



Die Datenschutzgrundverordnung Teil 2





Whitepaper

Die Datenschutzgrundverordnung
Teil 2

Inhalt

01

Rückblick | Inhalte Teil 1

03

Rechte und Pflichten der
Verantwortlichen und Auftragsverarbeiter

05

Meldepflichten

07

Besonderer Handlungsbedarf bei
Webseiten und Social-Media

02

Betroffenenrechte

04

Datensicherheit und Datenschutz
durch Technikgestaltung

06

Datenschutzkonzept

08

Haftung und Sanktionen

Wir bei MORGENSTERN legen großen Wert auf inklusive Sprache. Deswegen gendern wir – und zwar gerne! Du sollst dich von unseren Texten angesprochen fühlen, egal wer du bist.

Fachbegriffe gendern wir jedoch nicht, da sie wie Eigennamen feststehende Begriffe sind. Hier geht es nicht um das generische Maskulinum, sondern um fachliches Vokabular, das seine eigene juristische Bedeutung hat.

...dir aber nun **viel Spaß**, liebe*r Leser*in!

01. Einführung

Nachdem Du in Teil 1 schon einiges über die Datenschutz-Grundverordnung erfahren hast, folgt nun der zweite Teil unseres Whitepapers. Freu Dich auf spannende Themen wie etwa Betroffenenrechte, Sanktionen bei Verstößen oder den besonderen Handlungsbedarf bei Webseiten und Social-Media. Viel Spaß!

Du kannst beide Teile des DS-GVO Whitepaper auf unserer [Webseite](#) runterladen.

Brauchst du Rat? Kontaktiere uns! Wir bei MORGENSTERN haben ein erfahrenes und hoch spezialisiertes Team bestehend aus Anwälten, Datenschutz- und IT-Sicherheitsexperten!



contact@morgenstern-privacy.com

+49 (0) 6232 - 100119 44



Mehr MORGENSTERN Whitepaper findest du übrigens auch unter:
morgenstern-privacy.com & morgenstern-legal.com

02. Betroffenenrechte

Der Verantwortliche ist verpflichtet, geeignete Maßnahmen zu treffen, um den Betroffenen alle Informationen, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und zugänglicher Form zu übermitteln. Außerdem hat er ihnen die Ausübung ihrer Rechte zu erleichtern bzw. sicherzustellen.

Die zentralen Betroffenenrechte sind in den Artikeln 12 ff. der DS-GVO normiert. Das BDSG regelt ergänzend die Einschränkung der Betroffenenrechte im Kapitel 2 (§ 32 bis 37 BDSG).

Recht auf Information

Gemäß Art. 13 und 14 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen über die Details der Datenverarbeitung informiert zu werden. Die DS-GVO unterscheidet danach, ob die Daten bei der betroffenen Person (Art. 13 DS-GVO) oder nicht bei dieser erhoben werden (Art. 14 DS-GVO).

- ▶ Sinn und Zweck dieser Vorschriften ist es, der betroffenen Person die Abschätzung zu ermöglichen, wer was wann und bei welcher Gelegenheit über sie weiß, um selbstbestimmt über die Geltendmachung ihrer Betroffenenrechte entscheiden zu können. Sie soll insbesondere in die Lage versetzt werden, ihren Auskunftsanspruch (Art. 15 DS-GVO) oder ihre Korrekturrechte (Art. 16 DS-GVO) wahrnehmen zu können.

Folgende Informationen sind u. a. zu erteilen:

- ▶ die Identität des Verantwortlichen
- ▶ die Kontaktdaten des*r Datenschutzbeauftragten
- ▶ die Verarbeitungszwecke und Rechtsgrundlage
- ▶ die Empfänger bzw. Kategorien von Empfängern
- ▶ gegebenenfalls Absicht der Datenübermittlung an ein Drittland (vgl. Art. 13 Abs. 1 f) DS-GVO)
- ▶ die Dauer der Speicherung
- ▶ die Rechte der betroffenen Person gem. Art. 15 ff. DS-GVO
- ▶ die Widerrufbarkeit von Einwilligungen
- ▶ das Beschwerderecht bei der Aufsichtsbehörde
- ▶ ob die Bereitstellung personenbezogener Daten gesetzlich / vertraglich vorgeschrieben bzw. für einen Vertragsabschluss erforderlich ist, ob der Betroffene zur Bereitstellung verpflichtet ist sowie mögliche Folgen einer Nichtbereitstellung
- ▶ Informationen zu automatisierten Entscheidungsfindungen und Profiling

Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, bestehen für den Verantwortlichen ebenfalls die oben erwähnten Informationspflichten (vgl. Art. 14 DS-GVO). Zusätzlich muss der Verantwortliche die betroffene Person darüber aufklären, aus welcher Quelle die personenbezogenen Daten stammen und ob es sich dabei um eine öffentlich zugängliche Quelle handelt (Art. 14 Abs. 2 f) DS-GVO).

Allgemeine Aussagen zur Art der gespeicherten Daten sind für das Recht auf Information ausreichend, da die Information nicht die Auskunft ersetzen soll. Nach dem Zweck der Vorschriften soll die Information vor Beginn der Datenerhebung erfüllt werden. Sollen die Daten für einen anderen Zweck weiterverarbeitet werden, als den, für den sie erhoben wurden, ist die betroffene Person vorab über den anderen Zweck und die weiteren Bedingungen, u. a. die Speicherdauer und das Bestehen eines Beschwerderechts, zu unterrichten.

Die DS-GVO sieht Ausnahmen von der Benachrichtigungspflicht gegenüber der betroffenen Person vor. Eine Pflicht zur Information besteht danach nicht,

- ▶ wenn die betroffene Person über die Information bereits verfügt
- ▶ wenn Rechtsvorschriften der Union oder der Mitgliedstaaten die Erlangung oder Offenlegung der Daten ausdrücklich regeln oder sie einer Geheimhaltungspflicht unterwerfen (in Deutschland §§ 29, 32, 33 BDSG)
- ▶ bei indirekter Erhebung der Daten, wenn die Information sich als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist.

Das BDSG ergänzt in §§ 29, 32, 33 die Einschränkung der Informationspflicht.

Weitere Informationen zur Informationspflicht nach Art. 13, 14 DS-GVO und besonders der Datenerhebung bei Dritten oder auch über das Internet sind in unserem FAQ zur DS-GVO enthalten.

Auskunftsrecht

Von der Informationspflicht ist das Recht auf Auskunft (Art. 15 DS-GVO) abzugrenzen. Während die Informationspflichten proaktiv zu erfüllen sind, ist der Verantwortliche nur auf Antrag dazu verpflichtet, Auskunft zu erteilen.

Die betroffene Person hat ein Recht darauf zu erfahren, welche auf sie bezogenen Daten in welcher Form beim Verantwortlichen verarbeitet werden. Bei Geltendmachung dieses Rechts hat der Verantwortliche dem Betroffenen außerdem eine Kopie der entsprechenden Daten zur Verfügung zu stellen.

Die Auskunftserteilung muss unverzüglich erfolgen, spätestens aber innerhalb eines Monats. In Ausnahmefällen kann die Monatsfrist überschritten werden. Der Umfang des Anspruchs umfasst alle über die betroffene Person gespeicherten Daten. Dies bezieht sich auch auf den Zweck der Verarbeitung, die geplante Speicherdauer, die Herkunft der Daten und den Empfänger oder Kategorien von Empfängern der Daten, die Informationen über die Betroffenenrechte, gegebenenfalls das Bestehen einer automatisierten Entscheidungsfindung sowie bei Datenübermittlung in Drittländer über die insoweit gegebenen Garantien z. B. die Verwendung von Standarddatenschutzklauseln der EU-Kommission (vgl. Art. 15 Abs. 2 in Verb. m. Art. 46 DS-GVO).

Recht auf Berichtigung

Es kann für die betroffene Person wichtig sein, dass unrichtige Angaben, die über sie gespeichert wurden, berichtigt werden. Das Recht hierauf räumt Art. 16 Abs. 1 DS-GVO ein. Ebenso besteht ein Recht des Betroffenen auf Ergänzung unvollständiger personenbezogener Daten.

