RÖMERMANN RECHTSANWÄLTE AG

DSGVO-Kompass

mit Praxis-Beispielen

RÖMERMANN

RECHTSANWÄLTE
AKTIENGESELLSCHAFT

DSGVO-KOMPASS

Orientierung im Dschungel der Datenschutz-Grundverordnung

Am 25.05.2018 tritt die DSGVO (gleichzeitig mit BDSG nF) in Kraft. Es gibt keine Übergangsfrist. Die DSGVO gilt, sobald personenbezogene Daten von natürlichen Personen verarbeitet werden. Verarbeiten ist alles vom Sammeln bis Erheben, Speichern, Weitergeben oder Löschen. Die DSGVO wurde eingeführt, da die Technik das wirtschaftliche und gesellschaftliche Leben verändert hat und ein „hohes Datenschutzniveau zu gewährleisten ist“ (Erwägungsgrund 6 der DSGVO).

Wichtige Begrifflichkeiten

PERSONENBEZOGENE DATEN
sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

VERANTWORTLICHER
ist die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

AUFTRAGSVERARBEITER
ist eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

EINWILLIGUNG DER BETROFFENEN PERSON
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.

VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN
ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Was muss jetzt getan werden?

1. Datenschutz-Dokumentation erstellen und ein Verzeichnis aller Verarbeitungstätigkeiten vorhalten (und aktualisieren)

Eine wesentliche Pflicht der Verantwortlichen ist die **Dokumentation seines Datenschutzkonzeptes**. Dies spielt auch im Falle eines Datenschutzverstoßes für die Frage der Bußgeldhöhe eine entscheidende Rolle. Hier muss der Verantwortliche gedanklich seine **Prozesse durchdenken** und den **DSGVO-konformen Umgang dokumentieren**. Die Datenschutzdokumentation enthält insbesondere

!

1. eine allgemeine **Beschreibung des Unternehmens und des Umgangs mit Daten** (dazu nachfolgend),
2. das **Datenschutzverzeichnis** (dazu sogleich),
3. ein **Löschkonzept** (dazu Ziff. 2.) und
4. die **Maßnahmen zur Datensicherheit** (TOMs; dazu Ziff. 5.).

Folgende **Inhalte** sollten im Rahmen einer Datenschutzdokumentation skizziert werden:

- Gegenstand (Produkte und DL) des Unternehmens, Standorte, Standorte außerhalb der EU?, Anzahl Mitarbeiter
- Nennung der Verantwortlichen und des Datenschutzbeauftragten (Wenn kein Datenschutzbeauftragter benannt ist: Erklärung, warum dies nach Ihrer Meinung nicht erforderlich ist)
- Werden Daten automatisiert verarbeitet? Werden Daten von Kindern oder solche besonderer Art (Art. 9 DSGVO) verarbeitet?
- Vorlage des Verarbeitungsverzeichnisses
- Erklärung des Umgangs mit etwaigen Datenschutzverstößen (Meldewege, Fristeneinhaltung etc.)
- Erklärung des Löschkonzeptes
- Erläuterung des Rollen- und Rechtekonzeptes (Wer legt Zugriffsrechte und technische und organisatorische Maßnahmen [TOMs] fest?).
- Erklärung des Konzeptes zur Sicherstellung der Erfüllung der Betroffenrechte (insb. auf Auskunft und Löschung)
- Wie gestaltet sich der Umgang mit der Internetnutzung der Mitarbeiter?
- Übersicht über die IT-Infrastruktur und die TOMs

Jeder Verantwortliche muss ein **Verzeichnis aller Verarbeitungstätigkeiten**, die seiner Zuständigkeit unterliegen, führen (Art. 30 DSGVO).

Es enthält folgende Angaben:

- den **Namen und die Kontaktdaten des Verantwortlichen** und ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten,
- die **Zwecke der Verarbeitung**,
- eine Beschreibung der **Kategorien betroffener Personen** und der **Kategorien personenbezogener Daten**,
- die **Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- ggf. **Übermittlungen** von personenbezogenen Daten **an ein Drittland**,
- wenn möglich, die **vorgesehenen Fristen für die Löschung** der verschiedenen Datenkategorien sowie
- wenn möglich, eine allgemeine **Beschreibung der technischen und organisatorischen Maßnahmen** (Art. 32 Abs. 1 DSGVO).

