Datenschutz in Beratung, Supervision und Coaching

Hinweis: Der Foliensatz enthält urheberrechtlich geschütztes Material und darf nur zu internen Schulungszwecken genutzt werden. Der Auftraggeberin werden einfache Nutzungsrechte eingeräumt.

Was Sie heute lernen sollen:

Worum es ***nicht*** geht:
Es geht nicht darum, alle relevanten Paragrafen zu kennen und (auswendig) zu lernen.

Worum es geht:
1. Sie sollen verstehen, wie vertrauliche Kommunikation zwischen Ratsuchenden und Fachkraft gestaltet sein muss, damit sie gesetzeskonform erfolgt.

2. Sie sollen die Bedeutung wichtiger Begrifflichkeiten des Datenschutz kennen und auf das eigene praktische Handeln übertragen können.

Grundsätzlich gilt:
Wer personenbezogene Daten (pbD) erheben, speichern und verarbeiten will, darf dies nur

- wenn die Betroffenen der Erhebung, Speicherung und Verarbeitung explizit zustimmen,
- wenn eine gesetzliche Vorschrift zur Erhebung und Speicherung verpflichtet (z.B. im Zuge der Beantragung staatlicher Leistungen),
- bzw. wenn ohne die Erhebung personenbezogener Daten die angebotene Leistung nicht erbracht werden kann.

Wann handelt es sich bei Daten um pbD?

In Art. 4, Absatz 1 DSGVO heißt es:

„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.“

Mit anderen Worten: alles, was wir von den Ratsuchenden wissen müssen, sind im Sinne der DSGVO pbD.

Und warum zusätzlich das Bundesdatenschutzgesetz?

Bezüglich der Definition „pbD“ (§ 46 BDSG) ist der Wortlaut identisch, das BDSG regelt primär die nationale Umsetzung. In § 1 BDSG heißt es:

„Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes, öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie a) Bundesrecht ausführen oder b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt. ***Für nichtöffentliche Stellen*** gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.“

Zum Rollenverhältnis:

A = Agens erhebt/verarbeitet, ***B = Betroffene/r*** „erleidet“ die Datenerhebung.

A ist ***verantwortlich***, dass die Schutzbedürfnisse („informationelle Selbstbestimmung“, BfG 1983) von B durch die Erhebung der pbD nicht gefährdet werden, d.h. dass die Erhebung der pbD im Rahmen der geltenden gesetzlichen Bestimmungen erfolgt
(***= Datenschutz/Vertraulichkeit***).

A ist verpflichtet, ein adäquates Schutzniveau für die erhobenen Daten zu garantieren und die dazu notwendigen technischen und organisatorischen Maßnahmen (TOMs) zu ergreifen
(***= Datensicherheit = Datenintegrität/Schutz vor Verlust, Missbrauch***).

Bei welchen (typischen) Gelegenheiten werden pbD erhoben?

- Beim Ausfüllen eines Beratungsvertrages (Kontrakts),
- beim Ausfüllen eines Kontaktformulars auf einer Website,
- bei der Registrierung auf einer Website,
- beim Surfen im Internet, dem Besuch einer Website, der Nutzung einer Online-Dienstleistung (IP-Adresse, First-Party-Cookies, http-Cookies),
- Beim Führen eines Terminkalenders
- Beim Erstellen von (Sitzungs-)Protokollen/Protokollen (es handelt sich um pbD, auch wenn den Fotos keine Namen zugeordnet sind – warum?)

Frage:

Wann werden datenschutzrechtliche Normen relevant und welche?

Welche Rechtsvorschriften sind zu beachten, wenn es zur Erhebung personenbezogener Daten kommt?

aus beruflichen Gründen (z.B. vertragliche Regelungen)	DSGVO
in öffentlichen und nichtöffentlichen Stellen	BDSG (2018)
bei Durchführung sozialstaatlicher Aufgaben (Subsidiarität)	SGB I / SGB X

Flankiert werden die datenschutzrechtlichen Normen (DSGVO/BDSG) durch den Artikel 8 der europäischen Menschenrechtskonvention (EMRK): ***informationelle Selbstbestimmung.***

Wie lautet die datenschutzrechtliche Leitnorm?

