

The background of the slide is a blurred photograph of two hands holding a smartphone. One hand is at the top, and the other is at the bottom, both with fingers positioned as if they are about to interact with the screen. The phone is held horizontally.

Crashkurs DSGVO: Wie Sie die wichtigsten Anforderungen des neuen Datenschutzrechts erfüllen

Dr. Martin Schirnbacher
5. September 2018

Referent



Dr. Martin Schirmbacher
Rechtsanwalt, Fachanwalt für IT-Recht

- Studium in Berlin und London
- Seit 2005 Partner bei HÄRTING Rechtsanwälte
- Co-Chair des Technology Law Committee der International Bar Association
- Beratungsschwerpunkte im IT-Recht und im Datenschutz

Inhaltsverzeichnis

DSGVO-Grundlagen im Schnelldurchgang	4
Die Must-haves priorisiert	12
Verzeichnis für Verarbeitungstätigkeiten erstellen	17
Regeln für die Auftragsverarbeitung anpassen	22
Technische und organisatorische Maßnahmen	24
Datenschutz-Folgenabschätzung	27
Informations- und Meldepflichten	29
Datenschutzbeauftragter	31
Zusammenfassung	33

The background features a dark blue square in the upper right quadrant, which contains a large white number '1.' The rest of the background is a light gray with a subtle, wavy, textured pattern.

1.

DSGVO-Grundlagen im Schnelldurchgang

DSGVO – Datenschutz-Grundverordnung

- unmittelbare Anwendung in allen Mitgliedstaaten der EU seit dem **25.5.2018**
- keine weitere Umsetzung erforderlich
- Ablösung nationaler Regelungen zum Datenschutz aus BDSG, TMG und TKG
- zugleich: Schaffung eines BDSG-neu

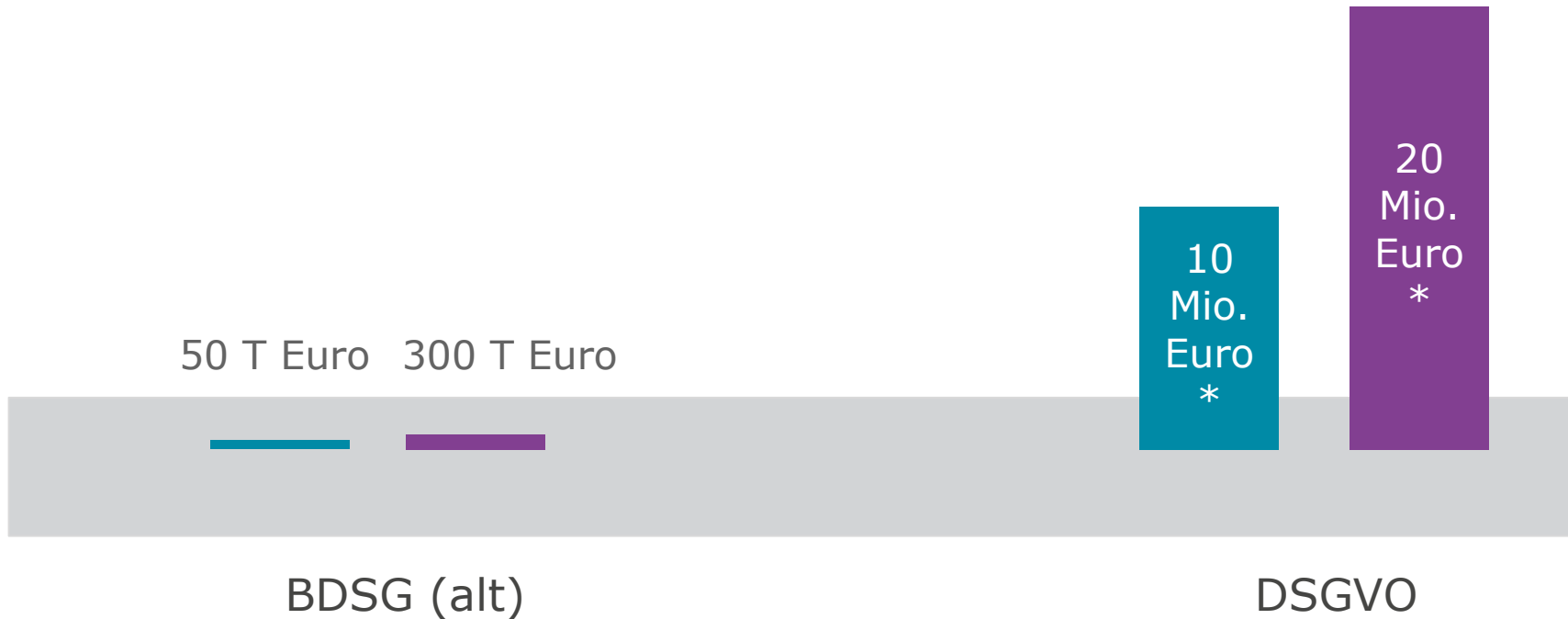
**Neuer Rechtsrahmen im
Datenschutz in der gesamten
Europäischen Union**

Viele (scheinbar) kleine Änderungen...

