BLD
BACH LANGHEID DALLMAYR

Die EU-Datenschutzgrundverordnung

Auswirkungen auf die Beratungspraxis – Ausgewählte Problemfelder

Dr. Tobias Britz I 08.03.2018

Agenda

- **Einführung**
- Anwendbarkeit, Rechtsbehelfe, Haftung und Sanktionen
- Einwilligung
- Berechtigtes Interesse
- Benachrichtigungspflichten
- Meldepflichten bei Verstößen gegen DS-GVO
- Kundenkontakt und Grundsätze „privacy by design“ und „privacy by default“
- Dokumentationspflichten

Einführung: DS-GVO in der Presse

BLD
BACH LANGHEID DALLMAYR

Quelle: F.A.Z. – Unternehmen „Die europäische Datenschutz-Reform schafft Stellen“ – Montag, 27.11.2017

„Hinzu komme, dass Interessenverbände für Verbraucher künftig ohne Auftrag klagen dürften. Es reicht dann eine Unterlassungsklage gegen ein Unternehmen – danach wäre es für Anwälte ein einträgliches Geschäft, die einzelnen Ersatzklagen gegen das Unternehmen zu führen, meint Wybitul. Und dann steht ja noch eine mögliche neue Sammelklage für Verbraucher im Raum – die „Musterfeststellungsklage“ wurde in der letzten Regierung zwar knapp durch die Union verhindert. Doch eine neue Regierung wird voraussichtlich einen neuen Anlauf unternehmen.“

Quelle: F.A.Z. – Unternehmen, 7.2.2018 - „Mail-Adressen speichern kann plötzlich teuer werden“

BILD Zeitung vom 13.01.2018,
Quelle: www.bild.de

86 Makler - und nur einer ohne Beanstandung

Dabei sind Verstöße gegen das Bundesdatenschutzgesetz offenkundig. 2015/16 blieb bei einer Überprüfung in Bayern nur einer von 86 Immobilienmaklern unbeanstandet, wie Alexander Filip berichtet, Referatsleiter beim Bayerischen Landesamt für Datenschutzaufsicht, kurz BayLDA.

Quelle: www.computerwoche.de

EU-Datenschutz 2018

Die Folgen für das Marketing

14.02.2017 Von Sachiko Scheuing (Experte) IDG EXPERTEN NETZWERK

Die europäische Datenschutzgrundverordnung birgt für Unternehmen Herausforderungen. Gerade für Marketing-Spezialisten ergeben sich aber auch neue Möglichkeiten.

Agenda

- Einführung
- **Anwendbarkeit, Rechtsbehelfe, Haftung und Sanktionen**
- Einwilligung
- Berechtigtes Interesse
- Benachrichtigungspflichten
- Meldepflichten bei Verstößen gegen DS-GVO
- Kundenkontakt und Grundsätze „privacy by design“ und „privacy by default“
- Dokumentationspflichten

DS-GVO und das BDSG n.F.

BLD
BACH LANGHEID DALLMAYR

DS-GVO
(EU) 2016/679 vom 27. April 2016

- Harmonisierung der Datenschutz-vorschriften in der EU
- Stärkung des Verbraucherschutz
- Datenportabilität
- **Unmittelbare Geltung** ab 25. Mai 2018

Bundesdatenschutzgesetz vom 05. Juli 2017
Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680

- **Konkretisierung der sog. Öffnungsklauseln DS-GVO**
- Umsetzung RL 2016/680 (EU)
- Regelungen für Anwendungsbereich außerhalb DS-GVO und RL 2016/680

Überblick

BLD
BACH LANGHEID DALLMAYR

Ziele der EU-DSGVO (VERORDNUNG (EU) 2016/679 vom 27. April 2016)

- Harmonisierung der Datenschutzvorschriften innerhalb der EU
  - Unionsweit gleichwertiger **Schutz der Grundrechte** und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten (Art. 1 Abs. 2 EU-DSGVO).
  - Gewährleistung des **freien Verkehrs personenbezogener Daten** zwischen den Mitgliedstaaten (Art. 1 Abs. 3 EU-DSGVO).
- Unmittelbar geltende **Verordnung** (Art. 288 Abs. 2 AEUV) statt umsetzungsbedürftiger Richtlinie, um
  - einzelstaatliche Gestaltungsmöglichkeiten gering zu halten;
  - das Ziel des gemeinsamen Marktes zu erreichen.

Überblick

Mittel zur Erreichung der Ziele der EU-DSGVO (VERORDNUNG (EU) 2016/679 vom 27. April 2016)

- Rechte der **Verbraucher** stärken und besser durchsetzen:
  - Hohe Bußgelder;
  - Verbandsklagen und Kopplungsverbote (Anlehnung an Verbraucherschutz).
- **Harmonisierung des Rechtsrahmens**, insbes. durch Beseitigung von Ungleichheiten zwischen den Mitgliedstaaten:
  - Richtlinie wird durch eine Verordnung ersetzt;
  - Bürokratische Pflichten sollen vereinfacht oder abgeschafft werden.
- **Technischer Datenschutz:**
  - „Privacy by design“ und „Privacy by default“
  - Datenportabilität

Anwendungsbereich DS-GVO

BLD
BACH LANGHEID DALLMAYR

Rückblick: EuGH zum Begriff der personenbezogenen Daten nach DSRL

§ 3 BDSG alt: „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“

EuGH (Urt. v. 19.10.2016, Az. C-582/14) i. S. Breyer vs. Deutschland

„… ist dahin auszulegen, dass eine dynamische Internetprotokoll-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, ***wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.“***

→ **Weites aber kein absolutes Verständnis** (vgl. auch BGH, Urt. 16.05.2017, Az. VI ZR 135/13, VersR 2017, 955 ff.)

Anwendungsbereich DS-GVO

BLD
BACH LANGHEID DALLMAYR

Personenbezogene Daten nach DS-GVO (Sachlicher Anwendungsbereich)

- **Ausgenommen:** familiäre oder private Tätigkeiten, personenbezogene Daten Verstorbener (EWG 27), personenbezogene Daten juristischer Personen.
- **Art. 4 Ziff. 1 DS-GVO:**
  - Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („Betroffene “) 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, **identifiziert werden kann**.

Anwendungsbereich DS-GVO

BLD
BACH LANGHEID DALLMAYR

Begriff der personenbezogene Daten

- EWG 26 (Auszug):
  - Grundsätze gelten für alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
  - Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die **von dem Verantwortlichen oder einer anderen Person** nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.
  - Bei dieser Feststellung sollten alle **objektiven Faktoren**, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.
  - **Nicht** für anonyme Informationen, d. h. Informationen, die sich **nicht auf eine identifizierte oder identifizierbare** natürliche Person beziehen.

→ **Anonymisierung** probates (und einziges?) Mittel, den Anforderungen der DS-GVO zu entgehen.

Anwendungsbereich DS-GVO

BLD
BACH LANGHEID DALLMAYR

Räumlicher Anwendungsbereich

- Einführung **Marktortprinzip** (vgl. bereits **Google-Urteil** des EuGH (EuZW 2014, 541) als zentrale materielle Änderung:
  - Art. 3 Abs. 1 DS-GVO:

    *„Diese **Verordnung findet Anwendung** auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, **unabhängig davon, ob die Verarbeitung in der Union stattfindet**."*
  - Art. 3 Abs. 2 DS-GVO:
    - Europäisches Datenschutzrecht gilt auch für außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind, **sofern sich**

      → **ein Angebot an einen bestimmten nationalen Markt in der EU richtet** (Art. 3 Abs. 2 lit. a.) **oder**

      → **die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient** (Art. 3 Abs. 3 lit. b.).