Die datenschutzrechtliche Leitnorm lautet:

Die Verarbeitung personenbezogener Daten ist verboten, es sei denn, sie ist erlaubt.

So genanntes „Verbotsprinzip mit Erlaubnisvorbehalt“.

Die beiden ***Grundprinzipien*** sind:

1. Datenvermeidung und Datensparsamkeit,
2. Zweckbindung und Rechtmäßigkeit.

Frage:

Werden strafrechtliche Normen relevant?

Strafrechtliche Auflagen gelten für alle im § 203 StGB genannten Berufsgruppen:

a) Angehörige eines Heilberufes (Arzt*in, Heilpraktiker*in etc.)	Abs. 1, Satz 1
b) Berufspsycholog*in mit staatlicher anerkannter Abschlussprüfung	Abs. 1, Satz 2
c) Mitarbeitende in einer anerkannten Ehe-, Familien-, Erziehungs- oder Jugendberatungsstelle oder Suchtberatungsstelle	Abs. 1, Satz 4
d) Mitarbeitende in einer anerkannten Schwangerenkonfliktberatungsstelle	Abs. 1, Satz 5
e) Staatliche anerkannte Sozialarbeiter*innen/Sozialpädagog*innen	Abs. 1, Satz 6

Die Norm des ***§ 203 StGB*** (Strafgesetzbuch) verpflichtet die dort genannten Berufsgruppen bzw. Mitarbeitenden in den genannten Einrichtungen

einseitig

zur Wahrung anvertrauter Privatgeheimnisse (so genannte Schweigepflicht). Angehörige dieser Berufsgruppen sind **Berufsgeheimnisträger*innen**.

Eine (einseitige) Entpflichtung (Haftungsausschluss, Disclaimer) ist rechtsunwirksam!

Von der Verschwiegenheit entpflichtet sind Berufsgeheimnisträger*innen im Falle eines rechtfertigenden Notstandes (z.B. § 138 StGB, in Verbindung mit § 34 StGB).

Was bedeutet diese Auflage für die (Beratungs-)Praxis?

Berufsgeheimnisträger*innen dürfen nur solche Kommunikationswege wählen, die vor einer (zufälligen/billigenden/fahrlässigen) Offenbarung des Privatgeheimnisses schützen.

Zulässige Kommunikationswege sind vor allem ***gesetzlich geschützte*** Übermittlungswege wie beispielsweise der Postweg oder das Telefon, die durch ein Gesetz (Art. 10 GG, Brief-, Post- und Fernmeldegeheimnis, § 88 TKG) geschützt sind.

Kommt es hier zu Verstößen, können dafür nicht die Nutzenden dieser Dienste verantwortlich gemacht werden, sondern die Person, die den Verstoß begeht.

Zulässig sind auch Wege, die eine (zufällige/billigende/fahrlässige) Offenbarung durch geeignete und robuste ***technische Maßnahmen*** verhindern.

Exkurs: Sichere Übermittlungswege

Ganz allgemein sind elektronisch übermittelte Informationen geschützt, wenn technische Maßnahmen verhindern, dass die übermittelten Informationen von Unbefugten eingesehen, gespeichert (verarbeitet) und verfälscht werden können (Datensicherheit und Datenintegrität).

Eine sichere elektronische Datenübermittlung setzt eine Ende-zu-Ende-Verschlüsselung voraus, oder anders formuliert: auf dem Weg von A (Sender) zu B (Empfänger) dürfen die gesendeten Informationen zu keinen Zeitpunkt unverschlüsselt vorliegen / weitergegeben werden.

Exkurs: Sichere Übermittlungswege

Frage:
Bietet eine eMail eine sichere Form der Übermittlung?

Stellen social-media-Dienste wie Skype, Facebook etc. eine sichere Form der Übermittlung dar?

Wie verhält es sich mit Zoom, Treema, Signal etc.?