- Dokumentationspflicht (Umkehr der Darlegungslast)
- Erweiterter Personenbezugsbegriff
- Höhere Anforderungen an eine Einwilligung
- Bessere Möglichkeiten, Datenverarbeitung auf berechtigte Interessen zu stützen
- Recht auf Opt-Out: Widerspruchs- und Widerrufsrecht
- Recht auf Datenübertragbarkeit
- Privacy by Default / Privacy by Design
- Erweiterte Meldepflichten



...und nur eine Revolution: Horrende Bußgeldandrohung



* bzw. 2 oder 4 Prozent vom weltweiten Jahresumsatz

Personenbezug von Daten

Personenbezogen sind

- alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO)
- jedenfalls alle Informationen, die einer natürlichen Person zugeordnet sind

„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 ... identifiziert werden kann“

- Online Identifier haben Personenbezug
- Pseudonyme Daten sind personenbezogene Daten

Besonderheiten bei Kanzleien

Personenbezug liegt vor bei

- Informationen über natürliche Personen (Mandanten, Gegner, Zeugen, Dritte) im Zusammenhang mit einem Mandat (**Mandatsakten**)
- Informationen über die Beschäftigten der Kanzlei (**Personalverwaltung und Gehaltsabrechnung**)
- Informationen über natürliche Personen aus der Buchhaltung (**Finanzverwaltung**)
- Informationen über die Besucher der Website der Kanzlei (**User**)
- Informationen über die Empfänger des Newsletters der Kanzlei (**Newsletterverwaltung**)
- Informationen über Besucher von Veranstaltungen der Kanzlei (**Veranstaltungsmanagement**)

Verbotsprinzip und Erlaubnistatbestände

Verarbeitung personenbezogener Daten ist verboten...
... es sei denn...

Einwilligung
des Nutzers

Vertragliche
oder ähnliche
Verbindung

Berechtigtes
Interesse des
Unternehmens

und/oder

und/oder

Personenbezug von Daten

*Für Mittelständler von Bedeutung sind insbesondere die Tatbestände der **Vertragserfüllung und –vorbereitung** (Art. 6 Abs. 1 Satz 1 lit. b DSGVO) und der **berechtigten Interessen** (Art. 6 Abs. 1 Satz 1 lit. f DSGVO). Die meisten Verarbeitungsprozesse lassen sich auf eine dieser Grundlagen stützen:*

- **Mitarbeiter:** Die Verarbeitung von Mitarbeiterdaten dient in aller Regel der Erfüllung des Arbeitsvertrages und lässt sich daher ohne weiteres auf Art. 6 Abs. 1 Satz 1 lit. b DSGVO stützen (vgl. auch § 26 BDSG).
- **Kunden:** Soweit die Datenverarbeitung zur Bearbeitung des Mandates erforderlich ist, liegt gleichfalls ein Fall der Vertragserfüllung vor, sodass die Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 lit. b DSGVO rechtmäßig ist.
- **Interessenten:** Auch die Verarbeitung von Personendaten eines Dritten bedarf keineswegs stets der Einwilligung des Betroffenen. Vielfach lässt sich eine Datenverarbeitung auf den Erlaubnisgrund der (überwiegenden) **berechtigten Interessen** an einer Datenverarbeitung stützen (Art. 6 Abs. 1 Satz 1 lit. f DSGVO). Ein berechtigtes Interesse kann laut Erwägungsgrund 47 DSGVO die **Direktwerbung** sein.

A close-up photograph of a person's hand holding a silver pen, poised to write on a document. The background is a soft-focus office setting. Overlaid on the right side of the image is a dark blue square containing a large white number '2.'.

2.

