FORUM

Die Datenschutzgrundverordnung Teil 1

präsentiert von MORGENSTERN

Inhalt

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

In diesem Whitepaper erfährst du alles über die Bestimmungen der Datenschutz-Grundverordnung.

- Was ist das überhaupt für ein Gesetz?
- Warum ist das so wichtig? Was gibt es alles für Vorgaben und wer muss diese umsetzen?

Da die Thematik rund um die Datenschutz-Grundverordnung durchaus komplex ist und die Betrachtung sämtlicher Inhalte den Rahmen eines einzigen Dokuments sprengen würde, haben wir uns dafür entschieden, das Ganze aufzuteilen.

Das Whitepaper besteht also aus insgesamt zwei Teilen (Part 1 und Part 2).

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. Was ist die Datenschutz-Grundverordnung?

Cookies, Datenschutzerklärung, Einwilligung, Auftragsverarbeitung – die datenschutzrechtlichen Anforderungen treiben viele Unternehmer in den Wahnsinn.

Und was genau hat es nun mit der Datenschutz-Grundverordnung (DS-GVO) auf sich? Wir erläutern dir dieses „Schreckgespenst", das seit 2018 durch die Unternehmen geistert.

Es handelt sich zunächst um eine EU-Verordnung, mit der die Speicherung und Verarbeitung personenbezogener Daten durch Verhaltensregeln und allgemeingültige Bedingungen vereinheitlicht wird. In Deutschland ersetzt sie das alte Bundesdatenschutzgesetz (BDSG).

Im Englischen spricht man von der „General Data Protection Regulation" (GDPR).

Im Kern ist es Aufgabe der DS-GVO, das Recht auf informationelle Selbstbestimmung zu unterstützen. Im Grunde besagt dieses Grundrecht: Jede*r darf selbst über seine Daten und deren Verarbeitung bestimmen.

Sie gilt verbindlich und unmittelbar in allen EU-Staaten. Eine Modifikation ist nicht möglich, die Umsetzung in nationales Recht nicht notwendig.

Allerdings existieren zahlreiche (über 60) Öffnungsklauseln. Sie erlauben es den Mitgliedsstaaten, unter gewissen Voraussetzungen, von den europäischen Standards abzuweichen. Es verbleibt also trotz Verordnungs-Charakter immer noch ein erheblicher Spielraum. Passender wäre es daher, die DS-GVO als ein Hybrid zwischen Verordnung und Richtlinie zu betiteln.

Aus diesem Grund trat in Deutschland zeitgleich das BDSG-neu in Kraft, welches das nationale Datenschutzrecht an die DS-GVO anpasst.

Beispiele für die Öffnungsklauseln:

- **Datenschutzbeauftragter (Art. 37 Abs. 4 DS-GVO):** Benennung
- **Meinungs- und Informationsfreiheit (Art. 85 DS-GVO):** Abweichungen von der DS-GVO, wenn notwendig um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen
- **Beschäftigtendatenschutz (Art. 88 DS-GVO):** Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Daten im Beschäftigungskontext vorsehen.

Ziele der DS-GVO

Die DS-GVO soll in der EU einen einheitlichen Standard gewährleisten, wie Unternehmen und Behörden mit personenbezogenen Daten, insbesondere denen ihrer Kundinnen und Kunden, Besucher*innen und Nutzer*innen, umgehen. Die Grundrechte natürlicher Personen, vor allem deren Recht auf informationelle Selbstbestimmung, sollen stärker geschützt werden. Kurz gesagt: Die Bürger*innen sollen mehr Kontrolle darüber erlangen, wann und wie ihre persönlichen Daten verwendet werden. Ihre Rechte diesbezüglich sollen gestärkt werden.

Zudem möchte man die Verantwortung der Unternehmen in Bezug auf den Umgang mit personenbezogenen Daten stärken. Die Verantwortlichen sowie Auftragsverarbeiter werden stärker in die Pflicht genommen, die Einhaltung der Datenschutzvorgaben nachweisen zu können.

Der Datenverkehr innerhalb der EU soll gewährleistet und die Bekanntmachung von Datenpannen sowie Datenlecks beschleunigt werden.

Da die Gesellschaft und die Technik sich ständig und immer rasanter fortentwickeln, waren die vorherigen Regelungen auch größtenteils nicht mehr zeitgemäß bzw. unbrauchbar.

Die Verordnung dient letztlich auch der Bestrebung eines effektiven europäischen Binnenmarkts. Bis 2018 galten europaweit sehr unterschiedliche Regelungen und Datenschutzstandards. Mit der DS-GVO versucht man sowohl den Interessen der Wirtschaftstreibenden als auch den Interessen der Verbraucher*innen gerecht zu werden. Während personenbezogene Daten innerhalb der Europäischen Union geschützt werden, gewährleistet man gleichzeitig den freien Datenverkehr im europäischen Binnenmarkt. Mögliche Wettbewerbsverzerrungen und Marktzugangsbarrieren, die durch unterschiedliche nationale Gesetze entstehen, können verhindert werden.

