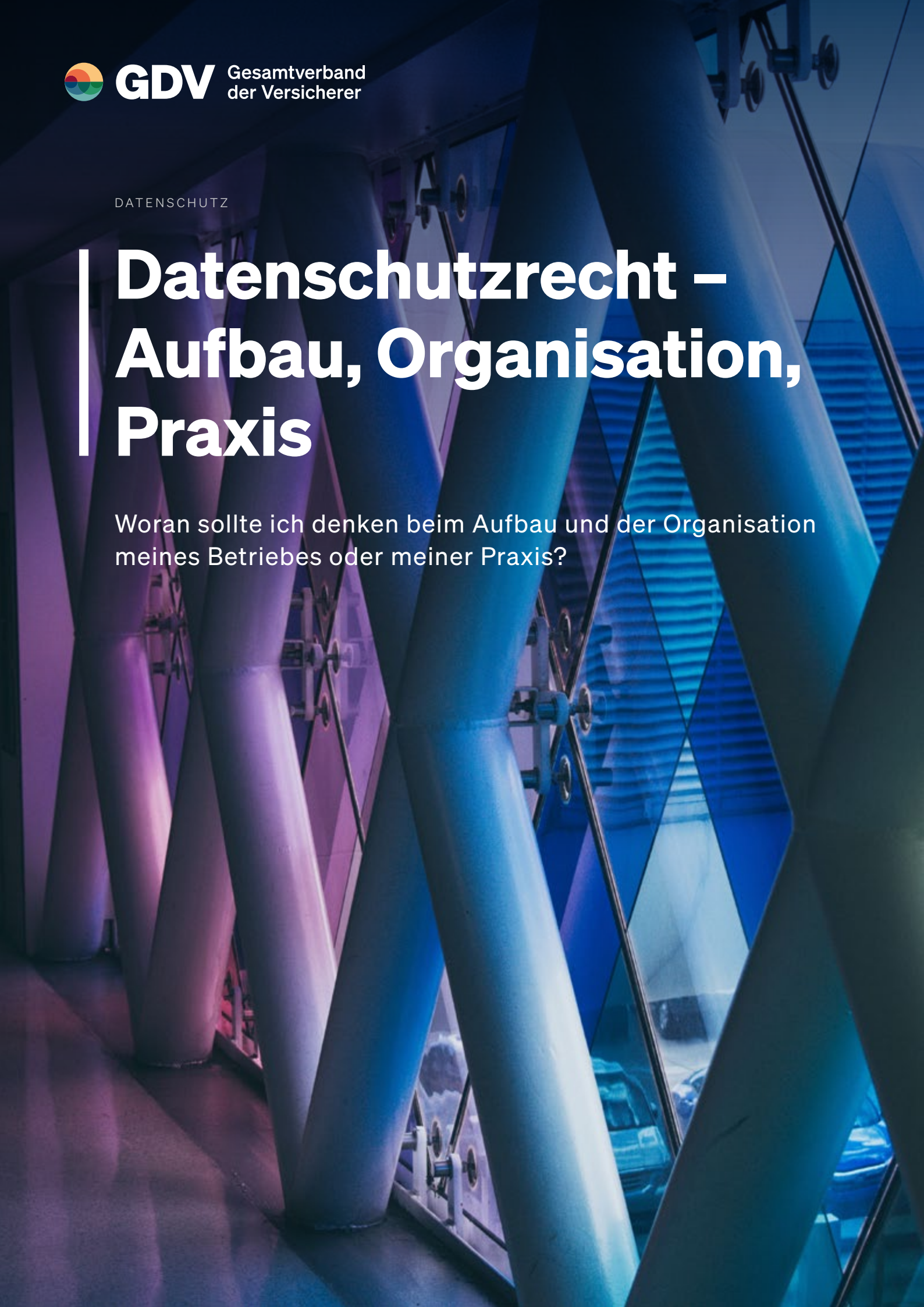
GDV Gesamtverband der Versicherer

DATENSCHUTZ

Datenschutzrecht – Aufbau, Organisation, Praxis

Woran sollte ich denken beim Aufbau und der Organisation meines Betriebes oder meiner Praxis?