**Die Must-haves
priorisiert**

To-Do-Liste nach Dringlichkeit

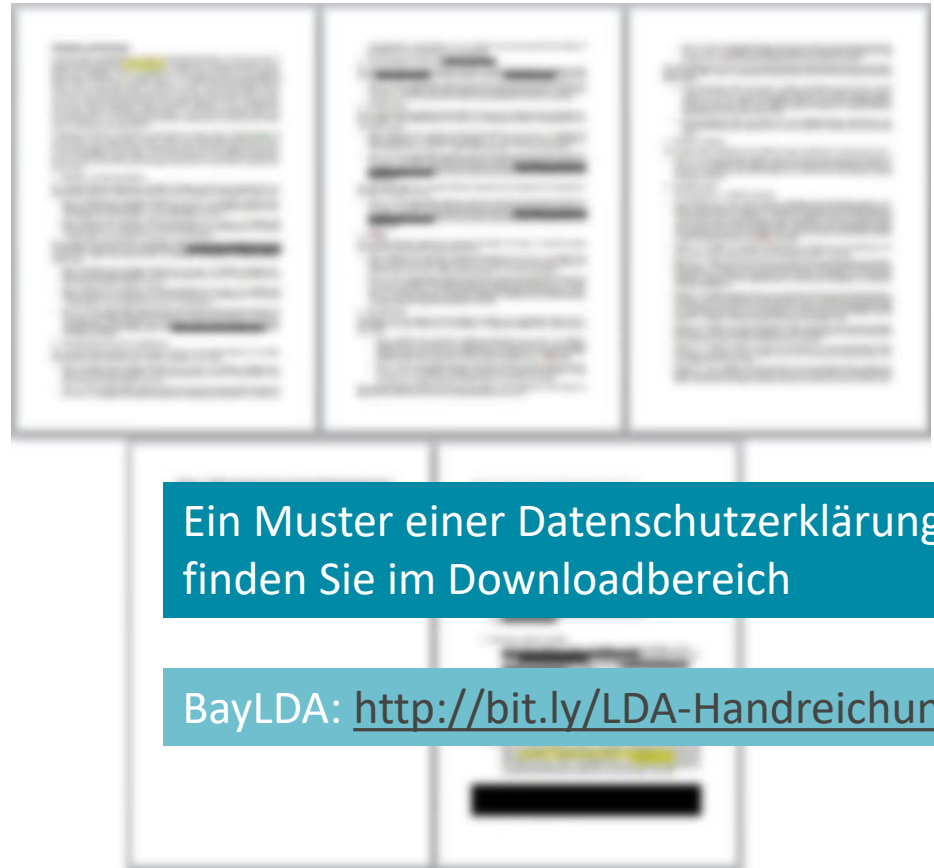
To-Do	Dringend	Wichtig	Aufwändig	
Anpassung Datenschutzerklärung	9	7	4	←
AV-Vereinbarungen mit Dienstleistern	7	6	4	←
Datenschutzbeauftragter?	6	7	(2)	←
Rechtliche Prüfung DMP/CRM	6	5	7	
Cookie-Banner?	5	5	3	
Datenschutzfolgeabschätzung	4	7	8	←
Prozess für Auskunftsansprüche	4	3	4	
Facebook/Social Media	3	4	2	
Verzeichnis von Verarbeitungstätigkeiten	3	9	9	←
Löschkonzept für Daten	3	7	7	

Anpassung der Datenschutzerklärung

Vorher



Nachher



Datenschutzerklärung

1. Name und Kontaktdaten des Unternehmens sowie des betrieblichen Datenschutzbeauftragten
2. Erhebung und Speicherung personenbezogener Daten sowie Art und Zweck von deren Verwendung
 - Beim Besuch der Website
 - Bei Anmeldung für unseren Newsletter
 - Bei Nutzung unseres Kontaktformulars
3. Weitergabe von Daten
4. Cookies
5. Analyse-Tools
6. Social Media Plug-ins
7. Betroffenenrechte
8. Widerspruchsrecht
9. Datensicherheit
10. Aktualität und Änderung dieser Datenschutzerklärung

Ein Muster einer Datenschutzerklärung
finden Sie im Downloadbereich

Bei Datenschutzerklärungen

Basics

- Über jede Datenerhebung muss informiert werden
- Datenschutzerklärungen müssen angepasst werden
- Einzelheiten sollten sich aus dem Verzeichnis über die Verarbeitungstätigkeiten ergeben

Kundenprozess einmal durchspielen

- Welche personenbezogenen Daten werden erhoben?
- Welche Rechtsgrundlage greift jeweils?
- Müssen zusätzliche Einwilligungen eingeholt werden?
- Was gehört in die Datenschutzerklärung?



3.

**Verzeichnis für
Verarbeitungstätig-
keiten erstellen**

Compliance: Verzeichnis der Verarbeitungstätigkeiten

Art. 30 DSGVO: Verzeichnis der Verarbeitungstätigkeiten

- Liste aller relevanter Datenverarbeitungsvorgänge
- Vorgänger: Verfahrensverzeichnis
- Ausnahmen: schwierig...
- Pflicht zur anlasslosen Vorlage bei Behörden
- Bei Nichteinhaltung drohen hohe Bußgelder!



