CORINNA GEKELER

Wellenlängen

Datenschutz nach DSGVO

Jahresfachtagung BAG SB

Kiel, 26.04.2018

Selbstverständnis

Vertrauensvolle Beratung basiert auf

- dem Grundsatz des selbstbestimmten Lebens der Ratsuchenden und
- dem Schutz von ihren Persönlichkeitsrechten.

Beim Datenschutz geht es nicht nur um gesetzliche Verpflichtungen, sondern um das hohe Gut VERTRAUEN.

Grundrecht

Unsere Verfassung schützt das Grundrecht auf

informationelle Selbstbestimmung

Ausgangspunkt für das bisherige Bundesdatenschutzgesetz (BDSG) ist das Urteil des Bundesverfassungsgericht aus 1983 - Volkszählungsurteil

Artikel 1 DSGVO
Gegenstand und Ziele

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

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

(…)

Datenschutz-Grundverordnung (EU) 2016/679

Geltendes Recht in ganz Europa ab **25. Mai 2018**

Öffnungsklauseln ermöglichen es Mitgliedstaaten, nationale Regelungen zu treffen.

So enthält das **BDSG neu** folgende **zusätzliche Regelungen:**

- Art. 37 GVO (Benennung Datenschutzbeauftragte)

  und § 38 BDSG neu
- Art. 83 GVO (Geldbußen)

  und § 43 Abs. 3 BDSG neu

Veränderungen durch DSGVO

- Umfangreichere Dokumentationspflichten zu Risikoeinschätzungen und Datenschutzmaßnahmen
- Höhere Bußgelder und Strafen
- Betroffene können ihre Daten „mitnehmen“
- Strengere Kriterien für den Nachweis einer Einwilligung
- Schweigepflicht erweitert auf Auftragsverarbeiter

173 Erwägungsgründe und 99 Artikel

Kapitel 1 Allgemeine Bestimmungen
Kapitel 2 Grundsätze
Kapitel 3 Rechte der Betroffenen Person
Kapitel 4 Verantwortlicher und Auftragsverarbeiter
Kapitel 5 Übermittlung personenbezogener Daten an Drittländer oder an int. Organisationen
Kapitel 6 Unabhängige Aufsichtsbehörden
Kapitel 7 Zusammenarbeit und Kohärenz
Kapitel 8 Rechtsbehelfe, Haftung und Sanktionen
Kapitel 9 Vorschriften für besondere Verarbeitungssituationen
Kapitel 10 Delegierte Rechtsakte und Durchführungsrechtsakte
Kapitel 11 Schlussbestimmungen

Art. 9
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, 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.

Wichtigster Grundsatz bleibt

Erlaubnisvorbehalt

Den Betroffenen (Klient_innen, Ratsuchende u.a.) gehören alle Daten über sie.

Art. 6: Daten dürfen nur mit ihrer Einwilligung oder auf der Basis einer anderen Rechtsgrundlage erhoben, verarbeitet oder gar an Dritte übermittelt werden.

Artikel 6

Rechtmäßigkeit der Verarbeitung

Die Verarbeitung von Daten ist nur zulässig, wenn eine Einwilligung oder eine andere in dieser Vorschrift normierte Ausnahme vorliegt. Dies ist der Fall, wenn

- die Verarbeitung für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Antrag der betroffenen Person erfolgen;
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt;
- (…)

Artikel 7

Bedingungen für die Einwilligung

- Eine wirksame Einwilligung zur Erhebung, Verarbeitung und Nutzung oder Weitergabe der Daten muss freiwillig erfolgen.

- Sie muss in verständlicher Sprache benennen, zu welchen Zweck welche Daten erhoben, verarbeitet und an wen innerhalb der Beratungsstelle weitergegeben werden dürfen.

- Geht es um eine Einwilligung zur Übermittlung an Dritte, so sind Anlass/Zweck, Datenkategorien, zeitlicher Rahmen und Angaben zur konkreten Zuordnung des Empfängers zu nennen.

- Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

- Es muss immer ein Hinweis zum Widerrufsrecht („jederzeit und ohne Angabe von Gründen“ usw.) enthalten sein, das wirksam umgesetzt werden kann.

- **Pauschale** Einwilligungen sind unwirksam.
  Nur **anlassbezogene** Einwilligung gelten!