Anwendungsbereich DS-GVO

BLD
BACH LANGHEID DALLMAYR

Zeitlicher Anwendungsbereich

- **DS-GVO gilt ab dem 25. Mai 2018**
- **Was ist mit Bestandsverträgen?**
  - Art. 99 Abs. 2 DS-GVO schreibt umfassende Geltung ab dem 25. Mai 2018 vor.
  - Kein Nebeneinander von alt und neu!
  - EWG 171 (Auszug): Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung **mit ihr in Einklang gebracht werden**.

  → **Es gibt keine weitere Übergangsfrist!**

  → **Grundsätze der DS-GVO auch in der Beratungspraxis ab dem 25.05.2018 zu beachten.**

Rechtsbehelfe, Haftung und Sanktionen

BLD
BACH LANGHEID DALLMAYR

Beschwerde bei der Aufsichtsbehörde, Art. 77 DS-GVO

- Abs: 1: Voraussetzungen
  - Beschwerdeführer: jede betroffene (natürliche) Person,
  - Beschwerdegegenstand: Verstoß gegen die DS-GVO,
  - Zuständige Behörde: richtet sich grundsätzlich nach der Person des Betroffenen; so z.B. die
    - → seines Mitgliedsstaates
    - → seines Aufenthaltsortes
    - → seines Arbeitsplatzes
    - → des Ortes des Verstoßes,
- Abs. 2: Pflichten der Aufsichtsbehörde:
  - Beschwerdeführer ist über den Stand und die Ergebnisse der Beschwerde sowie Möglichkeit eines gerichtlichen Rechtsbehelfs gegen die Aufsichtsbehörde (vgl. Art. 78 DS-GVO) zu unterrichten

Rechtsbehelfe, Haftung und Sanktionen

Direktes Klagerecht des Betroffenen, Art. 79 Abs. 1 DS-GVO (besteht kumulativ zu Art. 77 DS-GVO)

- Möglicher Kläger: jede betroffene (natürliche) Person
- Statthafte Klagemöglichkeiten bei Verstoß gegen die DS-GVO
  - Schadensersatz
  - Unterlassen
  - Feststellung
  - Auskunft
  - Berichtigung bzw. Berichtigung von Datensätzen
- Gerichtsstand: Ort der **Niederlassung** der datenverarbeitenden Stelle oder eigener **Aufenthaltsort des Betroffenen**
- **Neu**: Auftragsverarbeiter können unmittelbar rechtlich belangt werden

Rechtsbehelfe, Haftung und Sanktionen

Neu: die **Geltendmachung immaterieller Schäden** (insbes. Persönlichkeitsrecht) wird ausdrücklich normiert: Art. 82 Abs. 1 DS-GVO:

- Bei Verstößen gegen die Verordnung soll *„ein wirksamer Schadensersatz für die betroffene Person sichergestellt“* werden (Art. 82 Abs. 4 DS-GVO; EW 146)
  - → **Wesentliche Änderung gegenüber dem bisherigen Recht** (nach diesem war die erfolgreiche Geltendmachung von Schadensersatzansprüchen eher die Ausnahme, vgl. *Wybitul*, ZD 2016, S. 253),
  - → Vgl. aber **§ 7 BDSG**, wobei Norm nur materielle Schäden erfasste (vgl. Gola/Schomerus, 12. Auflage, § 7 Rn. 12 m.w.N.) und in praxi ein Schattendasein führte,
  - → Aufgrund eines *„derzeit ausgesprochen datenschutzfreundlichen Kurses“* des EuGH ist **zukünftig von deutlich höheren Bußgeldern auszugehen**, als sie die deutschen Gerichte bislang festgelegt haben (vgl. *Wybitul*, ZD 2016, S. 253).

Rechtsbehelfe, Haftung und Sanktionen

- **Art. 82 Abs. 2 DS-GVO:**

  „Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.“

  → **verschuldensunabhängige Haftung** für Schäden, die durch eine nicht der Verordnung entsprechenden Verarbeitung verursacht wurden (*Wybitul*, ZD 2016, S. 254),

  → mögliche Haftungsbefreiung lediglich durch **Nachweis, *„in keinerlei Hinsicht“*** für den Umstand, durch den der Schaden eingetreten ist, **verantwortlich zu sein** (Abs. 3).

Rechtsbehelfe, Haftung und Sanktionen

Neu: **Nachweisregelung zuungunsten der verarbeitenden Stelle** (Art. 24 Abs. 1 DS-GVO):

→ Die für die Verarbeitung verantwortlichen Unternehmen müssen **sicherstellen,** dass ihre Datenverarbeitung gemäß der DSGVO erfolgt **und** den **Nachweis hierfür erbringen können.**

- Hieraus wird sich voraussichtlich eine **Beweislastumkehr** ergeben als *„besonders folgenschwere Veränderung gegenüber dem bisherigen Recht“* (*Wybitul* ZD 2016, S. 254)
  - Sie **fordert** von den Unternehmen neben einer **umfassenden Implementierung** der strengen EU-DSGVO-Regelungen auch eine **umfassende Dokumentation sämtlicher Maßnahmen** zur Sicherstellung des Datenschutzes,
  - **Nachweis**, die Vorgaben der EU-DSGVO tatsächlich eingehalten zu haben, **ist in der Praxis *„ausgesprochen schwierig“ .***

→ Die **Beweislastregelung gilt für sämtliche Anforderungen der DS-GVO** (auch bei Verwaltungs- und Gerichtsverfahren über die Verhängung von Bußgeldern; *Wybitul* a.a.O.)

Rechtsbehelfe, Haftung und Sanktionen

Neu: Ausweitung des Bußgeldrahmens, Art. 83 DS-GVO

→ **Bußgelder** bis zu **4 % des Jahresumsatzes eines Unternehmens** bzw. 20 Mio. Euro sind zulässig.

- **kartellrechtlicher Unternehmensbegriff** i.S.d. Art. 101, 102 AEUV (ErwGr. 150):

  *„Unternehmen ist **jede eine wirtschaftliche Tätigkeit ausübende Einheit**, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung."* (St. Rspr. seit EuGH, Rs. C-41/90 (Höfner und Elser), Slg. 1991, I-1979, Rn. 21)

  → Die wirtschaftliche Einheit kann aus mehreren, natürlichen oder juristischen Personen bestehen; nicht nur aus einem einzelnen Unternehmen i.S.e. Rechtssubjekts (vgl. *Faust/Spittka/Wybitul* ZD 2016, S. 121 mwN),

  → Anknüpfung an das **Marktverhalten der wirtschaftlichen Einheit.**

Rechtsbehelfe, Haftung und Sanktionen

BLD
BACH LANGHEID DALLMAYR

Konsequenz des kartellrechtlichen Unternehmensbegriffs

- **Zurechnung** innerhalb der wirtschaftlichen Einheit erfolgt **von unten nach oben**, sofern ein bestimmender Einfluss gegeben ist (*Faust/Spittka/Wybitul* ZD 2016, S. 121):
  - z.B.: Haftung der Muttergesellschaft für Tochterunternehmen (+), wenn die Muttergesellschaft aus wirtschaftlichen, organisatorischen oder rechtlichen Gründen die **Möglichkeit eines bestimmenden Einflusses** auf die Tochtergesellschaft hat **und diesen Einfluss auch ausübt,**
  - **Vermutung eines bestimmenden Einflusses** bei (beinahe) 100 %-iger Tochtergesellschaft (grds. widerlegbar, in der Praxis aber noch nicht gelungen),
  - konkret handelnde Person muss nicht benannt werden, sofern sie die Grenzen ihrer Funktion nicht klar überschreitet (vgl. *Faust/Spittka/Wybitul* ZD 2016, S. 121 mwN).