Datenschutzrecht – Aufbau, Organisation, Praxis

Herausgeber
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020–5000, Fax: +49 30 2020–6000
www.gdv.de, berlin@gdv.de

Autor/-innen
Dr. Maurits Helmich
Tel.: +49 30 2020–5325
E-Mail: m.helmich@gdv.de

Doreen Michaelis
Tel.: +49 30 2020–5291
E-Mail: d.michaelis@gdv.de

Dr. Sarah Meckling-Geis
Tel.: +49 30 2020–5313
E-Mail: s.meckling-geis@gdv.de

Redaktionsschluss
28.02.2024

Gestaltung
Michel Arencibia

Bildnachweis
Unsplash | caio-pezzo | pL7-jHsxOuE

Vorwort

Wohl keine andere europäische Verordnung ist im Alltag von Bürgern und Unternehmen so spürbar wie die Datenschutz-Grundverordnung (DSGVO). Nahezu täglich – oft mehrmals täglich – willigen wir darin ein, dass unsere persönlichen Daten erhoben, gespeichert und verarbeitet werden. Kein Online-Shop, kein Handwerker, kein Arzt, keine Schule, keine Versicherung und kein Verein kommt ohne ausführliche Datenschutzerklärung aus. Jede Webseite hat mittlerweile ein Cookie-Banner, viele Unternehmen einen Datenschutzbeauftragten.

Fallstricke und Fehlerquellen gibt es beim Umgang mit personenbezogenen Daten zuhauf. Das spüren immer mehr Unternehmen sehr schmerzhaft: Die Aufsichtsbehörden verhängen nach Datenschutz-Verstößen inzwischen hohe Bußgelder. Immer mehr Menschen verlangen darüber hinaus Schadensersatz – und bekommen diesen auch. Die Summen mögen im Einzelfall nicht hoch sein, aber weil oft große Datenbestände betroffen sind, werden die Ansprüche schon durch die schiere Masse zum Problem.

Wir Versicherer bieten unseren Schutz und stehen unseren Kunden beratend zur Seite. In der Betriebshaftpflicht- und der Cyberversicherung sind Schadensersatzansprüche nach Datenschutzverletzungen zunehmend mitversichert. Dabei merken wir: Insbesondere in kleinen und mittleren Unternehmen ist die Sensibilität vielerorts noch gering und die Unsicherheit groß. Wann brauche ich welche Einwilligung von wem? Wo darf ich Daten speichern? An wen darf ich sie weitergeben? Wie kann ich sie am besten schützen? Wen muss ich nach einem Datenschutz-Verstoß informieren und bis wann? Alle diese Fragen müssen rechtssicher beantwortet werden, wenn ein Unternehmen Bußgelder, Schadenersatzforderungen und den mit einem Datenverlust einhergehenden Imageschaden vermeiden will.

Diese Broschüre zum Datenschutzrecht soll insbesondere für Selbständige sowie kleinere Unternehmen einen ersten Pfad durch den Datenschutz-Dschungel schlagen. Wir zeigen auf, an welchen Stellen Datenschutz im Berufsalltag eine Rolle spielt und welche technischen, rechtlichen und organisatorischen Mittel dabei helfen können, effektiven Datenschutz zu gewährleisten. Wir geben einen Überblick aktueller Gerichtsurteile, in denen Betroffenen zur Wiedergutmachung ihres Schadens auch schon fünfstellige Summen zugesprochen wurden. Und Sie finden seriöse Quellen, die Ihnen eine tiefere Beschäftigung mit dem Thema auf einzelnen Handlungsfeldern ermöglichen. Das alles ersetzt keine rechtliche Beratung durch Fachleute, sondern bietet einen ersten Einstieg in die Thematik und kann Ihnen dabei helfen, sich auf weitere Gespräche mit Datenschutzexperten gut vorzubereiten. Investieren Sie also die Zeit, werfen Sie einen Blick in unsere Broschüre und nehmen Sie die Verantwortung für den Schutz der Ihnen anvertrauten Daten ernst – es wird sich für Sie lohnen!