Verzeichnis erstellen oder von Datenschutzbeauftragten erstellen lassen

Verzeichnis der Verarbeitungstätigkeiten: Beispiel Rechtsanwaltskanzlei

Was ist zu erfassen?

- elektronische Akten;
- Kanzleisoftware (z. B. RA Micro, Phantasy usw.);
- elektronische Diktier- und Spracherkennungsprogramme;
- Buchhaltungssoftware (Finanzbuchhaltung und Lohnbuchhaltung);
- Software zur Versendung und Verwaltung von E-Mails;
- Adressdatenbanken;
- Software zur Terminverwaltung;
- Kanzlei-Websites;
- Kanzleiseiten in Sozialen Netzwerken (z. B. Twitter, Facebook, Xing);
- elektronische Personalakten;
- betriebliches Intranet;
- Urlaubslisten

Beispiel: Lohnbuchhaltung

Mindestinhalt des Verzeichnisses

- Name der Datenverarbeitung (Beispiel: Lohnbuchhaltung)
- Zwecke der Datenverarbeitung (Beispiel: Lohnabrechnung)
- Rechtsgrundlage (Beispiel: Art. 6 Abs. 1 lit. b DSGVO)
- Beschreibung der Verarbeitung
- Verarbeitung besonderer Arten personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO
- Betroffene / betroffene Personengruppen (Beispiel: Arbeitnehmer)
- Personenbezogene Daten / Datenkategorien (Beispiel: Stammdaten, Kontodaten)
- Empfänger / Empfängerkategorien (Beispiel: Steuerbüro)
- Drittstaatentransfer
- Zugriffsberechtigte
- Regelfristen für die Löschung (Beispiel: 10 Jahre nach Ausscheiden des Mitarbeiters)
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Verzeichnis über die Verarbeitungstätigkeiten

Muster 3: Handwerksbetrieb – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
ABC Install GmbH
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@abcinstall.de
Web: www.abcinstall.de

Geschäftsführerin: Susanne Kühnlein, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbezogenen Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohn-abrechnung (über Steuerberater)	Herbert Bauer 0981/123456-1 herbert@abcinstall.de	02.03.2018	- Auszahlung der Löhne/Gehälter - Abfuhr Sozialabgaben u. Steuern	Beschäftigte	- Name, Geburtsdatum - Adresse - Bankverbindungsdaten - Lohn-/Entgeltdaten - ggf. Religionszugehörigkeit - Sozialversicherungsdaten - Steuerdaten (Steuerklasse, Freibeträge,...) - Berufsgenossenschaftsangaben	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Personalverwaltung	Herbert Bauer 0981/123456-1 herbert@abcinstall.de	02.03.2018	- Personaladministration - Personalführung - Arbeitszeitverwaltung - Personalbeschaffung (betrifft Bewerber)	- Beschäftigte - Auszubildende - Bewerber	- Name, Adressen - Zeitwirtschaftsdaten - Daten zur Arbeitsleistung - Leistungsbeurteilung - Lebenslauf und Bewerbungsunterlagen (betr. Bewerber)	Keine	Keine	- Beschäftigte: in der Regel ca. 3 Jahre nach Ausscheiden - abgelehnte	Siehe IT-Sicherheitskonzept
Betrieb der Firmenwebseite (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@abcinstall.de	28.02.2018	Außendarstellung	Webseitenbesucher	IP-Adressen	Keine			
Kundenverwaltung	Janine Kleinlein 0981/123456-2 janine@abcinstall.de	02.03.2018	- Bearbeitung von Aufträgen inkl. Rechnungstellung - postalische Werbung	Kunden	- Name, Adresse - Angaben zum Auftrag - ggf. Bankverbindungsdaten	Keine			
***	***	***	***	***	***	***	***	***	***

Eine Word-Mustervorlage eines Verzeichnisses über Verarbeitungstätigkeiten finden Sie im Downloadbereich.

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

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Aktueller Virens Scanner/Sicherheitssoftware
- ✓ Papieraktenvernichtung mit Standard-Shredder



Eine Excel-Vorlage für ein Verzeichnis finden Sie unter
https://anwaltverein.de/files/anwaltverein.de/downloads/praxis/datenschutz/dav_muster-verzeichnis-der-verarbeitungstaetigkeiten-nach-art-30-dsgvo-1.xlsx



4.