→ Mutter- und Tochtergesellschaft haften **gesamtschuldnerisch!**

Rechtsbehelfe, Haftung und Sanktionen

BLD BACH LANGHEID DALLMAYR

Sanktionen

- **Kriterien** für Verhängung einer Geldbuße **nach Art. 83 Abs. 2 EU-DSGVO**:
  - **Art, Schwere und Dauer** des Verstoßes (lit. a),
  - Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes (lit. b),
  - **Getroffene Maßnahmen zur Minderung** des entstandenen Schadens (lit. c),
  - Grad der Verantwortung unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen (lit. d),
  - Etwaige einschlägige frühere Verstöße (lit. e),
  - **Umfang der Zusammenarbeit mit der Aufsichtsbehörde**, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern (lit. f),
  - **Kategorien personenbezogener Daten**, die von dem Verstoß betroffen sind (lit. g),
  - **Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde**, insbesondere Selbstanzeige (lit. h),
  - Einhaltung früher angeordneter Maßnahmen (lit. i),
  - Einhaltung von genehmigten Verhaltensregeln nach Art. 40 oder genehmigten Zertifizierungsverfahren nach Art. 42 (lit. j),
  - Jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste (lit. k).

Rechtsbehelfe, Haftung und Sanktionen

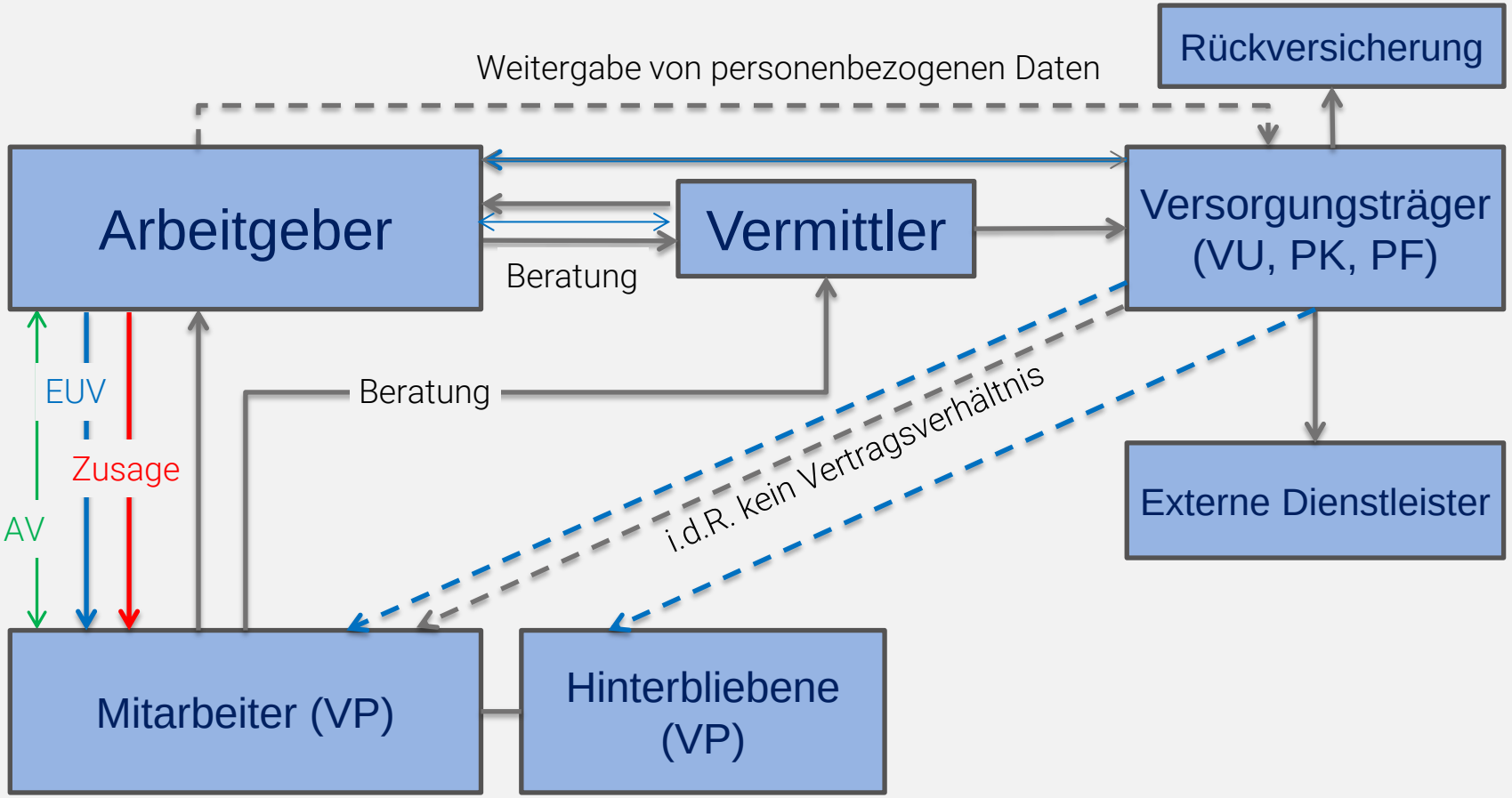
Fazit:

- Klagepotential und Klagebereitschaft wird steigen.
- Die Anforderungen des Datenschutzes mit Blick auf die Sanktionsmöglichkeiten der Behörden und Gerichte keine Nebensache mehr.
- Vorsicht bei „Umgehungsstrategien“ jeder Art.
- Vorsicht bei Versuchen, etwaig identifizierte Schwachstellen zu ignorieren oder zu verschleiern.

Agenda

- Einführung
- Anwendbarkeit, Rechtsbehelfe, Haftung und Sanktionen
- **Einwilligung**
- Berechtigtes Interesse
- Benachrichtigungspflichten
- Meldepflichten bei Verstößen gegen DS-GVO
- Kundenkontakt und Grundsätze „privacy by design“ und „privacy by default“
- Dokumentationspflichten

Weitergabe personenbezogener Daten in der Praxis – hier: DV, PK oder PF



Überblick Erlaubnistatbestände

BLD
BACH LANGHEID DALLMAYR

COC 2.0!

Rechtmäßigkeit der Datenverarbeitung

- Art. 6 Abs. 1 EU-DSGVO – auch weiterhin als ***„Verbot mit Erlaubnisvorbehalt“***
- Datenverarbeitung ist zulässig, wenn
  - die betroffene Person ihre **Einwilligung** gegeben hat (lit. a) *oder*
  - sie zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist; auf Antrag der betroffenen Person (lit. b) *oder*
  - sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt (lit. c) *oder*
  - sie zum Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen natürlichen Person erforderlich ist (lit. d) *oder*
  - sie im öffentlichen Interesse oder zur Erfüllung hoheitlicher Aufgaben erforderlich ist (lit. e) *oder*
  - sie zur **Wahrung berechtigter Interessen** des Verantwortlichen oder eines Dritten erforderlich ist, ohne dass die Interessen oder Grundrechte /-freiheiten der betroffenen Person überwiegen (lit. f)

Überblick Erlaubnistatbestände

BLD
BACH LANGHEID DALLMAYR

Was ist mit den „alten“ Einwilligungserklärungen?