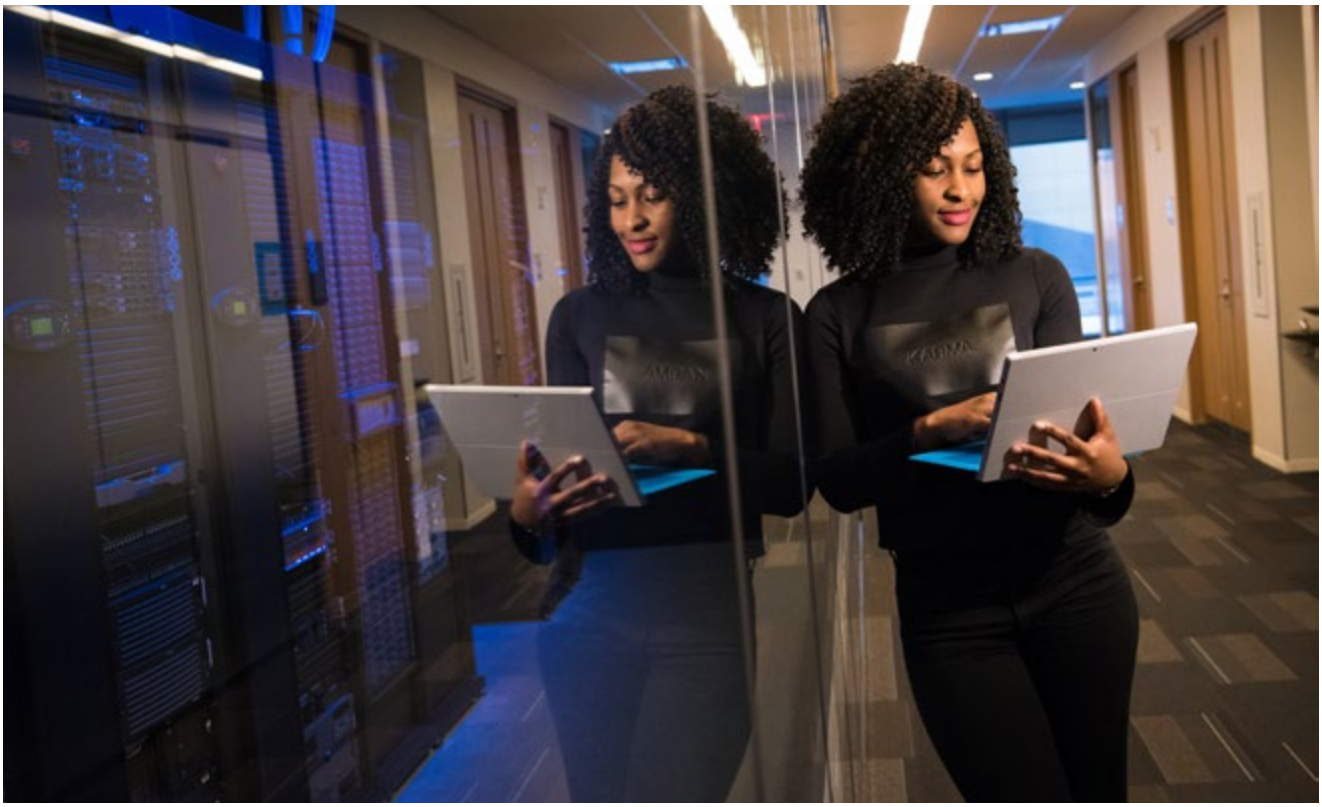
Anja Käfer-Rohrbach
Stellvertretende Hauptgeschäftsführerin
Berlin, Februar 2024

1. Datenschutzrecht – Woran sollte ich denken beim Aufbau und der Organisation meines Betriebes oder meiner Praxis?

Das Datenschutzrecht wirkt sich auf alle Bereiche Ihres Betriebes, Ihres Vereins, Ihrer Praxis oder Ihrer Kanzlei aus. Wir möchten Ihnen dazu eine kleine Hilfestellung an die Hand geben, die Ihnen einen ersten Eindruck von typische datenschutzrechtliche Fragestellungen geben, die Sie für sich klären müssen. Um einen ersten Einstieg in dieses Thema zu bieten, schauen wir uns den Verlauf eines Kundenverhältnisses an und geben Ihnen erste Hinweise zur datenschutzkonformen Organisation und sicheren technischen Gestaltung der Arbeitsabläufe. Am Ende finden Sie weitere Informationsquellen sowie aktuelle Rechtsprechung, wenn Sie tiefer in das Thema einsteigen möchten.