Schweige**pflicht** (§ 203 StGB)

1) Seit dem 30.10.2017 ist der Einbezug Dritter straffrei möglich, wenn der Dritte an der ***ordnungsgemäßen*** Ausübung der Tätigkeit mitwirkt (direkt mitwirkende Gehilfen, auch: Cloud-Dienstleister).

2) Der Einbezug an der Berufsausübung beteiligter Dritter ist nur unter ***strengen Voraussetzungen*** zulässig, d.h. die Verantwortliche schreibt den Dritten vor, wie mit den erhobenen Daten umzugehen ist und teilt mit, welche berufs-/straf-rechtlichen Auflagen auf den Dritten übergehen
=> Vertrag zur Datenverarbeitung im Auftrag (AV-Vertrag).

3) Eine Einwilligung der Betroffenen (Klienten) in den Einbezug Dritter ist ***nicht*** erforderlich, jedoch aus Gründen der Transparenz empfohlen.

Näheres unter https://dg-onlineberatung.de/datenschutz-faq/

Schweige**pflicht** (§ 203 StGB)

Problem:
Derzeit gibt es keine Aufzählung auslagerungsfähiger Tätigkeiten, die Psychologinnen oder Sozialpädagoginnen straffrei auslagern dürfen.
=> ***Rechtsunsicherheit.***

Unstrittig an Dritte ***auslagerungsfähige Tätigkeiten*** sind gemäß Neufassung des § 203 StGB:

- Einrichtung, Betrieb, Wartung – einschließlich Fernwartung – und Anpassung informationstechnischer Anlagen, Anwendungen und Systeme aller Art,
- Bereitstellung von informationstechnischen Anlagen und Systemen zur externen Speicherung von Daten,

soweit der mitwirkende Dritte vorab (also vor Ausführung der Tätigkeiten) explizit (d.h. schriftlich) auf das Datengeheimnis ***verpflichtet*** wurde.
Kommt es zur Prüfung, muss der korrekte Einbezug Dritter nachgewiesen werden (z.B. Nachweis schriftlicher Verpflichtung auf das Datengeheimnis etc.).

Entbindung von der Schweigepflicht

Ratsuchenden können der Weitergabe ihrer offenbarten Daten für bestimmte Zwecke zustimmen, d.h. ***Einwilligungen gelten*** nur für einen ***bestimmten*** Fall (Art. 4, Absatz 11), woraus umgekehrt folgt: „***pauschale***“ Einwilligungen sind rechtswidrig.

Für die Praxis bedeutet dies:

Jede Einwilligung muss ausweisen, ***welche*** Daten ***warum*** an ***wen*** weitergegeben werden sollen.

Einwilligungen sind immer ***schriftlich*** zu erteilen, um im Konfliktfall Rechtsunsicherheiten vorzubeugen.

Gruppenprotokolle dürfen an die TN nur dann verteilt werden, wenn ***alle***(!) zugestimmt haben.

Wichtig: auch bei Einwilligung in die Weitergabe sind Berufsgeheimnisträger*innen weiterhin verpflichtet, datensichere Übermittlungswege zu nutzen!