- DS-GVO gilt grundsätzlich auch für bestehende Datenverarbeitungsprozesse
- **EW 171:** Es ist nicht erforderlich, dass die betroffene Person zu einer gleichartigen fortgesetzten Datenverarbeitung erneut einwilligt, zu der sie gemäß der Datenschutzrichtlinie 95/46/EG bzw. der entsprechend Umsetzung durch das BDSG eingewilligt hat, ***wenn die Art der bereits erteilten Einwilligung den Bedingungen der DS-GVO entspricht.***

- Anforderungen nach § 4a BDSG
  - Informierte Einwilligung
  - Schriftlichkeit
  - Hinweis auf Widerrufsrecht
  - (Koppelungsverbot, str.)

- Beschluss Düsseldorfer Kreis 13./14.9.2016
  - Informationen nach Art. 13 DS-GVO (-), aber über Verantwortliche Stelle und Zweck
  - Erklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache
  - Freiwilligkeit (Koppelungsverbot)!
  - Altersgrenze 16 Jahre

Einwilligung

- **Begriffsbestimmung** gem. Art. 4 Nr. 11 DS-GVO: Einwilligung ist

  „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“.

- Art. 7 DS-GVO - **Bedingungen für die Einwilligung**:

*„(1) **Beruht** die Verarbeitung auf einer Einwilligung, muss der Verantwortliche **nachweisen** können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.*

*(2) Erfolgt die **Einwilligung** der betroffenen Person durch eine schriftliche Erklärung, die **noch andere Sachverhalte** betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten **klar zu unterscheiden** ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.“*

Einwilligung

BLD
BACH LANGHEID DALLMAYR

Anwendungsprobleme

- Schriftliche Einwilligung?
  - Grundsätzlich nicht mehr vorgeschrieben
  - Aber: **Nachweis** der Einwilligung sowie der Kenntnis des Betroffenen über Abgabe und Inhalt der Erklärung erforderlich (EWG 42).
- Einwilligung setzt voraus, dass Einwilligungserklärung „*in verständlicher und **leicht zugänglicher Form** in **einer klaren und einfachen Sprache***“ verfasst wird und „*keine missbräuchlichen Klauseln*“ beinhaltet.
- Betroffene Person sollte „*mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen*“.

Einwilligung

BLD
BACH LANGHEID DALLMAYR

Anwendungsprobleme

- Informierte und Freiwillige Einwilligung
  - EWG 42 (Auszug): „*eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden*.“
  - EWG 43: Bei „**klarem Ungleichgewicht**“ zwischen Vertragspartnern sollte Einwilligung keine Rechtsgrundlage liefern (!)
    - Schulz in Gola, DS-GVO Art. 7 Rn. 20: Versicherungswesen als Beispiel, Abstimmung mit Aufsichtsbehörden
    - Buchner/Kühling, Art. 7 DS-GVO Rn. 45: Einzelfall maßgeblich.
  - EWG 43: Einwilligung gilt als nicht freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen **nicht gesondert** (…) erteilt werden kann, obwohl dies im Einzelfall angebracht ist,

Einwilligung

BLD
BACH LANGHEID DALLMAYR

Anwendungsprobleme

- „Vorsorgliche“ Einwilligungserklärung bei Vorliegen anderer Rechtfertigungsgründe?
- Art. 7 Abs. 4 DS-GVO (allgemeines Koppelungsverbot)
  - Art. 7 Abs. 4 DS-GVO: *Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde,* ***muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden****, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrages nicht erforderlich ist.*
    - Wohl kein absolutes Verbot nach Wortlaut (str.; so etwa Schulz a.a.O. Art. 7 Rn. 20)
    - EWG 43: Einwilligung **gilt als nicht freiwillig erteilt**, (…) oder wenn die Erfüllung eines Vertrags (…) von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

Einwilligung

BLD
BACH LANGHEID DALLMAYR

Einwilligungen (auch) im elektronischen Verkehr

- EWG 32 stellt klar, dass Einwilligung
  - *„durch eine **eindeutige bestätigende Handlung** erfolgen [muss], mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch **elektronisch erfolgen kann**, oder einer **mündlichen Erklärung**."*
  - Nur Opting-In
  - Bei mehren Zwecken aus Sicht der DS-GVO idR auch mehre Einwilligungen

→ Kommission hatte ursprünglich sogar „explizite" Einwilligung verlangt, der es bei der „Verarbeitung besonderer Kategorien" personenbezogener Daten bedarf (vgl. Art. 9 Abs. 2 lit. a.; s.u.)

→ Formfreiheit ist damit ebenso anerkannt, wie konkludente oder stillschweigende Einwilligung regelmäßig ausgeschlossen ist.

Einwilligung

BLD
BACH LANGHEID DALLMAYR

Verarbeitung und Einwilligung besonderer Kategorien personenbezogener Daten

- Art. 9 Abs. 1 DS-GVO:

  *„… sowie **die Verarbeitung von** genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person **ist untersagt**."*

→ Entspricht restriktiverem Verständnis wie bereits § 3 BDSG.

→ **Verarbeitung aufgrund öffentlichen Interesses** (ohne Einwilligung der betroffenen Person) darf **nicht zur Datenverarbeitung durch Dritte** (u.a. Arbeitgeber, Versicherungs- oder Finanzunternehmen) **zu anderen Zwecken** führen (Erw. 54).

- Betroffene muss in diesem Fall in die Verarbeitung **dieser** *„Daten für einen oder mehrere festgelegte Zwecke **ausdrücklich** eingewilligt [haben]".*

Einwilligung

BLD
BACH LANGHEID DALLMAYR

Verarbeitung und Einwilligung besonderer Kategorien personenbezogener Daten (Forts.)

- Anforderungen an die Einwilligung
  - Ausdrücklichkeitserfordernis
  - Hinweis auf Sensitivität der Daten
  - Erhöhtes Maß an Bestimmtheit und Genauigkeit
  - Zwei-Schranken-Prinzip (ggf. zwei Erklärungen, str.)
- Ausnahmen bei „Veröffentlichung“ durch Betroffenen und Rechtstreitigkeiten (vgl. Art. 9 Abs. 2 lit. e)
- Auch keine Ausnahme für die **PKV**, da weder von DS-GVO (vgl. Art. 9 Abs. 2 lit. b DS-GVO) von Öffnungsklausel (Gesundheitsvorsorge pp., vgl. § 24 Abs. 2 i.V.m. § 22 Abs. 1 Nr. 1. b BDSG n.F.) erfasst

  → Vor dem Hintergrund der Überbetonung der Freiwilligkeit nicht nachvollziehbar (oder gar unsinnig?)

Einwilligung

BLD
BACH LANGHEID DALLMAYR

Zusammenfassung zur Einwilligung

- Die Erhebung personenbezogener Daten bedarf grundsätzlich einer **ausdrücklichen, Einwilligung**, die
  - eindeutig
  - freiwillig
  - für jeden Fall im Einzelnen und
  - **nach ausreichender Information über Zweck und Folgen** der Erhebung eingeholt wurde.
- Schriftformerfordernis entfällt, praktisch aber Nachweispflicht
- Koppelungsverbot wird verschärft
- Mustererklärungen GDV werden Erleichterung bringen
- Zugleich und systemimmanent: Gefahr einer Überforderung des Kunden („information overkill“)

→ Sorgfältiger Umgang mit Einwilligungserklärungen in der Beratungspraxis unerlässlich!