Achtung

Diese Darstellung kann nur Anregungen und einen ersten Eindruck von der Vielfalt der datenschutzrechtlichen Fragestellungen geben. Sie gibt nur unverbindliche Hinweise und ist nicht abschließend. Fachkundige – insbesondere rechtliche – Beratung einzuholen, wird empfohlen.



2. Datenschutz im Umgang mit Ihren Kunden – Abläufe prüfen!

1 Beim Online-Kontakt

Achten Sie darauf, dass Ihre Online-Umgebung Datenschutzrechte angemessen berücksichtigt!

- Vollständige Datenschutzhinweise auf der Homepage
- Kundendaten-Eingabe und Kontaktformular gut geschützt
- Sofern Cookies eingesetzt werden, ist die Einholung notwendiger Einwilligungen sichergestellt (z.B. Cookie-Banner)
- Externe Anwendungen geprüft, insb. hinsichtlich der Weitergabe von Nutzerdaten (z. B. IP-Adressen an Plug-In-Anbieter in den USA, wie u.a. Google-Maps, YouTube-Videos, Facebook-„Like-Button“)

2 Zugang zu Ihrem Büro

Manchmal werden Ihre Kunden Sie persönlich besuchen. Achten Sie darauf, dass nicht jeder unkontrolliert Zugang zu Ihrem Arbeitsplatz hat!

- Zutritt zu den Arbeitsräumen kontrollieren
- Wirksame Maßnahmen gegen Einbrüche
- Besonders sensible Arbeitsbereiche (z. B. Serverräume oder Archivflächen) zusätzlich sichern

3 Empfangsbereich

Im Empfangsbereich sollen sich Ihre Kunden wohlfühlen, sie dürfen aber nicht alles über andere Kunden erfahren!

- Kunden und Personal können persönliche oder berufliche Themen besprechen, ohne dass andere zuhören
- Bildschirme so einrichten, dass sie nicht eingesehen werden können
- Besuchslisten nicht offen ausliegen lassen
- Unbeaufsichtigte Computer konsequent sperren

4 Beim Erhalt von Kundendaten

Die Verarbeitung von Kundendaten braucht immer eine Erlaubnisgrundlage. Prüfen Sie die gesetzlichen Möglichkeiten und holen Sie, wenn nötig, wirksame Einwilligungen ein!

- Informationspflichten vollständig erfüllen, z. B. transparent kommunizieren, welche Daten zu welchen Zwecken verarbeitet und mit wem sie geteilt werden
- Datenverarbeitungssysteme ausreichend sichern
- Datenschutzvereinbarungen mit Dienstleistern schließen (z.B. Auftragsdatenverarbeitungsvereinbarung mit Cloud-Anbieter)
- Ordnungsgemäße Erfüllung der Ansprüche Betroffener sicherstellen, z.B. Auskunft, Berichtigung oder Löschung ihrer Daten

5 Nach dem Kundenkontakt

Auch wenn Sie nicht (mehr) direkt mit Ihren Kunden in Kontakt stehen, ist der Datenschutz umfassend sicher zu stellen!

- Ein vollständiges Verzeichnis aufstellen, welche Daten Ihrer (ehemaligen) Kunden wofür, in welchem Umfang und wie lange verarbeitet werden
- Prozesse festlegen, die das Löschen und Vernichten von nicht mehr benötigten Daten und Unterlagen sicherstellen

3. Die wichtigsten Schritte zum Datenschutz im Betrieb

Datenschutzmanagement, z.B.