Dieses Verzeichnis könnte in Form einer Tabelle geführt werden. Bspw. wie folgt:

BUCHHALTUNG

Name der Verarbeitung	Buchhaltung
Zweck	Durchführung Finanzbuchhaltung
Rechtsgrundlage	Art. 6 Abs. 1 lit. c DSGVO, § 257 HGB, § 147 AO
Besondere Kategorie von Daten (Art. 9 DSGVO)	Nein
Betroffene Person	Mitarbeiter, Kunden
Datenkategorie	Abrechnungsdaten
Empfänger	Mitarbeiter der Buchhaltung
Drittstaatentransfer	Nein
Zugriffsberechtigte	Mitarbeiter der Buchhaltung
Löschfristen	Art. 17 Abs. 3 lit. b DSGVO, § 147 Abs. 3 AO: zehn Jahre
TOMs	DSGVO-konformes Sicherheitskonzept

NEWSLETTER

Name der Verarbeitung	Newsletter
Zweck	Versand eines Newsletters
Rechtsgrundlage	Art. 6 Abs. 1 lit. a DSGVO, § 7 UWG
Besondere Kategorie von Daten (Art. 9 DSGVO)	Nein
Betroffene Person	Newsletter-Abonnenten
Datenkategorie	E-Mail-Adresse, Name
Empfänger	Mitarbeiter oder externer Dienstleister
Drittstaatentransfer	Nein
Zugriffsberechtigte	Mitarbeiter oder externer Dienstleister
Löschfristen	Bei Wegfall der Einwilligung
TOMs	DSGVO-konformes Sicherheitskonzept

BEWERBUNGSVERFAHREN

Name der Verarbeitung	Bewerbung
Zweck	Auswertung der Bewerbungen
Rechtsgrundlage	Art. 6 Abs. 1 lit. a DSGVO
Besondere Kategorie von Daten (Art. 9 DSGVO)	Möglich
Betroffene Person	Bewerber
Datenkategorie	Bewerberdaten wie Name, Adresse, E-Mail, Alter
Empfänger	Mitarbeiter Personalabteilung
Drittstaatentransfer	Nein
Zugriffsberechtigte	Mitarbeiter Personalabteilung
Löschfristen	§ 61b Abs. 1 ArbGG, § 15 AGG: Sechs Monate
TOMs	DSGVO-konformes Sicherheitskonzept

VERTRAGSABWICKLUNG

Name der Verarbeitung	Vertragsabwicklung
Zweck	Durchführung der Vertragsleistung
Rechtsgrundlage	Art. 6 Abs. 1 lit. b DSGVO
Besondere Kategorie von Daten (Art. 9 DSGVO)	Nein
Betroffene Person	Mitarbeiter, Kunden
Datenkategorie	Sämtliche Vertragsdaten, insb. personenbezogene E-Mail und Adressen
Empfänger	Mitarbeiter
Drittstaatentransfer	Nein
Zugriffsberechtigte	Mitarbeiter
Löschfristen	Nach Vertragsbeendigung (und ggfs. Ablauf der Gewährleistungsfrist)
TOMs	DSGVO-konformes Sicherheitskonzept

TRACKING

Name der Verarbeitung	Tracking
Zweck	Speicherung der Webaktivitäten durch Analysetool „Google Analytics“ zur Optimierung des Webauftritts
Rechtsgrundlage	Art. 6 Abs. 1 lit. f DSGVO
Besondere Kategorie von Daten (Art. 9 DSGVO)	Nein
Betroffene Person	Websitebesucher
Datenkategorie	Bewegungen und Klicks der Besucher auf der Webseite, Browser-Fingerprints
Empfänger	Mitarbeiter
Drittstaatentransfer	Möglich
Zugriffsberechtigte	Mitarbeiter
Löschfristen	§ 15 TMG. Sieben Tage
TOMs	DSGVO-konformes Sicherheitskonzept

2. Informations- und Löschungskonzept erarbeiten

Unternehmer müssen zum Start der DSGVO **alle mit Datenverarbeitung verbundenen Prozesse dokumentieren und ggfs. optimieren**.

Hier muss ein **Konzept** entwickelt werden, wie der Kunde über die Verarbeitung der personenbezogenen Daten informiert wird und wann dessen Daten gelöscht werden (Recht auf Vergessenwerden).

Der Unternehmer muss ein **Informationsschreiben** (über den Umgang mit den Kundendaten) erstellen, welches der Kunde vor Vertragsschluss erhält und welches auf der Homepage („Datenschutzerklärung“) abrufbar ist.