Agenda

- Einführung
- Anwendbarkeit, Rechtsbehelfe, Haftung und Sanktionen
- Einwilligung
- **Berechtigtes Interesse**
- Benachrichtigungspflichten
- Meldepflichten bei Verstößen gegen DS-GVO
- Kundenkontakt und Grundsätze „privacy by design“ und „privacy by default“
- Dokumentationspflichten

Berechtigtes Interesse

BLD
BACH LANGHEID DALLMAYR

Datenverarbeitung zur Vertragserfüllung

- **Art. 6 Abs. 1 lit. b) DS-GVO** gestattet Verarbeitung, wenn diese für die Erfüllung eines **Vertrages** mit betroffener Person als Vertragspartei oder als vorvertragliche Maßnahmen erforderlich!
  - Begriff des Vertrages (bislang Schuldverhältnis)
  - Vertragszweck gibt Umfang der Verarbeitung vor (sachlicher Zusammenhang)
  - Begriff der **Erforderlichkeit** in Praxis problematisch:
    - Wohl nicht im Sinne einer absolut zwingenden Notwendigkeit zu verstehen, wonach andernfalls Vertrag nicht durchführbar (Schulz, a.a.O. Art. 6 Rn. 36).
    - Aber bloße Zweckdienlichkeit genügt nicht
    - Beispiele: Auswertung risikorelevanter Daten für Vertragsschluss (Buchner/Petri, a.a.O. Art. 6 Rn. 42)
    - HIS-Anfragen

Berechtigtes Interesse

BLD
BACH LANGHEID DALLMAYR

Datenverarbeitung zur Wahrnehmung berechtigter Interessen

- **Art. 6 Abs. 1 lit. f) DS-GVO** gestattet Verarbeitung, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen **oder eines Dritten erforderlich ist**, sofern nicht Interessen, Grundrechte oder Grundfreiheiten des Betroffenen überwiegen.
  - Wie bereits bei § 28 BDSG auch hier wirtschaftliche, rechtliche oder ideelle Interessen (Schulz, a.a.O. Rn. 51; Buchner/Petri, a.a.O. Rn. 146; EW 46 ff. nennen z.B. Verhinderung von Betrug, Direktwerbung, Datenaustausch innerhalb einer Unternehmensgruppe sowie Gewährleistung von IT Sicherheit.)
  - Keine Abwägung mit Blick auf Art. 9 DS-GVO (bei Gesundheitsdaten ist Einwilligung idR obligatorisch)
- **Art. 6 Abs. 1 lit. c) DS-GVO** gestattet Verarbeitung, wenn diese für die Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich ist.
  - Rechtliche Verpflichtung aus EU-Recht oder Recht des MS, Beispiele § 257 HGB; § 147 AO; VO (EG) 881/2002; 2580/2001)

Berechtigtes Interesse

BLD
BACH LANGHEID DALLMAYR

Rechtmäßigkeit der Verarbeitung: Zweckbindung

- Art. 5 Abs. 1 lit. b DS-GVO sieht eine **enge Zweckbindung** vor
  - Datenerhebung nur für festgelegte, eindeutige und rechtmäßige Zwecke
  - Änderungen des Verarbeitungszwecks sind grundsätzlich nur erlaubt, sofern sie mit dem ursprünglichen Erhebungszweck vereinbar sind
- Art. 6 Abs. 4 DS-GVO: für eine etwaige Zweckänderung hat der Verantwortliche **diverse Umstände zu berücksichtigen** (z.B. Kontext der Erhebung, Konsequenzen für den Betroffenen pp)
- **Fazit:**
  - Berechtigtes Interesse, z.B. für Datenverarbeitung im Rahmen der Erstberatung, kann bei „einfachen“ personenbezogenen Daten helfen;
  - Aufgrund Abwägungsoffenheit aber Rechtsunsicherheit;
  - Strenge Zweckbindung und Zweckfestlegung.

Agenda

- Einführung
- Anwendbarkeit, Rechtsbehelfe, Haftung und Sanktionen
- Einwilligung
- Berechtigtes Interesse
- **Benachrichtigungspflichten**
- Meldepflichten bei Verstößen gegen DS-GVO
- Kundenkontakt und Grundsätze „privacy by design“ und „privacy by default“
- Dokumentationspflichten

Benachrichtigungspflichten

- **Bisherige Regelung des § 4 Abs. 3 BDSG**:

  Betroffene war *„von der verantwortlichen Stelle über*

  1. *die **Identität** der verantwortlichen Stelle,*
  2. *die **Zweckbestimmung** der Erhebung, Verarbeitung oder Nutzung und*
  3. *die **Kategorien von Empfängern** nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,*

  zu unterrichten.“

- **Mit DS-GVO verschiedene Arten der Unterrichtung:**
  - Art. 13 EU-DSGVO: Direkterhebung
  - Art. 14 EU-DSGVO: Dritterhebung
  - Art. 15 EU-DSGVO: Auskunftsansprüche des Betroffenen

Benachrichtigungspflichten

BLD
BACH LANGHEID DALLMAYR

Informationspflichten bei Direkterhebung

- Art. 13 Abs. 1 EU-DSGVO **erweitert Mitteilungspflichten** auf die Angabe
  - der **Kontaktdaten** des für die Verarbeitung Verantwortlichen und des Datenschutzbeauftragten (lit. a und b)
    - → lediglich die Identität der verantwortlichen Stelle genügt nicht mehr
  - **der Rechtsgrundlage** und **des berechtigten Interesses**, sofern die Datenerhebung auf einem solchen beruht (lit. c und d)
  - **stets** der Kategorien von Empfängern der personenbezogenen Daten (lit. e)
  - der beabsichtigten Übermittlung von personenbezogenen Daten an ein Drittland oder eine internationale Organisation inkl. Angemessenheitsbeschluss (lit. f)

In der Beratungspraxis zwingend zu beachten:

- → Informationspflicht besteht **im Zeitpunkt der Erhebung** (EW. 61)
- → Verpflichtung zum **Nachweis!**

Benachrichtigungspflichten

BLD
BACH LANGHEID DALLMAYR

Informationspflichten bei Direkterhebung

- Nach Art. 13 Abs. 2 DS-GVO zur Gewährleistung der **fairen und transparenten** Verarbeitung der Daten **zusätzlich** zu Informieren u.a.:
  - die **Dauer der Speicherung** bzw. Kriterien der Festlegung der Dauer (lit. a);
  - **Betroffenenrechte** wie Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs- und Widerspruchsrechte und das Recht auf Datenübertragbarkeit (lit. b);
  - die **Möglichkeit des Widerrufs** (lit. c);
  - die Beschwerderechte bei der Aufsichtsbehörde (lit. d);
  - ob Bereitstellung vertraglich oder gesetzlich vorgeschrieben (lit. e);
  - …
  - Ausnahmen nach § 32 DS-GVO

Benachrichtigungspflichten

BLD
BACH LANGHEID DALLMAYR

Informationspflichten bei indirekter Erhebung (Art. 14 DS-GVO)

- **Information analog Art. 13 DS-GVO** zzgl.:
  - **Regelm. Darlegungspflicht des berechtigten Interesses** (Art. 6 Abs. 1 lit. f EU-DSGVO), sofern die Datenerhebung auf einem solchen beruht;
  - Betroffenen sind die **Quellen mitzuteilen**, aus denen die personenbezogenen Daten stammen und **ob** diese öffentlich zugänglich sind (Art. 14 Abs. 2 lit. F DS-GVO);
- **Weniger Ausnahmen, u. a.**:
  - Betroffene Person verfügt bereits über die Information
  - Informationserteilung ist **unmöglich**
    - Rückgriff auf § 275 BGB (vgl. Franck, in Gola, DS-GVO, Art. 14 Rn. 23), aber europarechtskonforme Auslegung!
    - Identifikation der betroffenen Person erforderlich? idR Nein → Art. 11 DS-GVO