Geltungsbereich

Wen schützt die DS-GVO?

Es können nur natürliche Personen „Betroffene“ (und damit Rechteinhaber) im Sinne der DS-GVO sein. Unternehmen bzw. juristische Personen werden nicht von der DS-GVO geschützt, wohl aber die Daten der Personen, die Teil der juristischen Person oder bei ihr beschäftigt sind.

Was ist vom Schutzumfang umfasst?

„Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.“ [Art. 1 Abs. 2 DS-GVO der Verordnung]

Eindeutig ist die Frage nach dem „Schutzbereich“ damit aber nicht beantwortet.

Festzuhalten ist jedenfalls, dass es im Zentrum nicht um den Schutz von Daten an sich geht (was der Begriff ja nahelegen könnte). Beabsichtigt wird vielmehr der Schutz der Grundrechte und Grundfreiheiten der natürlichen Person, auf die sich diese Daten beziehen. Dementsprechend ist in der DS-GVO auch stets die Rede vom "Schutz personenbezogener Daten".

Gemäß Art. 2 Abs. 1 DS-GVO gilt die DS-GVO für „die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen."

Was sind personenbezogene Daten?

Art. 4 Nr. 1 DS-GVO: Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Im Einzelnen bedeutet das: Erstens sind nur Daten über natürliche Personen, nicht hingegen über juristische Personen, wie etwa Unternehmen, geschützt. Zweitens muss die Information Rückschlüsse auf die Person zulassen; anonymisierte Daten fallen also nicht in den Anwendungsbereich. Dabei reicht es für die Ablehnung des Vorliegens von Anonymität bereits aus, wenn die Person hinter den Daten mittelbar identifiziert werden kann, etwa durch die Zuordnung einer Kennnummer zu einem Kunden bzw. einer Kundin. Der Personenbezug ist also im konkreten Einzelfall stets in Hinblick darauf zu ermitteln, welche Identifizierungsmöglichkeiten der Verantwortliche besitzt. So können neben Namen oder Telefonnummern auch Standortdaten oder IP-Adressen personenbezogen sein.

Was sind automatisierte Verarbeitungen?

Automatisierte Verarbeitungen umfassen im Wesentlichen alle Verarbeitungen personenbezogener Daten durch eine elektronische Datenverarbeitung (Computer, Scanner, Digitalkameras, Smartphones) sowie strukturierte analoge Datensammlungen (wie etwa ein sortiertes Aktenregal).

Von dieser Definition – und damit von der Anwendbarkeit der DS-GVO – nicht umfasst werden lediglich unsortierte analoge Datensammlungen (z.B. unsortierte Zettel).

Für bestimmte Bereiche gibt es jedoch Sonderregeln (wie etwa für den Beschäftigtendatenschutz, vgl. § 26 BDSG) oder Ausnahmen von der Anwendbarkeit der DS-GVO.

Neben den personenbezogenen Daten im Sinne des Art. 4 Abs. 1 Nr. 1 DS-GVO gibt es auch noch die besonderen Kategorien personenbezogener Daten. Man spricht hier auch von sensiblen Daten.

Hierunter fallen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiösen oder weltanschaulichen Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben und zur sexuellen Orientierung. Neu in dieser Aufzählung sind biometrische Daten zur eindeutigen Identifizierung.

Grundsätzlich ist die Verarbeitung besonderer Kategorien personenbezogener Daten untersagt. Ausnahmen zu diesem Grundsatz findest du in Art. 9 Abs. 2 DS-GVO. Hiernach ist die Verarbeitung entgegen der Regelung gestattet, wenn

- die*der Betroffene ausdrücklich eingewilligt hat.
- eine arbeits- oder sozialrechtliche Verpflichtung dazu besteht.
- die Verarbeitung zur Ausübung oder Verteidigung von Rechtsansprüchen dient.
- sie zur Gesundheitsvorsorge, Diagnostik und Behandlung erforderlich ist.

Merke: Bei der Verarbeitung besonderer Kategorien personenbezogener Daten ist insbesondere die Erforderlichkeit einer Datenschutz-Folgeabschätzung zu bedenken.

Was gilt in Ausnahmefällen?

Die DS-GVO gilt nur dann nicht, wenn die Datenverarbeitung zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgt, die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, tätig werden – hierfür ist die neue Richtlinie 2016/680/EU maßgeblich.

Wo die Datenverarbeitung erfolgt, ist unerheblich: Ladenbesitzer, die Daten ihrer Kundinnen und Kunden im Ladenlokal verarbeiten, sind ebenso an die DS-GVO gebunden wie diejenigen, die online Produkte über Plattformen oder den eigenen Onlineshop vertreiben und hierbei Daten verarbeiten.

Es kommt auch nicht darauf an, wie umfangreich die unternehmerische Tätigkeit ist – selbst Kleinunternehmer sind den Regelungen unterworfen.