Bei sensitiven Daten (Art. 9) muss im Vertrag und in einer evtl. notwendigen Einwilligung ein ausdrücklicher Hinweis auf die Art der Daten erfolgen.

Zweckbindung

Datensparsamkeit: Nur Daten erheben, die für den klar definierten Zweck nötig sind und diese nur so lange wie nötig speichern (Löschfristen).

Datenvermeidung: Daten möglichst anonymisiert oder pseudonymisiert erfassen und nutzen.

Das **Erheben** der Daten hat nach Möglichkeit beim Betroffenen zu erfolgen (Direkterhebung).

Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.

Datenübermittlung an Dritte

Einwilligung oder Schweigepflichtentbindung?

Wer Daten von Ratsuchenden an Dritte übermitteln möchte, braucht dazu

- eine Rechtsgrundlage (über die Ratsuchende z.B. im Beratungsvertrag aufzuklären sind) oder
- eine wirksame Einwilligung (bzw. Schweigepflichtentbindung).

Art. 32 Abs. 4

Verpflichtung auf die Vertraulichkeit

Nach Art. 29 DS-GVO dürfen Beschäftigte (…) personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen (…) verarbeiten, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor.

Ergänzend dazu regelt Art. 32 Abs. 4 DS-GVO, dass der Verantwortliche (…) Schritte unternehmen muss, um sicherzustellen, dass ihnen unterstellte Personen (insbesondere ihre Beschäftigten), die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten (…)

Datenweitergabe

Was dürfen Kolleg_innen einsehen?

Innerhalb einer „funktionierenden Einheit“ spricht man von Datenweitergabe (statt Übermittlung).

Das bedeutet aber nicht, dass alle Mitarbeitenden Zugang bzw. Zugriff auf alle Daten der Ratsuchenden haben dürfen. Dies dürfen sie nur zur Erfüllung ihrer jeweiligen Aufgabe.

So erhält die Verwaltung z.B. nur Zugang zu Bestandsdaten, aber nicht zum Inhalt der Beratung.

In einem Zugriffs- und Rollenkonzept muss festgelegt werden, wer zu welchen Daten Zugang bzw. Zutritt hat. Das gilt für Akten und Dateien.

Es muss für Ratsuchende erkennbar sein, bis wohin der Schutzraum der Beratung reicht und wer zu welchem Zweck Einsicht in die Akte hat.

Aufbewahrungs- und Löschfristen

Grundsatz der Erforderlichkeit:

> Daten werden gelöscht, wenn sie zur Erfüllung der jeweiligen Aufgaben nicht mehr gebraucht werden bzw. wenn das Beratungsverhältnis zu Ende ist.

Neben fachlichen Kriterien zur Aufbewahrung müssen gesetzliche Aufbewahrungsfristen eingehalten werden; zum Beispiel bestimmte Abrechnungsdaten müssen (gesperrt) länger bewahrt werden als der Inhalt der Beratung.

Die Aktenführung ist so zu gestalten, dass sie das Einhalten der Fristen (automatisch) unterstützt.

Weitere Gesetze

DSGVO und BDSG neu gelten neben bereichsspezifischen Gesetzen, wie etwa

- StGB (§203 StGB)
- ÜSchuldStatG
- InsoStatG
- TMG (Website)
- Steuerrecht, Arbeitsrecht, SGB, AsylbLG usw.

Artikel 30
Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder **Verantwortliche** und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben: (…)

(2) Jeder **Auftragsverarbeiter** und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält: (…)

- Bezeichnung (Beratung, Spendenakquise, Personalverwaltung, Website, Mitglieder, Veranstaltungen etc.)
- Verantwortliche
- Zwecke der Verarbeitung
- Rechtsgrundlage (Vertrag, Einwilligung)
- Betroffene
- Datenkategorien (Art. 9, Kontaktdaten, Bankdaten etc.)
- Datenherkunft
- Empfänger der Daten (intern und extern: Beratungsteam, Behörden, Bank, Dienstleister, inkl. Rechtsgrundlagen)
- Lösch- und Aufbewahrungsfristen
- Übermittlung an Drittstaaten (Doodle, Facebook, Software usw.)
- Technisch-organisatorische Maßnahmen (IT-Konzept, Räume etc.)