Benachrichtigungspflichten

BLD
BACH LANGHEID DALLMAYR

Informationspflichten bei indirekter Erhebung (Art. 14 DS-GVO) –

- **Oder …**
  - Mit **unverhältnismäßigem Aufwand** verbunden ist,
    - Abwägung Informationsinteresse des Betroffenen und Aufwand
    - Anzahl der Benachrichtigungen entscheidend (EW 61)
  - … insbesondere **Verwirklichung der Ziele dieser Verarbeitung** würde unmöglich
    - Wohl eng zu verstehen (Bäcker, in Kühling, DS-GVO, Art. 14 Rn. 55)
  - Verarbeitung der Daten ist durch Rechtsvorschriften ausdrücklich geregelt
  - Daten unterliegen dem Berufsgeheimnis der EU oder eines Mitgliedsstaates und müssen vertraulich behandelt werden.
- **Sowie** nach § 33 Abs. 1 Nr. 2 BDSG n.F
  - insbes. wenn Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigt würde, **sofern nicht** das berechtigte Interesse der Betroffenen Person überwiegt

Benachrichtigungspflichten

BLD
BACH LANGHEID DALLMAYR

Informationspflichten

- Wenn keine Information nach Art. 14 **Ergreifen geeigneter technischer und organisatorischer Maßnahmen** inkl. Dokumentation der Gründe der Nichtinformation.
- **Andernfalls**: die Übermittlung der Informationen hat unentgeltlich zu erfolgen:
  - Keine Form vorgeschrieben, problematisch ist „Medienbruch“
  - Bei Art. 14 DS-GVO: Innerhalb angemessener Frist, spätestens jedoch binnen 1 Monat, ggf. auch früher (z. B. bei Offenlegung an Dritte)
  - z.B. durch Bereitstellung auf einer Website, sofern sie für die Öffentlichkeit bestimmt ist (etwa bei Werbung im Internet).

Benachrichtigungspflichten

BLD
BACH LANGHEID DALLMAYR

Fazit für die Beratungspraxis:

- Datensparsamkeit im Hinblick auf Daten der zu versichernden oder bereits versicherten Arbeitnehmer in der Beratungspraxis obligatorisch zur Vermeidung entsprechender Pflichten – gilt v.a. in der Vertragsanbahnungsphase;
- Benachrichtigungspflichten können andernfalls insbes. VR in der Anbahnungsphase (Stichworte z.B. Kollektivgeschäft, Voranfragen pp) vor erhebliche Probleme stellen;
- Benachrichtigungspflichten können aber auch auf den Berater zurückfallen, wenn VR diese erfüllen muss;
- Unsachgemäße und nicht erforderliche Weitergabe von Daten der AN kann überdies v.a. für den Arbeitgeber und/oder seinen Makler selbst zum Problem werden.

Daher: in der Anbahnungsphase möglichst keine personenbezogenen Daten der Arbeitnehmer an den VR, d.h. Anonymisierung soweit Daten der AN benötigt werden!

Agenda

- Einführung
- Anwendbarkeit, Rechtsbehelfe, Haftung und Sanktionen
- Einwilligung
- Berechtigtes Interesse
- Benachrichtigungspflichten
- **Meldepflichten bei Verstößen gegen DS-GVO**
- Kundenkontakt und Grundsätze „privacy by design“ und „privacy by default“
- Dokumentationspflichten

Meldepflichten

BLD
BACH LANGHEID DALLMAYR

Meldepflichten bei Verletzung des Schutzes personenbezogener Daten

- Art. 33 DS-GVO: Gegenüber der **Aufsichtsbehörde**, sofern
  - der **Schutz personenbezogener Daten verletzt** wurde und
  - **Risiken für die persönlichen Rechte und Freiheiten** natürlicher Personen bestehen.

- Zeitrahmen (Abs. 1):
  - Grundsätzlich **unverzüglich**, d.h. ohne schuldhaftes Zögern (§ 121 BGB), und binnen **72 Stunden** (andernfalls inkl. Begründung für Verzögerung);
  - **Ausnahme:** Verletzung führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten (z.B. durch geeignete Verschlüsselung).
- **Neu**: Meldepflicht des Auftragsverarbeiters (Abs. 2).

Meldepflichten

Meldepflichten bei Verletzung des Schutzes personenbezogener Daten

- Art. 34 DS-GVO: Gegenüber der **betroffenen Person**
- **Neu:** Meldepflicht **nur, wenn** die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein **hohes Risiko für die persönlichen Rechte und Freiheiten** zur Folge hat (Abs. 1);
  - Zeitrahmen: unverzüglich
- Der Mindestinhalt der Benachrichtigung richtet sich nach den in Art. 33 Abs. 3 lit. b, c, d DS-GVO genannten Informationen und Maßnahmen (Abs. 2).
- Ausnahme: Vorliegen eines **Befreiungsgrundes** (Abs. 3)
  - wenn <u>vorher</u> geeignete technische und organisatorische Sicherheitsvorkehrungen (z.B. Verschlüsselung) getroffen wurden *oder*
  - durch <u>nachfolgende</u> Maßnahmen die Beseitigung des hohen Risikos für die Rechte und Freiheiten der Betroffenen sichergestellt wurde *oder*
  - dies mit unverhältnismäßigem Aufwand verbunden wäre.
  - → dann öffentliche Bekanntmachung zur Information der Betroffenen.

Meldepflichten

BLD
BACH LANGHEID DALLMAYR

Meldepflichten bei Verletzung des Schutzes personenbezogener Daten

- Mindestinhalt (Abs. 3):
  - Art der Verletzung des Datenschutzes, soweit möglich mit Angabe der Kategorie und der ungefähren Zahl der betroffenen Personen, Datenkategorien und personen-bezogenen Datensätzen (lit. a),
  - Namen und Kontaktdaten des Datenschutz-Beauftragten (lit. b),
  - Beschreibung der wahrscheinlichen Folgen (lit. c),
  - Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen (lit. d),

→ Bereitstellen der Informationen ist **auch schrittweise** möglich (Abs. 4).

- **Neu:** Dokumentationspflicht (Abs. 5):
  - **Alle etwaigen Verletzungen des Schutzes personenbezogener Daten** sind unter Beschreibung aller im Zusammenhang mit der Verletzung stehenden Fakten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen **zu dokumentieren;**

  → **Zweck:** Ermöglicht die Überprüfung der Aufsichtsbehörde, ob die Meldepflicht eingehalten wurde (Art. 31 Nr. 4).