Um unrichtige personenbezogene Daten handelt es sich, wenn sie Informationen über Tatsachen enthalten, die mit der Wirklichkeit nicht übereinstimmen oder nur ein unvollständiges Abbild derselben abgeben.

Falls die betroffene Person die Richtigkeit von personenbezogenen Daten bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt, ist die Verarbeitung der Daten einzuschränken und diese Daten dürfen nicht verwendet werden (Art. 18 Abs. 1 a) DS-GVO). Der Verantwortliche ist dann verpflichtet, die Richtigkeit zu prüfen. Solange diese nicht erwiesen ist, wird die Verarbeitung eingeschränkt.

Recht auf Löschung

Das „Recht auf Vergessenwerden“ gehört wohl zu den am meisten diskutierten Neuerungen des europäischen Datenschutzrechts. Fotos, Kleinanzeige, Postings – das Internet vergisst nichts. Wer über eine Suchmaschine nach Daten einer bestimmten Person sucht, kann oft direkt ein aussagekräftiges Persönlichkeitsprofil erstellen.

Mit Art. 17 Abs. 1 DS-GVO soll dieser Entwicklung Einhalt geboten werden. Der Betroffene hat das Recht, unter bestimmten Umständen die Löschung auf ihn bezogener Daten vom Verantwortlichen zu verlangen. Die Umstände ergeben sich aus Art. 17 Abs. 1 a) bis f) DS-GVO:

- ▶ wenn die Zwecke, für die die Daten erhoben wurden, mittlerweile erreicht sind,
- ▶ wenn die Einwilligung, auf der die Verarbeitung beruhte, widerrufen wurde oder
- ▶ die Verarbeitung der Daten an sich bereits unrechtmäßig war.

Wurden Daten bereits veröffentlicht, müssen Maßnahmen ergriffen werden, um die allgemeine Löschung der Daten herbeizuführen. So müssen z.B. andere Unternehmen informiert werden, die auf diese Daten verlinken oder sie ebenfalls veröffentlicht haben.

Einschränkung der Verarbeitung

Die betroffene Person kann in bestimmten Fällen auch die Einschränkung der Verarbeitung verlangen (vgl. Art. 18 DS-GVO).

Laut der Definition in Art. 4 Nr. 3 DS-GVO handelt es sich hierbei um die Markierung gespeicherter Daten, mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Die personenbezogenen Daten dürfen dann nicht mehr nach den allgemeinen Erlaubnistatbeständen verarbeitet werden.

Die Einschränkung ist nicht als bloße Kennzeichnung (Einschränkungsvermerk) zu verstehen. Der Verantwortliche muss vielmehr durch die Einrichtung geeigneter Verfahren bzw. durch technische und organisatorische Maßnahmen sicherstellen, dass eine weitere Verarbeitung der markierten Daten nur noch zu den in Art. 18 Abs. 2 DS-GVO genannten Zwecken erfolgen kann.

Recht auf Datenübertragbarkeit

Mit der DS-GVO wurde zum ersten Mal das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO) eingeführt.

Der Verbraucher darf seine Daten nun zu einem anderen Anbieter mitnehmen, frei nach dem Motto „meine Daten, meine Entscheidung“. Das vereinfacht jeden Vertragswechsel deutlich.

Bei Geltendmachung ist der bisherige Anbieter verpflichtet, alle gespeicherten Kundendaten in einem standardisierten Formular bereitzustellen (sofern die Funktionalität bereits gegeben ist). Der neue Anbieter muss die Daten dann in sein System übernehmen. Im Optimalfall übermittelt der alte Anbieter direkt an den neuen Vertragspartner des*r ehemaligen Kunden/Kundin (sofern diese*r eingewilligt hat).