**Regeln für die
Auftragsver-
arbeitung anpassen**

Checkliste – Zusammenarbeit mit Dienstleistern

- Verarbeitung personenbezogener Daten?
- Verarbeitung im Auftrag (oder z.B. gemeinsame Verantwortlichkeit)?
 - Compliance der Dienstleistung (z.B. Online-Marketing-Tool)
 - Auftragsverarbeitung-Vertrag als Grundvoraussetzung
 - Anbieter in den USA (Privacy-Shield-Zertifizierung)
 - Anbieter außerhalb der EU (EU-Standardvertragsklauseln, BCR)

5.

Technische und organisatorische Maßnahmen

T-O-M Datensicherheit – Art. 32 DSGVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Checkliste

- **Verschlüsselung:** Es empfiehlt sich, die Verschlüsselung von E-Mails mit Verschlüsselungsprogrammen **zu ermöglichen**.
- **Stabilität:** Die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme ist auf Dauer sicherzustellen. Hierzu bedarf es einer fachkundigen Einschätzung einer IT-Fachfirma oder eines fachkundigen Mitarbeiters.
- **Wiederherstellbarkeit:** Verarbeitungsprozesse müssen gegen Datenverlust geschützt werden durch eine fachgerechte Datensicherung. Auch hierzu bedarf es der Unterstützung durch IT-Fachleute.
- **Regelmäßige Überprüfung:** Eine regelmäßige Routineprüfung ist für die Datensicherheit gleichfalls vorgeschrieben.

6.

Datenschutz- Folgenabschätzung

Pflicht zur Datenschutz-Folgeabschätzung

- Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten
- Notwendig, wenn die **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 hat
- **Blacklist der Behörden:**
 - Big-Data-Analyse von Kundendaten
 - Umfangreiche Profilbildung
 - Betrieb von Bewertungs- oder Datingportalen
 - Inkassodienstleistungen
 - Zahlartensteuerung
 - Scoring

The background features a dark blue field with vertical columns of glowing binary code (0s and 1s) in a lighter blue-green hue. A large, white, stylized number '7.' is positioned on the right side, partially overlapping a dark blue rectangular area.

7.

Informations- und Meldepflichten

Informationspflicht und Transparenz

Pflicht zur Information über die Datenerhebung (online und offline) Mindestinhalt einer Datenschutzhinweisung

- Namen und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- Kontaktdaten des Datenschutzbeauftragten
- Zwecke und Rechtsgrundlagen der Datenverarbeitung
- Ggf. die berechtigten Interessen an einer Datenverarbeitung
- Ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- Ggf. die Absicht einer Übermittlung in Drittstaaten oder an eine internationale Organisation
- Weitere Informationen, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten
- Dauer der Datenspeicherung bzw. Kriterien für die Festlegung der Dauer = Löschkonzept
- Bestehen von Betroffenenrechten wie Auskunft, Berichtigung, Löschung, Sperrung, Widerrufsrecht, Widerspruchsrecht, Datenübertragbarkeit



Deutlich umfangreichere Datenschutzerklärung, detaillierte Prüfung erforderlich



8.

**Datenschutz-
beauftragter**

Datenschutzbeauftragter

Brauchen wir einen Datenschutzbeauftragten?

- Art. 37 DSGVO: nur in bestimmten Fällen, wenn die Datenverarbeitung die Kerntätigkeit des Unternehmens ist
- § 38 BDSG-neu: wenn in der Regel mindestens 10 Personen ständig mit der Datenverarbeitung beschäftigt sind
- Nichtbestellung ist bußgeldbewehrt

Extern oder intern?

- Kurzfristig mag extern besser sein, längerfristig lohnt sich der Aufbau eigenen Knowhows
- Pflicht zur Mitteilung des Datenschutzbeauftragten an die Behörde



9.

Zusammenfassung

To-Do-Liste nach Dringlichkeit

To-Do	Dringend	Wichtig	Aufwändig	
Anpassung Datenschutzerklärung	9	7	4	←
AV-Vereinbarungen mit Dienstleistern	7	6	4	←
Datenschutzbeauftragter?	6	7	(2)	←
Rechtliche Prüfung DMP/CRM	6	5	7	
Cookie-Banner?	5	5	3	
Datenschutzfolgeabschätzung	4	7	8	←
Prozess für Auskunftsansprüche	4	3	4	
Facebook/Social Media	3	4	2	
Verzeichnis von Verarbeitungstätigkeiten	3	9	9	←
Löschkonzept für Daten	3	7	7	



**Herzlichen Dank
für Ihre
Teilnahme**

Techniker Krankenkasse

www.firmenkunden.tk.de