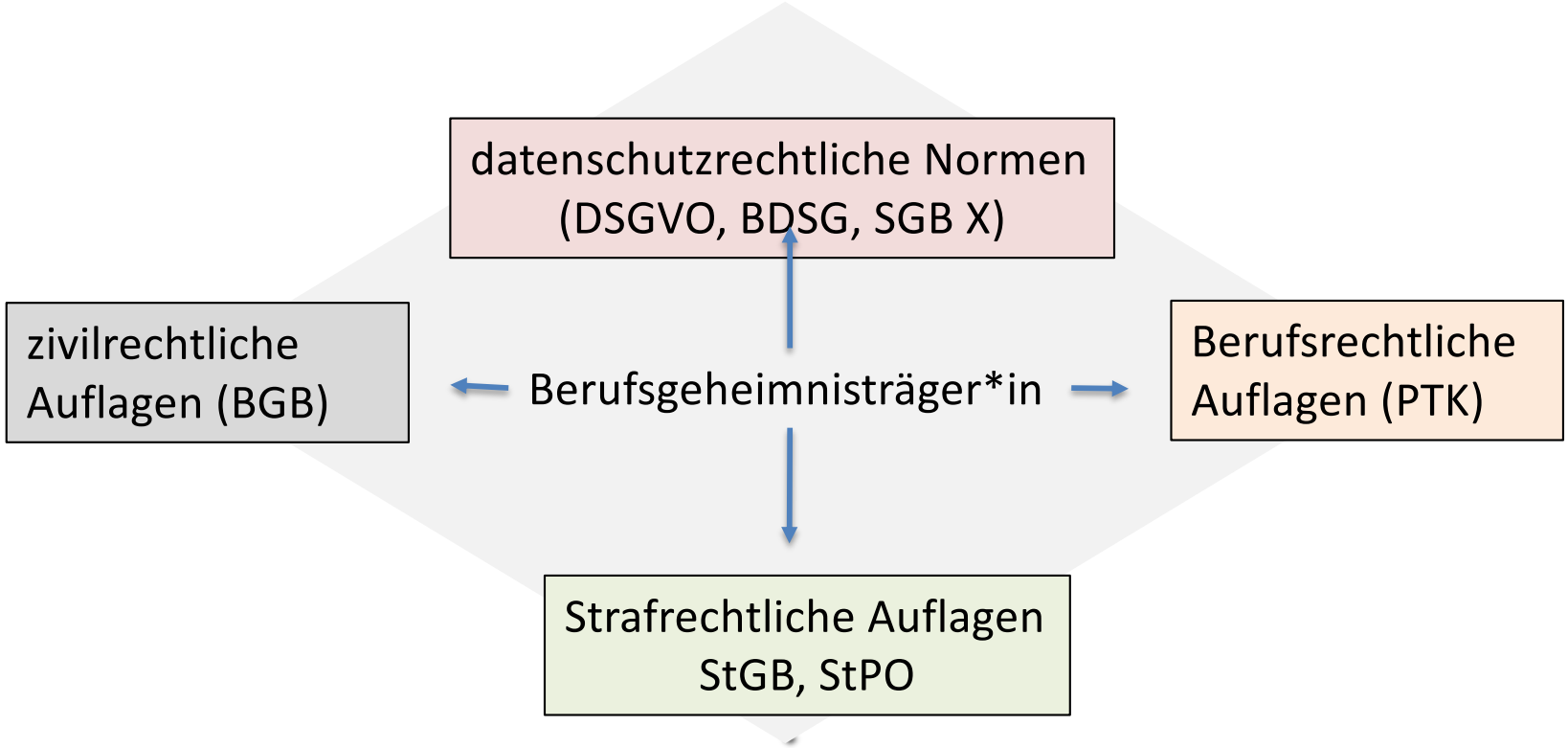
Meldepflicht / zwingende Offenbarung

Keine Regel ohne Ausnahme:

Wer im Rahmen einer (Online)-Kommunikation von einer geplanten Straftat im Sinne der Vorschriften des ***§ 138 StGB*** erfährt, ist zur ***Anzeige verpflichtet***, sofern die angekündigte Tat glaubhaft erscheint und durch geeignete (beraterische) Maßnahmen nicht abgewendet werden kann (vergl. § 139 StGB).

Im Rahmen dieser Meldepflicht sind beispielsweise die IP (Internet-Protocol-Adresse), sofern vorhanden, der Nutzername (Realidentität oder Nickname) oder andere Hinweise (Hoster, Zeitstempel der Meldung, Referrer (d.h. die Angabe, von welcher Website der Aufruf dieser Website erfolgte) etc.) der örtlich zuständigen Staatsanwaltschaft zu melden (ersatzweise Polizeidienststelle, Landeskriminalamt).

Rechtliches Spannungsfeld, in dem psychosoziale/heilkundliche Beratung/Coaching/Supervision stattfindet



Frage:

Was bedeutet „***berechtigt***“ verarbeiten?