Widerspruch

Die betroffene Person hat gegenüber Verantwortlichen die Möglichkeit, einer Verarbeitung ihrer personenbezogenen Daten zur Wahrung berechtigter Interessen gemäß Art. 6 Abs. 1 f) DS-GVO zu widersprechen (vgl. Art. 21 DS-GVO). Hierzu muss sie ihre besonderen persönlichen Gründe anführen. Der Widerspruch ist begründet, wenn bei einer Interessenabwägung die schutzwürdigen Interessen gegenüber den Interessen des Verantwortlichen an der Datenverarbeitung überwiegen.

Dem Widerspruch muss der Verantwortliche nicht nachkommen, wenn er zwingende schutzwürdige Gründe für die Verarbeitung nachweisen oder die Verarbeitung mit der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen begründet werden kann (vgl. Art. 21 Abs. 1 S. 2 DS-GVO).

03. Rechte und Pflichten der Verantwortlichen und Auftragsverarbeiter

Datenschutzbeauftragte*r

Für Unternehmen stellt sich zunächst die Frage, ob sie verpflichtend eine*n Datenschutzbeauftragte*n zu benennen haben. Eine Bestellpflicht liegt vor, wenn eines der nachfolgenden Kriterien auf das Unternehmen zutrifft.

- ▶ mindestens 10 Personen sind mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt
- ▶ Es werden Verarbeitungen vorgenommen, die eine Datenschutz-Folgenabschätzung (DS-FA) nach Art. 35 DS-GVO erfordern
- ▶ die Kerntätigkeit des Verantwortlichen umfasst die regelmäßige und systematische Überwachung von betroffenen Personen
- ▶ sensible Daten i.S.v. Art. 9 DS-GVO werden verarbeitet

Das Unternehmen hat freie Wahl, ob es eine*n Mitarbeitenden oder eine*n externe*n Datenschutzbeauftragte*n benennen möchte. In jedem Fall muss der*die Ernante der Datenschutzaufsichtsbehörde gemeldet werden.

Bezüglich der Qualifikation gibt es keine spezifischen Erfordernisse. Zu berücksichtigen sind das Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis, sowie die Fähigkeit, die Aufgaben aus Art. 39 DS-GVO zu erfüllen.

Zu den Aufgaben des*r Datenschutzbeauftragten gehören:

- ▶ Unterrichtung und Beratung des Verantwortlichen: Dies beinhaltet die allgemeine Information über die bestehenden datenschutzrechtlichen Pflichten sowie die aktive Unterstützung bei der Lösung konkreter Schwierigkeiten
- ▶ Überwachung, Sensibilisierung und Schulung
- ▶ Beratung auf Anfrage im Zusammenhang mit der Datenschutz-Folgenabschätzung
- ▶ Zusammenarbeit mit der Aufsichtsbehörde
- ▶ Anlaufstelle für Aufsichtsbehörde und betroffene Personen für Fragen, die mit der Verarbeitung zusammenhängen

Merke: Die Benennung eines*r Datenschutzbeauftragten befreit das Management nicht von der eigenen Verantwortung: Die meisten Aufgaben aus der DS-GVO richten sich direkt an das Management.

Der*die Datenschutzbeauftragte hat nur eine beratende, unterstützende Funktion und dient als Ansprechpartner*in für betroffene Personen und Aufsichtsbehörden.

Datenschutz-Folgenabschätzung (DS-FA)

In manchen Fällen entsteht bei der Verarbeitung personenbezogener Daten ein gewisses Risiko. Wenn Rechte und Freiheiten betroffener Personen durch die Verarbeitung personenbezogener Daten unmittelbar gefährdet werden können, ist eine schriftliche Folgenabschätzung vorzunehmen. Hier müssen Unternehmen genau erläutern, warum die Notwendigkeit einer Datenerhebung besteht. Es sind die bestehenden Risiken zu bewerten und die ergriffenen Maßnahmen zur Minimierung anzuführen. Ein solches Risiko kann z.B. bestehen, wenn neue Technologien der Datenverarbeitung verwendet werden.

Wichtig: Die Einwilligung der betroffenen Person befreit nicht von der Verpflichtung zur Durchführung einer Folgenabschätzung.



