)
  - Durch nachfolgende Maßnahmen sichergestellt wurde, dass das hohe Risiko für die Rechte und Freiheiten aller Wahrscheinlichkeiten nicht mehr besteht
  - Die direkte Information der Betroffenen mit einem unverhältnismäßigen Aufwand verbunden wäre -> dann öffentliche Bekanntmachung

# HAFTUNG

- Die Haftung wird durch die DS-GVO erheblich verschärft.
- bei Verstößen gegen Grundprinzipien wird ein Bußgeld von bis zu 20 Mio. Euro oder 4 % des weltweiten letztjährigen Jahresumsatzes angedroht leichtere Verstöße (maximal zehn Mio. Euro und 2 % des weltweiten letztjährigen Jahresumsatzes)

# MAßNAHMENPLAN

Bestandsaufnahme notwendig!

- Welche Prozesse bestehen derzeit im Unternehmen bei denen personenbezogene Daten verarbeitet werden
- Bestimmung der Rechtsgrundlage auf der die Verarbeitung erfolgt
- Prüfung der Datenschutzorganisation, welche technischen Vorkehrungen bestehen oder geschaffen werden müssen, um die Sicherheit der Daten zu gewährleisten (Backup-Systeme, Verschlüsselung, Pseudonymisierung, Rollen-/Zugriffskonzepte)
- Prüfung bestehender Verträge mit Dienstleistern, Auftragsdatenverarbeitungsverträge, Wartungsverträge - findet hier eine Übermittlung außerhalb des EWR statt?
- Betriebsvereinbarungen zum Umgang mit Beschäftigtendaten
- **Datenschutzhinweise auf Vollständigkeit und Verständlichkeit prüfen**
- Vorformulierte Einwilligungserklärungen prüfen
- Dokumentationspflichten / Verarbeitungsverzeichnis

# HANDLUNGSEMPFEHLUNG

- Dokumentation der Datenverarbeitungsprozesse im Unternehmen
  - Erstellung und / oder Aktualisierung der Verarbeitungsübersicht
  - ToMs dokumentieren und Wirksamkeit prüfen
  - Einführung von Risikobewertungen (Risikomatrix)
  - Vereinbarung zu Auftragsdatenverarbeitung

- Organisatorisches
  - Datenschutzerklärung (Erweiterung der Informationspflichten)
  - Einwilligungserklärungen (Verschärfung der formalen Vorgaben)

- Meldepflichten
  - Prozess der Meldung von Datenpannen
  - Empfehlungen der deutschen Aufsichtsbehörden

- Wahrung der Rechte Betroffener
  - Prozess zur Auskunftserteilung
  - Prozess zum Widerruf der Einwilligung
  - Prozess zum Umgang der Rechte auf Löschung, Sperrung, Vergessen werden

# DATENSCHUTZ 2018 – NEUE REGELUNGEN

Vielen Dank für die
Aufmerksamkeit