Die Verarbeitung erfolgt berechtigt, wenn die pbD

1. ausschließlich zum Zweck einer sachgerechten/fachgerechten Durchführung der beruflichen Tätigkeit erhoben werden (Kontrakt, Vertragserfüllung, Durchführung der Beratung),
2. erhoben werden in Verbindung mit der Wahrnehmung einer öffentlichen (staatlichen) Aufgabe (z.B. Durchführung einer subsidiären Leistung).
3. erhoben werden zum Schutz lebenswichtiger Interessen der betroffenen (betreuten) Person,
4. nur dann weitergegeben (übermittelt) werden, wenn Rechtsnormen dies vorschreiben (z.B. Leistungserbringung im Rahmen des SGB etc.).

Wichtig:
Die Erhebung persönlicher Daten setzt die explizite ***Einwilligung*** der betroffenen Person voraus (Ausnahme: Erhebungspflicht).

Besondere Kategorien (Art. 9 DSGVO)

Im Zusammenhang mit Beratung/Coaching /Supervision kommt es regelmäßig zur Erhebung ***besonderer Kategorien*** personenbezogener Daten wie

- rassische oder ethnische Herkunft,
- religiöse oder weltanschauliche Überzeugungen,
- Gesundheitsdaten,
- Daten zur sexuellen Orientierung,
- Daten zum Sexualleben etc.

Gemäß der Vorschriften des Art. 9, Absatz 3 DSGVO dürfen diese Daten nur von **Fachpersonal** verarbeitet werden, das dem **Berufsgeheimnis** unterliegt.

Empfohlene Verfahrensweise bei der Erhebung „besonderer Kategorien“

1) ***Pseudonymisierung*** so frühzeitig wie möglich: Art. 5 Absatz 1, Satz c, Art. 25 DSGVO in Verbindung mit § 48 BDSG.

2) ***Logisch getrennte*** Erfassung der Personenmerkmale der Ratsuchenden und der "persönlichen Aufzeichnungen“ (Handakte) der Fachkraft (Art 25, Absatz 2).

Durch die Trennung in „offizielle“ und „persönliche“ Datenbestände (Offizialakte/Verwaltungsakte versus Handakte, Ziffer 8 der Anlage zu § 9 BDSG) kann die Fachkraft verhindern, dass bei einem Herausgabeverlangen des Gerichts die persönlichen Aufzeichnungen zusammen mit der Offizialakte herausgegeben werden müssen.
Empfehlung: persönliche Aufzeichnungen am besten ‚old school‘ auf Papier (z.B. Notizheft, separat gelagerte Aktenmappe etc.).

Umsetzung der Vorschriften in die Praxis

Mit wem muss ein AV-Vertrag geschlossen werden?
(Art. 4 in Verbindung mit Art. 28 DSGVO)

Mit jeder Person/Institution/Firma, die als weisungsgebundener „Dritter“ in die Leistungserbringung einbezogen ist („Innenverhältnis“).

Hinweise für den Einbezug Dritter mittels AV-Vertrag:

Unbedingt zu empfehlen ist die ***Trennung*** der Dienstleistungen in
1. Webhoster (eigene Website) und
2. Hoster für die Online-Beratung (Branchensoftware).

<u>Grund für die Trennung:</u>
Für den Einbezug eines Webhosters (z.B. Betrieb der eigenen Website) gelten niedrigere Verpflichtungsgrade als für den Einbezug eines Herstellers einer Branchensoftware (= Online-Beratungssoftware). Auf Letzteren gehen die berufs- und strafrechtlichen Verpflichtungen der Berufsgeheimnisträger*in über.

Umsetzung der Vorschriften in die Praxis

Verzeichnis der ***Verarbeitungstätigkeiten*** (Art. 30 DSGVO / § 70 BDSG):

- Name / Kontaktdaten der Verantwortlichen
- Verarbeitungs***zwecke***,
- ***Rechtsgrundlagen*** der Verarbeitung,
- Beschreibung der ***Kategorien*** personenbezogener Daten,
- Beschreibung der ***Kategorien*** von (behandelten) Personen (Definition der Klientel),
- Löschfristen,
- (technische) Maßnahmen zur Löschüberwachung oder Anonymisierung / Pseudonymisierung der Daten,
- Beschreibung der ***TOMs*** gemäß Art. 32 DSGVO und § 64 BDSG (=> Beschreibung des **Schutzniveaus**).