Einige Fälle, die eine Folgenabschätzung erfordern, findest du in Art. 35 Abs. 3 DS-GVO. Die Aufsichtsbehörden müssen Listen mit Verfahren erstellen und veröffentlichen, für die eine Folgenabschätzung erforderlich oder entbehrlich ist. Die deutsche Aufsichtsbehörde hat für nicht öffentliche Stellen die aktuelle „Liste der Verarbeitungstätigkeiten, für die eine DS-FA durchzuführen ist“ auf ihrer [Homepage](#) veröffentlicht.

Verzeichnis von Verarbeitungstätigkeiten

Gemäß Art. 30 Abs. 1 DS-GVO muss jeder Verantwortliche oder Auftragsverarbeiter für jede Verarbeitungstätigkeit ein Verzeichnis führen. Gemeint ist hiermit ein elektronisch oder in Papierform geführtes Verzeichnis, in welchem die Speicherung personenbezogener Daten dokumentiert wird. Dieses Verzeichnis muss der Aufsichtsbehörde auf Verlangen vorgelegt werden.

Es sollten folgende Angaben aufgenommen werden:

- ▶ Name und Kontaktdaten des Verantwortlichen, des Vertreters des Verantwortlichen sowie des*r Datenschutzbeauftragten
- ▶ die Zwecke der Verarbeitung
- ▶ eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- ▶ die Kategorien von Empfängern, gegenüber denen die Daten offengelegt werden, einschließlich Empfängern in Drittländern
- ▶ eine geplante Datenübermittlung in Drittstaaten sowie die Dokumentierung geeigneter Garantien
- ▶ Regelfristen für die Löschung der Daten
- ▶ eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art.32 Abs. 1 DS-GVO

04. Datensicherheit und Datenschutz durch Technikgestaltung

Mit der DS-GVO wurde ein neuer Referenzrahmen zur Bewertung technisch-organisatorischer Maßnahmen geschaffen.

Es ergibt sich hieraus die Pflicht zur datenschutzkonformen Technikgestaltung (Privacy by Design und Privacy by Default).

Technische und organisatorische Maßnahmen

Verantwortliche und Auftragsverarbeiter haben angemessene technisch-organisatorische Sicherheitsmaßnahmen gegen unbefugte Zugriffe und Datenverlust zu treffen.

Bei der Auswahl angemessener Maßnahmen dürfen Wirtschaftlichkeitserwägungen berücksichtigt werden. Außerdem müssen sich die Maßnahmen am Stand der Technik orientieren. Hierzu empfiehlt es sich jedenfalls für größere Organisationen, anerkannte Standards wie IT-Grundschutz (bzw. ISO 2700x) umzusetzen oder zumindest als Orientierung zu nutzen.

Neu eingeführt werden die Schutzziele der Belastbarkeit der Systeme und der raschen Wiederherstellbarkeit personenbezogener Daten nach Zwischenfällen (Art. 32 Abs. 1 b) und c) DS-GVO).

Privacy by Design

Verantwortliche werden verpflichtet, sowohl bei der Planung von IT-Anwendungen als auch bei der anschließenden Nutzung technische und organisatorische Maßnahmen (z.B. Pseudonymisierung) einzusetzen, um die Rechte der betroffenen Personen zu schützen und den Anforderungen der DS-GVO zu genügen. Verantwortliche sollten daher sicherstellen, dass jeder Prozess der Datenverarbeitung so geplant und implementiert wird, dass er den Grundsätzen der Datenminimierung und Vertraulichkeit gerecht wird.

Privacy by Default

Durch entsprechende Voreinstellungen von Systemen ist sicherzustellen, dass nur erforderliche personenbezogene Daten verarbeitet werden. Die Voreinstellungen von Systemen sind so zu gestalten, dass personenbezogene Daten nicht ohne Eingreifen des Verantwortlichen einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Verantwortliche sollten das Konzept der "datenschutzfreundlichen Voreinstellung" umsetzen, insbesondere dann, wenn Dienstleistungen an Endverbraucher angeboten werden (d.h. bei Auswahlmöglichkeiten, sollte die „datenschutzfreundliche“ Option voreingestellt sein).