- Hauptverantwortlichen bestimmen (in der GF/im Betriebsvorstand)
- Ggf. Datenschutzbeauftragten intern oder extern bestellen
- Einhaltung der Grundsätze: Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Begrenzung der Speicherzeit, Integrität u. Vertraulichkeit
- Datenschutzkonzept und interne Richtlinien (z. B. RL für Homeoffice, Passworte, IT-Nutzung)
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen
- Verzeichnis der Verarbeitungen personenbezogener Daten anlegen
- Fristgerechte Bearbeitung von Auskunftsersuchen und anderen Betroffenenanliegen sichern

Rechtsgrundlagen für jede Datenverarbeitung

- Gesetzliche Erlaubnisgrundlagen prüfen
- Durchgeführte Interessenabwägungen dokumentieren
- ggf. Einwilligungen und/oder Schweigepflichtentbindungen einholen und dokumentieren

ORGANISATORISCH

Datenschutz-Schulungen

- Mitarbeiter und Führungskräfte
- Spezielle Bereiche: Personalabteilung bzgl. Mitarbeiterdaten, Callcenter, Vertrieb...

Verträge über Datenverarbeitungen abschließen mit

- Auftragsverarbeitern nach Art. 28 DSGVO
- Geschäftspartnern
- Mitarbeitern, soweit nicht § 26 BDSG greift

Achtung

Diese Darstellung kann nur Anregungen und einen ersten Eindruck von der Vielfalt det datenschutzrechtlichen Fragestellungen geben. Sie gibt nur unverbindliche Hinweise und ist nicht abschließend. Fachkundige – insbesondere rechtliche – Beratung einzuholen, wird empfohlen.

Dokumentierte Prozesse, z.B.

- Ordnungsgemäße Dokumentation von Datenverarbeitungen
- Dokumentation mündlich/elektronisch eingeholter Einwilligungen/SSE
- Dokumentation und ggf. Meldung von Datenpannen an Aufsichtsbehörden und betroffene Personen

Datenschutzkonforme Videoüberwachung, z.B.

- Kennzeichnung der Videoüberwachung
- Dem Zweck entsprechende Speicherdauer
- Erfüllung der Informationspflichten

Informationssicherheit herstellen, z.B.

- Risiken regelmäßig analysieren
- Passende technische Maßnahmen treffen für
  - Vertraulichkeit, z.B. Pseudonymisierung und E-Mail-Verschlüsselung serverseitig
  - Verfügbarkeit und Belastbarkeit der Systeme herstellen, z.B. durch Backups
  - Zuverlässigkeit und Integrität der Systeme herstellen, d.h. Daten werden nicht durch Fehlfunktionen beschädigt
- Weitere Maßnahmen treffen gegen:
  - unbefugten Zutritt zum Gebäude und Zugang zu Rechnern
  - unbefugtes Lesen, Kopieren, Verändern oder Löschen von Daten
  - unbefugten Zugriff auf die personenbezogenen Daten

TECHNISCH

Website datenschutzkonform gestalten, z.B.

- Keine externen Anwendungen, die Daten unzulässig (in Drittstaaten) exportieren
- Vollständige Datenschutzhinweise implementieren
- Sicheres Kontaktformular
- Ggf. Cookie-Banner und Einwilligungsmanagement
- Festgelegte Prozesse, um ungenutzte Webseiten offline zu nehmen

4. Drohen Bußgelder und/oder Schadenersatzforderungen?

Bußgelder drohen praktisch immer, wenn Pflichten aus der DSGVO nicht erfüllt werden. Gemäß Art. 83 DSGVO können Geldbußen von bis zu 20 Mio. EUR oder – wenn dies höher ist – 4 % des Unternehmensumsatzes verhängt werden.

Schadenersatzforderungen drohen, wenn die betroffenen Personen einen materiellen Schaden erleiden oder in ihren Rechten beeinträchtigt sind. Es gibt nicht nur Schadenersatzansprüche für finanzielle Schäden. Bereits geringfügige Rechtsverletzungen können zu Schadenersatzansprüchen führen (vgl. Urteil des EuGH vom 04.05.23 - C 300/21). Auch deutsche Gerichte haben bereits Schadenersatzansprüche für immaterielle Schäden zugesprochen, z.B.:

Art des Datenschutzverstoßes	Vom Gericht zugesprochene Entschädigung
Website-Anwendung benutzen, die automatisch IP-Adressen weiterleitet	**€ 100** (LG München I, 20.01.2022 – 3 O 17493/20)
Übersendung Werbe-E-Mails ohne wirksame Einwilligung	**Bis zu € 300** (bspw. AG Pfaffenhofen 09.09.2021 – 2 C 133/21)
Rechtswidrige Videoüberwachung	**€ 500** (LG Berlin, 15.07.2022 – 63 O 213/20)
Datenleck aufgrund mangelhafter Sicherheitsvorkehrung bei der Beauftragung von Dienstleistern	**Bis zu € 2.500** (LG München, 09.12.2021 – 31 O 16606/20 siehe auch LG Köln, 18.05.2022 – 28 O 238/21)
Rechtswidriges Veröffentlichen persönlicher Daten, z. B. von Fotos ehemaliger Beschäftigter	**Bis zu € 5.000** (bspw. ArbG Münster 25.03.2021 – 3 Ca 391/20)
Auskunfts- und Informationsansprüche nicht rechtzeitig und/oder nicht ordnungsgemäß erfüllen	**Bis zu € 10.000** (bspw. ArbG Oldenburg (3. Kammer) 09.02.2023 – 3 Ca 150/21)
Teilen sensibler Informationen, wie Gesundheitsdaten, ohne Zustimmung	**Bis zu € 10.000** (bspw. LG Meiningen, 23.12.2020 – 3 O 363/20)

Achtung

Anders als gesetzlich begründete Schadenersatzforderungen sind Bußgelder in der Regel nicht von der Haftpflichtversicherung gedeckt!

Achtung

Wenn sich eine Vielzahl von Kläger*innen in einem Kollektivverfahren zusammenschließen, kann das zu Entschädigungssummen führen, die für Unternehmen jeder Größe existenzbedrohend werden können!

5. Wo finden Sie weitere Hinweise?

Wo finden Sie weitere Hinweise?

Allgemeine Hinweise[1]

- www.bfdi.bund.de/DE/Fachthemen/Gremienarbeit/Datenschutzkonferenz/DSK-tableKurzpapiere.html
- www.gdd.de/
- www.dr-datenschutz.de/
- www.datenschutz-praxis.de/

Videoüberwachung

- www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf

Betrieb von Websites

- www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf
- www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

Datenschutz am Arbeitsplatz

- www.datenschutz.de/leitfaeden/
- www.datenschutz.de/muster-formulierungshilfen/
- www.datenschutz.de/broschueren-und-flyer/
- www.datenschutz.de/faqs/

1 Berufsspezifische Informationen finden Sie auch auf den Homepages der Kammern der freien Berufe

Achtung

Datenschutzrechtliche Fragen sind oftmals komplex und individuell. Passende Lösungsansätze für Ihre Geschäftsprozesse kann Ihnen der Versicherer leider nicht bieten. Lassen Sie sich bei Bedarf kompetent beraten!

Datenschutz im Verein

→ www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf

→ www.sport-fuer-sachsen.de/fuer-mitglieder/downloads/muster-fuer-die-erstellung-von-datenschutzunterlagen

Verzeichnis der Verarbeitungen

→ www.bfdi.bund.de/DE/Fachthemen/Inhalte/Allgemein/Verzeichnis-Verarbeitungstaetigkeiten.html

→ www.sport-fuer-sachsen.de/fuer-mitglieder/downloads/muster-fuer-die-erstellung-von-datenschutzunterlagen

Standarddatenschutzklauseln & Angemessenheitsbeschlüsse

→ commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_de

→ www.datenschutz.rlp.de/de/themenfelder-themen/angemessenheitsfeststellung-der-eu-kommission/

Risikobeurteilung

→ www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf

Datenschutz-Folgenabschätzung

→ www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf

→ www.ldi.nrw.de/liste-von-verarbeitungsvorgaengen-nach-art-35-abs-4-ds-gvo-fuer-den-oeffentlichen-bereich

→ ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

→ www.datenschutz-bayern.de/dsfa/

Achtung

Anders als gesetzlich begründete Schadenersatzforderungen sind Bußgelder in der Regel nicht von der Haftpflichtversicherung gedeckt!

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020–5000, Fax: +49 30 2020–6000
www.gdv.de, berlin@gdv.de