Frage:

Was bedeutet Zweckbindung?

Definition „Zweckbindung“

Zwecke sind ***Gründe***, die angeben, weshalb pbD erhoben werden (dürfen).

Zwecke müssen ***vor*** (!) der Verarbeitung festgelegt und benannt werden und haben ***bindende*** Wirkung (=> Zweckbindung). Nachträgliche Zweckänderungen sind rechtsunwirksam, wenn nicht ***alle*** Betroffenen der Zweckänderung zustimmen.

Zwecke müssen eindeutig (formuliert) sein.

Sollen personenbezogene Daten zu anderen Zwecken verarbeitet werden, bedarf es eines Rechtfertigungsgrundes (rechtliche Verpflichtung, Zustimmung der Betroffenen, Erfordernisse aus der Leistungserbringung etc.).
So ist z.B. die Weitergabe personenbezogener Daten an Dritte (auch wenn verpflichtend) ein „anderer“ Zweck und bedarf der (expliziten / schriftlichen) Einwilligung der Betroffenen.

Anforderungen an die Zweckbindung (Art. 5)

Es gilt:

1) Keine Verarbeitung ***außerhalb*** der mitgeteilten Zwecke (ausschließlich zu Beratungszwecken erhobene Daten dürfen nicht für Marketingzwecke verwendet werden).

2) Keine Verarbeitung pbD nach der zugesagten ***Löschung*** (Art. 17 DSGVO), sofern Daten aus vertraglichen Pflichten (z.B. Steuerrecht) weiterhin aufbewahrt (gespeichert) werden müssen.
   => ***Löschung*** bedeutet in diesem Fall ***Sperrung***.

<u>Rechtliche Präzisierung ausstehend:</u>
Wie wird die eingeschränkte Verarbeitung (Einschränkung) bzw. Nichtverarbeitung (Sperre) nachgewiesen (durch welche technisch-organisatorische Maßnahmen / TOMs) (vergl. Art 18, Absatz 2)?

Frage:

Wie wird das Schutzniveau nachgewiesen?

Nachweis der Einhaltung der Vorschriften

Wer prüft?

Die Aufsichtsbehörden (Landesdatenschutzbehörde) überprüfen auf Grundlage der Bestimmungen des § 38 BDSG sowie in Übereinstimmung mit dem Landesrecht die Einhaltung der datenschutzrechtlichen Bestimmungen bei nicht-öffentlichen Stellen.

Wann kommt es zu einer Überprüfung?

Entweder als Folge einer Meldung an die Behörde (z.B. durch Ratsuchende) oder im Rahmen routinemäßiger Überprüfungen, etwa im Zusammenhang mit bekannt gewordenen Sicherheitslücken bei Software (z.B. Wordpress) oder dem (verbotenen, aber verbreiteten) Einsatz von Tracking-Software.

Nachweis der Einhaltung der Vorschriften

Wie wird die Einhaltung datenschutzrechtlicher Vorgaben nachgewiesen?

Der Nachweis erfolgt anhand eines Verarbeitungsverzeichnisses, das die organisatorisch-technischen Maßnahmen (**TOM**s) listet, die zur Etablierung des Schutzniveaus ergriffen worden sind (§ 64 BDSG).

Der konkrete Inhalt des Verarbeitungsverzeichnisses ist weder in der DSGVO noch im BDSG ausdrücklich (d.h. im Klartext) geregelt.

Für die Praxis haben sich aber – in Zusammenarbeit mit den Aufsichtsbehörden der Länder - folgende Kriterien (**Checklisten**) als hilfreich erwiesen.