Meldepflichten

Um Verbraucherdaten besser zu schützen, ist eine sofortige Meldepflicht vorgesehen (Art. 33 DS-GVO). Unternehmen müssen im Fall einer Datenschutzverletzung die zuständige Datenschutzbehörde innerhalb von 72 Stunden informieren. Eine Meldung ist entbehrlich, wenn die Datenschutzverletzung kein Risiko für die Freiheit und die persönlichen Rechte der Betroffenen bedeuten. Betroffene sind zu informieren, sofern ein hohes Risiko für deren persönlichen Rechte und Freiheiten besteht.

Datenschutzkonzept

Das Datenschutzkonzept stellt das Herzstück eines Unternehmens dar, wenn es um den Datenschutz geht. Es handelt sich um eine schriftliche Dokumentation der Verarbeitungen und der „Unternehmensstrategie“ im Bereich Datenschutz.

Bestenfalls werden hier sämtliche notwendigen Informationen zur Erhebung, Verwendung, Nutzung und Löschung personenbezogener Daten und den damit verbundenen Prozessen und Zuständigkeiten festgehalten. Das Dokument liefert die zuständigen Verantwortlichen und Kontaktdaten, sodass beispielweise alle Mitarbeitenden im Unternehmen über das komplexe Thema Datenschutz informiert sind und genau wissen, wen Sie kontaktieren müssen, falls Fragen oder Herausforderungen in dem Bereich auftreten.

Merke: das Datenschutzkonzept sollte regelmäßig überarbeitet und gepflegt werden. Nur so können die Maßnahmen zu Datenschutz und Datensicherheit auch aktuell überprüft, bewertet und evaluiert werden.

Eine gesetzliche Pflicht zur Erstellung bzw. Führung besteht nicht, es empfiehlt sich aber unbedingt. Mit einem Datenschutzkonzept kann der Verantwortliche seinen Rechenschafts- und Dokumentationspflichten nachkommen.

05. Besonderer Handlungsbedarf bei Webseiten und Social-Media

Du fragst dich, welche Auswirkungen die DS-GVO nun konkret für deine Webpräsenzen mit sich bringt?

Datenschutzerklärung

Wenn du eine Website betreibst, hast du Ihre Besucher*innen umfassend darüber zu informieren, wie deren personenbezogenen Daten bei Aufruf und Nutzung (der Funktionen) der Website verarbeitet werden. Hierfür wird eine Datenschutzerklärung verfasst, die mit einem Klick von jeder Unterseite der Webseite aus einzusehen sein sollte. Sie muss in jedem Fall die von der DS-GVO vorgeschriebenen Pflichtinformationen (Art. 13 DS-GVO) enthalten. Hierunter fallen grundlegende Informationen wie die Nennung des Verantwortlichen sowie des*r Datenschutzbeauftragten, die Hinweise auf die Betroffenenrechte, der Empfänger der Daten sowie ob eine Übermittlung an ein Drittland stattfindet.

Außerdem solltest du für jeden einzelnen Verarbeitungsprozess Informationen über den Zweck und die Rechtsgrundlage für die Datenverarbeitung sowie die Dauer der Speicherung (bzw. die Angabe ob eine Aufbewahrungspflicht vorliegt) bereitstellen.

Die Datenschutzerklärung sollte in konkreter Abstimmung auf die jeweiligen Bedürfnisse und technischen Vorgänge verfasst werden. Wichtig ist, eine leicht zugängliche, verständliche und klare Sprache zu verwenden.

Impressum

Grundsätzlich müssen Diensteanbieter, die geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien bereithalten, bestimmte Informationen zur Verfügung stellen. Diese Informationen werden dann in einem sogenannten Impressum auf der Webseite oder der jeweiligen Webpräsenz auf Social Media (wie z.B. Facebook, Instagram, LinkedIn) gesammelt.

Als Diensteanbieter wird generell jeder Anbieter von Webseiten oder Newslettern bezeichnet, auch wenn diese ausschließlich für Werbezwecke genutzt werden. Eine unmittelbare Bestellmöglichkeit, wie etwa in einem Online Shop oder z.B. über die Funktion „Instagram Shopping“ oder andere Interaktionen müssen nicht bereitgestellt oder genutzt werden.