Technisch-organisatorische Maßnahmen

An mehreren Stellen fordert die DSGVO, angemessene technisch-organisatorischen Maßnahmen (TOMs) zu ergreifen, um Datensicherheit und Datenschutz auf dem erforderlichen Schutzniveau zu gewährleisten.

Bei der Auswahl der Maßnahmen ist die Verhältnismäßigkeit zwischen der Schutzbedürftigkeit der Daten und der Schadenseintrittswahrscheinlichkeit zu berücksichtigen.

Verhältnismäßigkeit der Maßnahmen

Perspektive der Betroffenen

Physischer, materieller oder immaterieller Schaden für natürliche Personen:

- Kontrollverlust über persönliche Daten / Schutz vor Überwachung
- Einschränkung von Persönlichkeitsrechten
- Diskriminierung, Rufschädigung
- Identitätsdiebstahl
- Finanzieller Schaden
- Unbefugte Aufhebung der Pseudonymisierung
- Verlust des Vertrauensverhältnis, der Vertraulichkeit der Beratung

Verhältnismäßigkeit der Maßnahmen

Perspektive der Einrichtung

- Compliance / Gesetze einhalten
- Rufschädigung
- Sicherung der Geschäftsprozesse
- Sicherung IT-Systeme
- Finanzieller Schaden

Matrix zur Risikobewertung

Wahrscheinlichkeit	Auswirkung / Schaden			
	NIEDRIG	MITTEL	HOCH	SEHR HOCH
Sehr wahrscheinlich	gering	mittel	hoch	sehr hoch
Wahrscheinlich	gering	mittel	hoch	hoch
Möglich	gering	gering	mittel	mittel
Unwahrscheinlich	gering	gering	gering	gering

Kapitel 3

Betroffenenrechte

Betroffene müssen beim Zeitpunkt der Erhebung über Zweck, Rechtsgrundlage, Umstände der Verarbeitung und Nutzung ihrer Daten sowie über Ihre Auskunfts- und Beschwerderechte informiert werden.

Sie können Auskunft über alle sie selbst betreffenden Daten bei der Einrichtung verlangen. Die Auskunft muss in verständlicher Sprache, kostenfrei, richtig und umfassend erteilt werden.

Neu ist, dass Ratsuchende ihre Daten auch erhalten können müssen, um sie auf andere Angebote übertragen zu können.

Datenhaltung ist so zu gestalten, dass Betroffene alle ihre Rechte umstandslos wahrnehmen können.

Artikel 35
Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

(…)

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder

(…)

Artikel 28
Auftragsverarbeiter

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

- Maßstab ist das definierte Schutzniveau des Auftragsgebers.
- Der Auftraggeber ist verantwortlich für die vertraglich vereinbarte Verarbeitung.
- Er überprüft die Einhaltung fortlaufend.

Risiken

„*Was soll schon passieren?*“

„*Wer interessiert sich schon für unsere Daten?*“

Bußgelder und Strafen

Nicht erst bei Datenverlust!

Art. 37 + §38 BDSG neu

Beauftragte/r für den Datenschutz (DSB)

- Wer besonders sensible Daten (Art. 9) erhebt, muss eine/n Beauftragte/n für den Datenschutz benennen (Art. 37 Abs 1c).
- Die Person muss über die nötige Fachkunde verfügen, die zu den Anforderungen der Organisation passt.
- Es darf kein Interessenkonflikt bestehen.
- Intern und extern ist gleichwertig.
- DSB ist Ansprechperson für Mitarbeitende, Betroffene und Behörden.

Variante „gemeinsame/r DSB“

DSB der Dachorganisation entwickelt (ggf. zusammen mit AG aus MOs) ein gemeinsames Datenschutz-Regelwerk und Muster-Vorlagen. Denkbar sind:

- Richtlinien / Leitfaden
- Einwilligungen (Muster)
- IT-Standards (ggf. auch Tools)
- Verpflichtung Beschäftigter
- Verträge zur Auftragsverarbeitung
- Verzeichnisse von Verarbeitungstätigkeiten
- Datenschutzfolgenabschätzung
- Schulungen

DSB der Dachorganisation kann gleiche/r sein wie die von den MOs benannten.

Auf der sicheren Seite