Der Unternehmer sollte ein **Antwortmuster** für die Anfragen von Kunden bereithalten. Um die Betroffenenrechte (insb. auf Auskunft und Löschung) zu erfüllen, müssen die Mitarbeiter sensibilisiert und geschult werden.

Das **Informationsschreiben** hat einen ähnlichen Inhalt wie die Datenschutzerklärung auf der Website. Beides muss enthalten:

- Name und Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten
- Erhebung und Speicherung personenbezogener Daten sowie Art und Zweck von deren Verwendung
- Information über die Weitergabe an Dritte
- Darstellung der Betroffenrechte
- Widerspruchsrechte
- Informationen über die Datensicherheit
- Informationen über Cookies, Tracking-Tools etc. (vor allem bei der Datenschutzerklärung)
- Muster finden sich bspw. unter: https://anwaltverein.de/de/praxis/datenschutz

Die Übermittlung der Informationen (Art. 13 und 14 DSGVO) und Mitteilungen (Art. 15 bis 22 und Art. 34 DSGVO) müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache erfolgen. !

3. Ggfs. einen Datenschutzbeauftragten ernennen und hier ggfs. arbeitsrechtliche Anpassungen vornehmen

Nach der DSGVO ist ein Datenschutzbeauftragter unter bestimmten Voraussetzungen zu benennen, z.B. **wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters** in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen** erforderlich machen (Art. 37 Abs. 1 Nr. 2 DSGVO).

! Kerntätigkeit: Kerntätigkeiten sind **Geschäftsbereiche, die für die Umsetzung der Unternehmensstrategie entscheidend sind** und nicht bloß routinemäßige Verwaltungsaufgaben darstellen.

Keine Kerntätigkeit dürfte demgegenüber vorliegen bei der Analyse von Kundendaten neben dem Kerngeschäft des Vertriebes von Waren, um Produktvorschläge ggü. den Kunden machen zu können.

Der Unternehmern muss sicherstellen, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben **keine Anweisungen bezüglich der Ausübung dieser Aufgaben** erhält (Art. 38 Abs. 3 DSGVO). Es müssen **ausreichend personelle, finanzielle und zeitliche Ressourcen** zur Verfügung gestellt werden.

Ergänzend zur DSGVO benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie **in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen**; § 38 Abs. 1 BDSG nF.

ToDos des Verantwortlichen zur Ernennung des Datenschutzbeauftragten (DSB):

1. Prüfung, ob ein DSB ernannt/bestellt werden muss (10 Personen im Unternehmen?)
2. Festlegung, ob es ein Mitarbeiter (dann entsprechende Anpassung des Arbeitsvertrages) oder ein externer DSB sein soll (dann entsprechende Beauftragung)
3. Daten des DSB an den Landesdatenschutzbeauftragten melden
4. Kontaktdaten des DSB in der Datenschutzerklärung und Kundeninformation benennen

4. Vertragsanpassungen

Mitarbeiter und externe Dienstleister müssen gesondert auf die Einhaltung der Grundsätze der DSGVO **verpflichtet werden**. Externe Auftragsdatenverarbeiter haben besondere Verpflichtungen.

Für die Mitarbeiter-Information kann eine Kurzfassung verwendet werden; Bspw.:

Vertraulichkeitsverpflichtung

Personenbezogene Daten (Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen) dürfen nicht unbefugt erhoben, genutzt, weitergegeben oder sonst verarbeitet werden.

Ich verpflichte mich, personenbezogene Daten vertraulich zu behandeln und ausschließlich auf Weisung des Verantwortlichen zu verarbeiten. Diese Vertraulichkeitsverpflichtung besteht auch nach Beendigung meines Arbeitsverhältnisses fort.

Verstöße gegen meine Vertraulichkeitsverpflichtung können nach Art. 83 DSGVO und den §§ 42 und 43 BDSG und anderen Gesetzen mit Geldbuße von bis zu 20.000.000 EUR, Geld- oder Freiheitsstrafe geahndet werden. Eine Verletzung meiner Vertraulichkeitsverpflichtung kann zugleich eine Verletzung arbeitsvertraglicher Pflichten oder spezieller Geheimhaltungspflichten darstellen und beispielsweise zu Abmahnung, fristloser oder fristgerechter Kündigung und/oder Schadensersatzpflichten führen.