- ▶ Das bedeutet, dass auch eine Unternehmensseite auf einer Social-Media-Plattform, z.B. eine Fanpage auf Facebook, eine „Webseite“ darstellt, auf der du dich und dein Unternehmen als Anbieter präsentierst. Kurz um: Du musst ein Impressum vorhalten können.

Die meisten Anforderungen findest du in § 5 Abs. 1 TMG. Danach müssen mindestens Informationen zum vollständigen Namen, der Anschrift und Angaben zur Kontaktaufnahme enthalten sein. Sofern vorhanden, trifft dies auch auf Angaben zur Umsatzsteueridentifikationsnummer zu. Für bestimmte Berufe sind zudem Angaben über die Kammerzugehörigkeit, die gesetzliche Berufsbezeichnung, den Verleihungsstaat der Berufsbezeichnung sowie den Zugang zu den berufsrechtlichen Regelungen vorzuhalten. Außerdem können sich auch noch weitere Informationspflichten aus anderen Rechtsvorschriften ergeben (wie etwa dem Verbraucherschlichtungsverfahren oder dem Medienstaatsvertrag).

Letzteres insbesondere dann, wenn du z.B. einen Blog auf deiner Webseite betreibst oder eben auch auf Social Media gelegentlich journalistisch-redaktionelle Beiträge erstellst.

Wichtig ist, dass all diese Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind. Doch genau das ist auf Social Media nicht immer so leicht. Häufig gibt es keine speziell dafür vorgesehenen Möglichkeiten, ein Impressum zu hinterlegen. Die Anforderungen des deutschen Gesetzgebers sind aber klar: Ein Impressum muss ohne wesentliche Zwischenschritte erreichbar sein. Daher hat sich inzwischen in der Praxis etabliert, dass man mit maximal zwei Klicks das Impressum erreichen sollte.

Social Media

Ob Facebook, LinkedIn oder Instagram – eine Datenschutzerklärung und ein Impressum sind auch in deinen Social-Media-Profilen Pflicht. Je nach Plattform gibt es unterschiedliche Anforderungen an die Platzierung. Zunächst muss analysiert werden, welche Verarbeitungsvorgänge über die Kanäle stattfinden. Falls dich das Thema interessiert, gibt es auf der [Webseite](#) der MORGENSTERN Rechtsanwaltsgesellschaft mbH ein spannendes Whitepaper dazu.

Newsletter

Wenn du einen Newsletter versenden möchtest, gilt es einiges zu beachten. Der Versand ist grundsätzlich nur nach Bestätigung des Kunden/der Kundin bzw. Interessenten zulässig. Erforderlich ist in jedem Fall, eine Einwilligung per Double-Opt-In einzuholen und in der Datenschutzerklärung einen Passus zum Newsletter aufzunehmen.

Kontaktformular

In einem Kontaktformular werden personenbezogene Daten der Nutzer*innen erfragt. Hier sind die DS- GVO Grundsätze wie Datensparsamkeit und Zweckbindung verpflichtend zu beachten.

Cookies

Für Cookies musst du zwingend eine Einwilligung einholen, sofern diese nicht für den Betrieb der Seite technisch notwendig sind. Die Umsetzung kann mittels Cookie Banner oder einem Cookie Consent Tool erfolgen.

Weitere Informationen zum Einsatz von Cookies und den (datenschutz-)rechtlichen Anforderungen findest du in unserem [FAQ zur DS-GVO](#).

06. Haftung und Sanktionen

Mit der DS-GVO wurden außerdem neue und stark verschärfte Sanktionen für Datenschutzverstöße eingeführt und das Haftungsregime verschärft.

Die DS-GVO sieht Bußgelder von bis zu 20.000.000 Euro oder 4 Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres vor, abhängig davon welcher Betrag höher ist (Art. 83 Abs. 5 DS-GVO).