Checkliste „Verarbeitungsverzeichnis “

Hinweise zum Verzeichnis von Verarbeitungstätigkeiten

https://www.datenschutzzentrum.de/uploads/dsgvo/Hinweise-zum-Verzeichnis-von-Verarbeitungstaetigkeiten.pdf

Muster zum Verarbeitungsverzeichnis Auftragsverarbeiter
Download Muster zum Verarbeitungsverzeichnis Auftragsverarbeiter (PDF, 306KB)

Muster zum Verarbeitungsverzeichnis Verantwortlicher
Download Muster zum Verarbeitungsverzeichnis Verantwortlicher (PDF, 232KB)

Quelle:
https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/Muster_Verzeichnis_Verarbeitungstaetigkeiten.html

Datenpanne – was tun?

An wen ist zu melden und wie schnell?

Kommt es als Folge einer Datenpanne zur (ungewollten) Veröffentlichung pbD, muss der/die Verantwortliche den Vorfall der zuständigen Landesbehörde **innerhalb 72 Stunden** melden (Art. 33/34 DSGVO und
§ 42a BDSG).

Kann auf eine Meldung verzichtet werden?

Auf eine Meldung darf nur dann verzichtet werden, wenn der/die Verantwortliche nachweisen kann, dass die Betroffenen durch die Datenschutzverletzung weder gegenwärtig noch zukünftig einen physischen, materiellen oder immateriellen Schaden (z.B. Identitätsdiebstahl oder -betrug, finanzielle Verluste, Diskriminierung, Rufschädigung) erleiden.

Datenpanne – was tun?

Was ist zu melden:

Welche Art von Verletzung liegt vor? (Datenverlust, Diebstahl usw.)

In welche Kategorie fallen die Betroffenen? (Ratsuchende, Mitarbeiter)

Wie viele Betroffene gibt es?

Welche Kategorien von Datensätzen sind betroffen?

Welche Folgen zieht die Schutzverletzung nach sich? (z.B. ideelle, finanzielle Nachteile)?

Welche Schutzmaßnahmen wurden ergriffen oder werden noch ergriffen?

Frage :

Was bedeutet Auskunftsrecht?

Checkliste „Auskunftsrecht“ (Art. 15)

1. Information zum Verarbeitungszweck / ***Rechtmäßigkeit,***
2. Mitteilung über die erhobenen Daten-***Kategorien***,
3. Information zu den ***Empfängern*** der erhobenen Daten (sofern Datenübermittlung erforderlich und rechtmäßig),
4. geplante ***Dauer*** der Speicherung,
5. ob und für welche Daten ein Recht auf ***Löschung auf Verlangen*** besteht,
6. Nennung der ***Aufsichtsbehörde*** (Beschwerdestelle),
7. ob zusätzliche Daten zur betroffenen Person bei ***Dritten*** erhoben werden (z.B. Krankenkasse, Arbeitgeber).

Im Falle eines **Auskunftsverlangens** müssen folgende Daten zur Verfügung gestellt:

a) Eine ***Kopie*** der Akte (sofern elektronisch: in gängigem Format, vergl. Art. 15, Absatz 3),
b) eine bereinigte Kopie, wenn die Rechte und Freiheiten ***anderer Personen*** beeinträchtigt würden (Art 15, Absatz 4) => Begründung erforderlich!

Datenschutz als Verhaltenskodex

Niemand von uns kommt auf die Idee, ohne Kenntnis der Straßenverkehrsordnung ein Auto zu lenken. Das kann gut gehen, muss es aber nicht, denn bei einem festgestellten Regelverstoß müssen wir mit Bestrafung rechnen.

Gleiches gilt für den Datenschutz: wer pbD erfasst und verarbeitet muss die einschlägigen „Verkehrs“-Vorschriften für den Umgang mit pbD kennen. Eine Erhebung und Verarbeitung ohne Kenntnis kann gut gehen, muss es aber nicht. Wird ein Verstoß festgestellt, droht Bestrafung!

Heinz Thiery

Geschäftsführer DGOB

thiery@dg-onlineberatung.de

06232/3128633