Meldepflichten

Fazit:

- **Neu:** Unabhängig von den betroffenen Daten und der Art der Daten-schutzverletzung werden **Informationspflichten durch jedes personen-bezogene Datum ausgelöst** (auch unbefugter Zugriff innerhalb der verantwortlichen Stelle!).
- **Neu**: Schwellen bei der Risikoabwägung bzgl. einer Meldung werden gesenkt
  - „einfaches“ Risiko reicht (keine schwerwiegende Beeinträchtigung)
  - die Interessen jeder natürlichen Person sind zu berücksichtigen (nicht nur die des Betroffenen, z.B. des Kunden)
- **Neu:** Konkrete Fristvorgaben für Meldungen an Aufsichtsbehörden

→ Die Meldepflichten stellen für Unternehmen einen **nicht unerheblichen Mehraufwand** dar. Sie sind aber **auch in der Beratungspraxis** zwingend zu beachten (s. Folien zu Rechtsfolgen bei Verstößen)

Agenda

- Einführung
- Anwendbarkeit, Rechtsbehelfe, Haftung und Sanktionen
- Einwilligung
- Berechtigtes Interesse
- Benachrichtigungspflichten
- Meldepflichten bei Verstößen gegen DS-GVO
- **Kundenkontakt und Grundsätze „privacy by design“ und „privacy by default“**
- Dokumentationspflichten

Technischer Datenschutz

BLD
BACH LANGHEID DALLMAYR

Art. 24 „Verantwortung des Verantwortlichen“

- Dokumentation
- Risikobasierter Ansatz
- Technische und organisatorische Anforderungen

Sicherheit der Verarbeitung (Art. 32 DSGVO)

- Vgl. zu § 9 BDSG a. F.
- ***Stand der Technik***, Implementierungskosten, Art, Umfang, Umstände, Zwecke der Verarbeitung, Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen = ***ein dem Risiko angemessenes Schutzniveau***

Geeignete technische und organisatorische Maßnahmen (Art. 25 DSGVO)

- Sicherstellung Datenschutzgrundsätze
- Datenschutzfreundliche **Voreinstellung** (Privacy by Default, Art. 25 Abs. 2)
- Datenschutz durch **Technikgestaltung** (Privacy by Design)
- Sanktionsbewehrte Pflicht, nicht nur Zielvorgabe!

Privacy by Design and Privacy by Default

BLD
BACH LANGHEID DALLMAYR

Art. 25 DSGVO

- „Privacy by Default“
  - z. B. Privatsspähre-Einstellungen; kein „opt-out“
- „Privacy by Design“
  - Bereits zu beachten bei **Planung und Konzeption** eines technologischen Systems, d. h. der Mittel der Verarbeitung
  - Grundsätze der Transparenz, Datenminimierung, Integrität und Vertraulichkeit (z. B. Verschlüsselung, hierzu sogleich)
  - Rechenschaftspflicht (Dokumentation der Vorgänge durch datensparsames Logging)
  - Umfang anhand **Stand der Technik**, Kosten und Risikoanalyse

→ **Zentrale Frage** ist stets: entsprechen die angewandten Systeme und Routinen dem aktuellen Stand der Technik (Praxisbeispiel: ROM-Speicher und Löschungspflicht)?

Privacy by Design and Privacy by Default

BLD
BACH LANGHEID DALLMAYR

Praxisbeispiel: E-Mail-Verkehr

- Verschlüsselung als Pflicht?
  - Sächsicher Landesdatenschutzbeauftragter hat in aktuellem Tätigkeitsbericht auf die Pflicht zur Verschlüsselung bei E-Mails von Berufsgeheimnisträgern (§ 203 StGB) hingewiesen, **wenn** diese sensible personenbezogene Daten enthalten.
  - Bislang in Anlage zu § 9 BDSG Verpflichtung zur Umsetzung „geeigneter technischer und organisatorischer Maßnahmen“.
  - Schutzziele des Datenschutzes (§ 9 BDSG) bei E-Mail erfüllt?
    - Vertraulichkeit: E-Mail darf nicht durch Unbefugte gelesen werden können → wohl (-) da E-Mail nach Aufsichtsbehörden vergleichbar zu einer „Postkarte“
    - Authentifizierung → Identitätsbeweis nicht zu führen
    - Integrität: Nachricht darf während der Übermittlung nicht von Unbefugten verändert werden → Derjenige der Zugriff auf Transportknotenpunkt hat, kann sie verändern
    - Verbindlichkeit → Es ist nicht möglich rechtssicher nachzuweisen, dass E-Mail versendet und empfangen wurde

Privacy by design and privacy by default

BLD
BACH LANGHEID DALLMAYR

E-Mail – Verschlüsselung aus datenschutzrechtlicher Sicht

- Arten der Verschlüsselung
  - **Symmetrische Verschlüsselung** (z. B. IDEA) = Empfänger und Absender verwenden denselben Schlüssel
  - **Asymmetrische Verschlüsselung** = jeder Nutzer erzeugt unter Einbindung Zertifizierungsstelle sein eigenes Schlüsselpaar (aus öffentlichem und privatem Schlüssel). Der private Schlüssel kann ein mit dem öffentlichen Schlüssel (dieser muss dem anderen bekannt sein) verschlüsseltes Dokument öffnen.
- **PKI und Digitale Signatur** (z. B. S/MIME und PGP bzw. GPG) als Ende zu Ende Verschlüssellung
- **TLS** als reine „Transportverschlüsselung“ (keine Ende-zu-Ende Verschlüsselung)
- Aufsichtsbehörden verlangen „Ende-zu-Ende Verschlüsselung“ trotz **fehlender praktischer Verbreitung**

Privacy by design and privacy by default

BLD
BACH LANGHEID DALLMAYR

- **Verschlüsselung nach DS-GVO?**
  - Verschlüsselung als Beispiel in Art. 32 DS-GVO ausdrücklich genannt, allerdings nicht in jedem Einzelfall zwingend geboten (vgl. Martini in Paal/Pauly, DS-GVO BDSG Art. 32 Rn. 34). **Risikoklassifizierung erforderlich!**
  - Übermittlung personenbezogener Daten per E-Mail nach verbreiteter Auffassung nur verschlüsselt.
  - Abhängig von Risikoklasse: TLS; Ende-zu-Ende (PGP); Signatur
  - Lösung Internetpostfach zur Übermittlung in Textform?
    - EuGH NJW 2017, 871 (BAWAG/VKI) zu Kundenmailbox und E-Banking: Einsehbarkeit auf angemessene Dauer sowie unveränderte Wiedergabe, ohne dass der Inhalt durch den Zahlungsdiensteleister oder Admin einseitig geändert werden kann
    - Empfänger muss informiert werden, dass Information auf Webseite verfügbar

Privacy by design and privacy by default

- Einwilligung in die unverschlüsselte E-Mail Korrespondenz?
  - Nach richtiger Auffassung: ja, da gerade Ausdruck der informationelle Selbstbestimmung des Individuums.
- **Aber:**
  - Mindestens TLS- Verschlüsselung muss immer gewährleistet sein; Verzicht nach Auffassung BayLDA nicht zulässig (!)
  - Bei Gesundheitsdaten nach BayLDA Einwilligung zur Verwendung lediglich von TLS denkbar; andere Aufsichtsbehörden abweichend !?
  - Voraussetzung ist umfangreiche Einwilligungserklärung unter Hinweis auf Risiken etc.
  - Kein solcher Verzicht bei Kommunikation verantwortlicher Stellen untereinander!