Bei Verstößen gegen die DS-GVO ist die Höhe des Bußgeldes nach dem Umsatz des "Unternehmens" zu berechnen, welches gegen die Verordnung verstoßen hat. An dieser Stelle ist der Umsatz der gesamten Unternehmensgruppe relevant, unabhängig davon, welches Unternehmen gegen die DS-GVO verstoßen hat.

§ 43 BDSG-neu sieht zudem vor, dass Verstöße gegen Auskunfts- und Informationspflichten mit bis zu 50.000 Euro Bußgeld geahndet werden können.

Für deutsche Verantwortliche relevant sind die Regelungen in § 42 BDSG-neu. Danach wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft, wer nicht allgemein zugängliche personenbezogene Daten einer großen Anzahl betroffener Dritten zugänglich macht. Mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe wird bestraft, wer personenbezogenen Daten, die nicht allgemein zugänglich sind, ohne Berechtigung verarbeitet oder erschleicht.

Zusätzlich zur Verhängung von Bußgeldern durch die Aufsichtsbehörden können betroffene Personen Schadensersatzansprüche gegen Verantwortliche und Auftragsverarbeiter geltend machen, wenn Ihnen durch deren Datenschutzverstoß ein materieller oder immaterieller Schaden entstanden ist (Art. 82 DS-GVO).

Ansonsten können auf ein Unternehmen noch folgende Sanktionen zukommen:

- ▶ Anordnungen zur Beendigung des Verstoßes gemäß Art. 58 Abs. 2 DS-GVO, z.B. Rüge
- ▶ Anweisung, die Datenverarbeitung den gesetzlichen Vorgaben anzupassen
- ▶ zeitlich begrenzte oder endgültiges Verbot der Datenverarbeitung

DATEN SCHUTZ PERFEKT UMGESETZT

Unser Beratungsteam bietet eine interdisziplinäre Expertise im Bereich Datenschutz und Datensicherheit. Mit spezialisierten Rechtsanwältinnen und -anwälten und zertifizierten Datenschutzbeauftragten sowie IT-Beraterinnen und -Beratern legen wir den Fokus auf die datenschutzkonforme Umsetzung von Systemen, Prozessen und Managementvorgaben. Die Verbindung von rechtlicher Beratung und praktischer Umsetzung steht dabei im Mittelpunkt unserer Lösungsorientierung. Unsere fundierte rechtliche Basis ermöglicht eine umfassende Betrachtung der technisch-organisatorischen Aspekte im Unternehmen, um eine ganzheitliche Lösung für komplexe Datenschutzerfordernisse zu schaffen.

**Sichere deine Daten richtig ab!
Kontaktiere uns jetzt für eine individuelle Beratung!**

[www.morgenstern-privacy.com/
deine-data-protection](http://www.morgenstern-privacy.com/deine-data-protection)





MORGENSTERN consecom GmbH

Große Himmelsgasse 1
DE - 67346 Speyer

Telefon

+49 (0) 6232 - 100119 44

E-Mail

contact@morgenstern-privacy.com

Passende Weiterbildungen finden Sie hier:

Weiterbildung zum Thema Recht

Finden Sie aus unserem erstklassigen Weiterbildungsangebot die für Ihre Bedürfnisse passende Fortbildung. Profitieren Sie von unseren maßgeschneiderten Seminaren und Lehrgängen mit erfahrenen, hochkarätigen Experten rund um das Thema Recht.

Wir garantieren fachlich hochwertige Weiterbildung für Ihren Erfolg – unsere ISO-Zertifizierungen nach 9001 und 21001 unterstreichen dies. [Jetzt informieren.](#)

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.

[Jetzt testen.](#)

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als [Inhouse-Training](#).

Jetzt individuelles [Angebot anfordern](#).

Dieses Whitepaper wurde Ihnen von unserem Content-Partner präsentiert. sichern Sie sich jetzt eine individuelle und zielgenaue Beratung.



MORGENSTERN legal | Dein Partner in Sachen IT-Recht & Digitalisierung
morgenstern-legal.com



MORGENSTERN privacy | Dein Partner in Sachen Datenschutz & IT-Sicherheit
morgenstern-privacy.com