Ich bestätige, dass ich heute über die Bedeutung meiner Verpflichtung zur Verschwiegenheit über personenbezogene Daten belehrt wurde. Ein Exemplar dieses Formulars sowie ein Merkblatt mit Erläuterungen und dem Text der Art. 29 DSGVO, Art. 83 Abs. 4 bis 6 DSGVO, § 42 Abs. 1 und 2 BDSG und § 43 Abs. 1 und 2 BDSG habe ich erhalten.

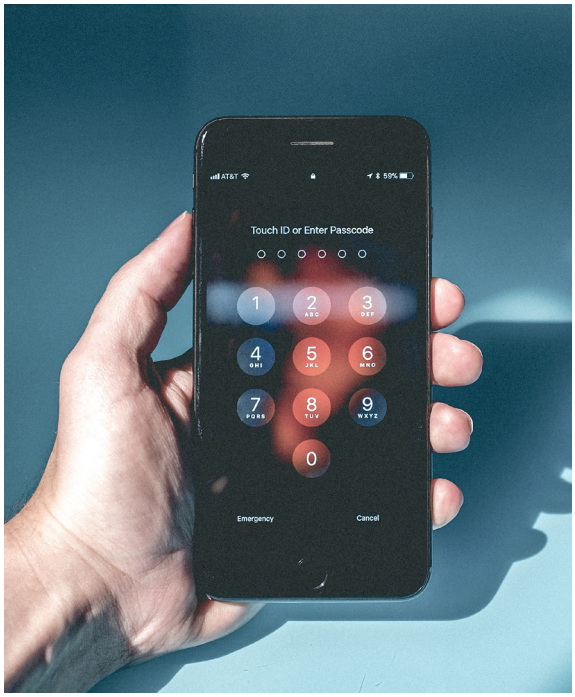
_____

Unterschrift Mitarbeiter

5. Datensicherheit

Nach Art. 32 Abs. 1 DSGVO treffen **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 der Verantwortliche geeignete technische und organisatorische Maßnahmen, um ein dem Risiko **angemessenes Schutzniveau zu gewährleisten**.

Dabei müssen **Schwachstellen erkannt und behoben** werden (bspw. Datensparsamkeit, Datenrichtigkeit, Rechtmäßigkeit, Löschfristen, Zugriffsrechte und Zugangskontrollen). Zudem müssen **technische und organisatorische Maßnahmen („TOMs“) zum Schutz der Daten** getroffen werden (bspw. Verschlüsselung, Stabilität und Wiederherstellbarkeit; ggfs. auch Cyberriskversicherung).



ÜBERSICHT DER DATENSICHERUNGSMASSNAHMEN / TOMs

Zugangskontrolle	Bspw. durch Sicherheitsschlösser
Datenträgerkontrolle	Idealerweise mit VPN-Tunnel arbeiten
Speicher-, Benutzer und Zugriffskontrolle	Bspw. durch Passwortrichtlinien, Protokollierungen, Festlegung der Berechtigungen, Differenzierung zwischen Lesen/Löschen/Ändern
Übertragungskontrolle	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
Transportkontrolle	Schutz der Daten durch Festlegung der Abläufe
Wiederherstellbarkeit und Schutz	Bspw. Backup, Firewall, Virenschutz, unabhängige Systeme oder entsprechend ausgestatteter Serverraum

DSGVO-Checkliste: An alles gedacht?

1. Datenschutz-Dokumentation erstellen und ein Verzeichnis aller Verarbeitungstätigkeiten vorhalten (und aktualisieren) ❐
2. Löschungskonzept für das „Vergessen-werden“ von Daten erarbeiten ❐
3. Ggfs. einen Datenschutzbeauftragten ernennen und hier ggfs. arbeitsrechtliche Anpassungen vornehmen ❐
4. Interne Anpassung der Verpflichtungen der Mitarbeiter ❐
5. Sicherstellung der Erfüllung der Auskunfts-verpflichtungen an den Berechtigten (sowie Verhinderung der Auskunftserteilung an Nichtberechtigte) ❐
6. Organisation und Schulung der Mitarbeiter ❐
7. Anpassung der Verträge mit externen Dienstleistern (Art. 28 DSGVO) ❐
8. Erstellung eines Informationsschreibens an Kunden zur Erfüllung der Informationspflicht (Art. 12 f. DSGVO) ❐