Privacy by design and privacy by default

BLD
BACH LANGHEID DALLMAYR

Möglichkeiten einer Zertifizierung

- Zertifizierung nach Art. 42, 43 DS-GVO ausdrücklich vorgesehen
  - *… dienen nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsdatenverarbeitern eingehalten wird,* befreien aber nicht von Aufsichtsmaßnahmen und Einhaltung
  - Erteilung durch **Zertifizierungsstellen** nach Art. 43 oder durch die **zuständige Aufsichtsbehörde** (Art. 42 Abs. 4 DS-GVO) anhand vom Ausschuss genehmigter Kriterien.
  - Widerrufliche Erteilung für max. 3 Jahre mit Verlängerungsoption.
- Zertifizierungsverfahren in öffentlichem Register
- ISO 27001? …DSK: „… *decken nur einen Teilbereich des Datenschutzes ab und haben mitunter auch die betroffenen Personen mit ihren Rechten und Freiheiten nicht im Mittelpunkt der Betrachtung*.“

Privacy by design and privacy by default

Deutsche Akkreditierungsstelle GmbH

↓

Aufsichtsbehörden und Befugniserteilung (Kriterien z. B. nach ISO)

↓

Akkreditierung Zertifizierungsstelle

↓

Erteilung der Zertifizierung nach DS-GVO

„Unternehmen, die bereits jetzt Informationssicherheit leben, über ein Datenschutz-Managementsystem verfügen und sich mit der Umsetzung der DS-GVO befassen, erfüllen bereits wesentliche Voraussetzungen. **Kurzpapier DSK Zertifizierung**“

Privacy by design and privacy by default

BLD
BACH LANGHEID DALLMAYR

Möglichkeiten einer Zertifizierung

- DS-GVO nennt explizit Anwendungsbereiche für Nachweis durch Zertifizierung als Faktor
  - *Erfüllung der Pflichten des Verantwortlichen (Art. 24 Abs. 3 DS-GVO)*
  - Erfüllung der Anforderungen an Technikgestaltung (Art. 25 Abs. 1, 2 DS-GVO)
  - Garantien des Auftragsverarbeiter nach Art. 28 Abs. 5, 6 DS-GVO
  - Sicherheit der Verarbeitung (Art. 32 Abs. 3 DS-GVO)
  - Datenübermittlung an ein Drittland (Art. 46 Abs. 2 lit. F)
  - Datenschutzfolgeabschätzung (EW 90)

Agenda

- Einführung
- Anwendbarkeit, Rechtsbehelfe, Haftung und Sanktionen
- Einwilligung
- Berechtigtes Interesse
- Benachrichtigungspflichten
- Meldepflichten bei Verstößen gegen DS-GVO
- Kundenkontakt und Grundsätze „privacy by design“ und „privacy by default“
- **Dokumentationspflichten**

Dokumentationspflichten

Allgemein: Einhaltung der Grundsätze, u.a. in Form von

- Rechtmäßigkeit, Treu und Glauben, Transparenz (Art. 5 Abs. 1 a DS-GVO)
- Zweckbindung (Art. 5 Abs. 1b DS-GVO)
- Datenminimierung (Art. 5 Abs. 1c DS-GVO)
- Richtigkeit (Art. 5 Abs. 1d DS-GVO

muss und sollte durch Unternehmen jederzeit nachgewiesen werden können (vgl. Art. 24 Abs. 1 DS-GVO).

Dokumentationspflichten

BLD
BACH LANGHEID DALLMAYR

Dokumentationspflichten

- Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO:
  - Zusammenfassung der wesentlichen Informationen der Datenverarbeitung (orientiert sich an der Systematik des § 11 BDSG);
  - Kein „Jedermannsverzeichnis“ (anders als § 4g Abs. 2 S. 2 BDSG).
- **Neu**: Ausnahme für Unternehmen bis 250 Mitarbeiter, sofern die Verarbeitung (Art. 30 Abs. 5 DS-GVO):
  - nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt,
  - nur gelegentlich erfolgt oder
  - nicht besondere Datenkategorien (Art. 9) oder Straftaten (Art. 10) einschließt.

Dokumentationspflichten

BLD
BACH LANGHEID DALLMAYR

Dokumentationspflichten (Forts.)

- **Neu**: die Dokumentationspflicht trifft **zukünftig auch den Auftragsverarbeiter** (vgl. Art. 30 Abs. 2 DS-GVO).
- **Neu:** die Einhaltung der Verpflichtungen des Auftragnehmers zu den technisch-organisatorischen Maßnahmen kann durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 Abs. 2 DS-GVO (**vgl. „Code of Conduct“**) oder durch eine Zertifizierung nach Art. 42 DS-GVO nachgewiesen werden.

  → **Rechtsfolge** CoC: Selbstbindung Verwaltung; Nachweiserleichterungen.
- Verhältnis von zwischen Verhaltensregeln und Zertifizierung komplementär zu sehen, d.h. Kombination denkbar, um durch Zertifikat zugleich Einhaltung bestimmter Verhaltensregeln zu demonstrieren (vgl. von Braunmühl, in: BDSG/DGSVO, 2. Aufl. 2016, Art. 40 Rn. 8)

→ **Fazit:** Dokumentation aller Verarbeitungen (z.B. Erhebung bei Betroffenen / Nicht-Betroffenen; Datenerfassung/ Speicherung; Einwilligungen; Bestandbearbeitung; Übermittlung an Dritte; Verabreitung im Konzern; Löschen) sinnvoll!

Vielen Dank für
Ihre Aufmerksamkeit.

Alle Inhalte dieser Präsentation sind urheberrechtlich geschützt. Das Urheberrecht liegt bei BLD Bach Langheid Dallmayr Rechtsanwälte Partnerschaftsgesellschaft mbB. Jede Verwertung, Nachdruck, Vervielfältigung einschließlich Speicherung und Nutzung auf optischen und elektronischen Datenträgern, die nicht ausdrücklich vom Urhebergesetz zugelassen ist, bedarf der vorherigen Zustimmung der Partnerschaftsgesellschaft. Die Zustimmung zum internen Gebrauch beim Mandanten ist in der Übersendung dieser Präsentation zu sehen. Diese Präsentation ist vertraulich zu behandeln und nicht – auch nicht dem wesentlichen Inhalt nach – an Dritte weiterzugeben, es sei denn, die Partnerschaftsgesellschaft hat sich damit in Textform einverstanden erklärt.

Zum Referenten

Dr. Tobias Britz
Rechtsanwalt I Partner

Theodor-Heuss-Ring 13-15
50668 Köln
Telefon: 0221/944027-971
britz@bld.de

TÄTIGKEITSBEREICHE

- Betriebliche Altersversorgung
- Lebensversicherung
- Öffentliche Zusatzversorgung
- Datenschutzrecht
- Aufsichtsrecht
- Insolvenzrecht

WERDEGANG

2000 – 2008	Studium an den Universitäten Bonn und Köln; Referendariat in Köln
seit 2009	Rechtsanwalt bei BLD
2011	Promotion am Institut für Versicherungsrecht der Universität zu Köln bei Prof. Dr. Rolfs (Die Erhebung personenbezogener Gesundheitsdaten durch Versicherungsunternehmen)
seit 2017:	Partner bei BLD

Standorte

Köln

Theodor-Heuss-Ring 13-15 | 50668 Köln
Tel +49 221 944027-0
Fax +49 221 944027-7

München

Karlstraße 10 | 80333 München
Tel +49 89 545877-0
Fax +49 89 545877-77

Frankfurt/Main

Stephanstraße 3 | 60313 Frankfurt/Main
Tel +49 69 920740-0
Fax +49 69 920740-40

Berlin

Kaiserin-Augusta-Allee 104-106 | 10553 Berlin
Tel +49 30 886269-0
Fax +49 30 886269-29

Karlsruhe

Reinhold-Frank-Str. 58 | 76133 Karlsruhe
Tel +49 721 869776-0
Fax +49 721 869776-20

BLD International

Einzelheiten zu BLD International finden Sie unter:
http://www.bld.de/weltkarte.html