Neu ist insbesondere das Marktortprinzip. Die europäischen Vorgaben gelten nicht nur für Betriebe mit EU-Standort. Vielmehr sind auch Unternehmen in der Pflicht, die ihre Waren und Dienstleistungen innerhalb der EU anbieten. Solche Unternehmen aus Drittländern müssen sich also genauso an die DS-GVO halten. Sie sind zudem verpflichtet, einen bestellten Vertreter in der EU zu benennen, sofern sie nicht über eine Niederlassung in Europa verfügen.

Wichtig: Entscheidend ist nicht mehr, wo ein Artikel produziert wurde, sondern ob ein Produkt oder eine Dienstleistung innerhalb des europäischen Binnenmarkts angeboten wird.

Wer ist für die Umsetzung der DS-GVO Vorgaben verantwortlich?

Die zahlreichen Pflichten der DS-GVO richten sich an den sogenannten „Verantwortlichen“ für die Verarbeitung der personenbezogenen Daten. Doch wer ist das eigentlich?

Art. 4 Nr. 7 DS-GVO: „Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.“

- Demnach ist verantwortlich derjenige, der über das "Warum" und "Wie" der Datenverarbeitung entscheidet.

Grundsätzlich kann die Rolle des Verantwortlichen auch einer einzelnen Person zufallen. In der Praxis wird aber regelmäßig das Unternehmen selbst als Verantwortlicher angesehen, nicht der*die Geschäftsführer*in oder bestimmte Mitarbeitende.

Verantwortlicher ist beispielsweise:

- Ein Arbeitgeber für die Verarbeitung von Daten über seine Beschäftigten.
- Ein Händler für die Verarbeitung von Daten über seine Kundinnen und Kunden.
- Ein Webseitenbetreiber für die Verarbeitung von Daten über die Nutzer*innen seiner Webseite.

Achtung: Datenschutzbeauftragte sind nie die Verantwortlichen! Sie haben nur unterstützende und beratende Funktion.

Gemeinsame Verantwortlichkeit, Art. 26 Abs. 1 DS-GVO

Wenn mehrere Unternehmen zusammenarbeiten und gemeinsam über den Zweck und die Mittel der Verarbeitung entscheiden, liegt gemeinsame Verantwortlichkeit vor (z.B. auf Plattformen oder in Logistikketten).

- Entscheidend ist die Mitbestimmungsmöglichkeit über die Verarbeitungszwecke.
- Sie ist anhand des tatsächlichen Einflusses auf die Ausgestaltung der Datenverarbeitung zu bestimmen.
- Keine gleichberechtigte Entscheidung notwendig.
- Verantwortung muss auch nicht gleichwertig sein.
- Es müssen nicht alle Parteien Zugriff auf die gemeinsam verarbeiteten Daten erhalten.
- Es genügt, dass ein Beitrag zur Entscheidung über die Zwecke und Mittel einer Verarbeitung erbracht wird, die durch die andere Partei und primär in deren Interesse erfolgt.

Beispiel Facebook Fanpages:

*Der Inhaber der Fanpage erhält lediglich anonyme Statistiken und mehr will er auch im Zweifel gar nicht. Über die Fanpage ermöglicht er es Facebook aber überhaupt erst, personenbezogene Daten der Besucher*innen zu sammeln und auszuwerten. Der Fanpagebetreiber hat damit maßgeblichen Einfluss zumindest auf die Frage, ob personenbezogene Daten verarbeitet werden; er liefert einen kausalen Beitrag zur Datenverarbeitung durch Facebook.*

Dieses gemeinsame Element genügt laut EuGH, um eine gemeinsame Verantwortlichkeit zu begründen.

Die gemeinsamen Verantwortlichen sollten in einer transparenten Vereinbarung regeln, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere wenn es um die Betroffenenrechte und Informationspflichten geht.

MORGENSTERN als externe*r Datenschutzbeauftragte*r

Datenschutz und Datensicherheit sind Bereiche, die vom Zusammenspiel rechtlicher und technisch-organisatorischer Faktoren geprägt sind. Dementsprechend interdisziplinär ist unser Beratungsteam aufgestellt:

- auf IT-Recht spezialisierte Rechtsanwältinnen und -anwälte / Fachanwältinnen und -anwälte für IT-Recht
- IHK-zertifizierte Datenschutzbeauftragte
- IT-Berater*innen mit Schwerpunkt IT- und Netzwerksicherheit

Die datenschutzkonforme Umsetzung und Implementierung von Systemen, Prozessen und Managementvorgaben bilden den Kern unseres Beratungsansatzes. Hierbei ist uns die Schnittstelle zwischen rechtlicher Beratung und tatsächlicher Umsetzung von gesetzlichen Vorgaben besonders wichtig.

Mit einer fundierten rechtlichen Basis betrachten wir insbesondere auch die technisch-organisatorische Umsetzung im Unternehmen: Denn Datenschutz besteht nicht nur aus komplexen rechtlichen Rahmenbedingungen sondern auch aus der praktischen Umsetzung in jedem einzelnen Unternehmen.

Unsere praktische Erfahrung vermitteln wir zudem gezielt und praxisorientiert im Rahmen von Seminaren, Workshops und Zertifikatslehrgängen. Auch hierbei konzentrieren wir uns ausschließlich auf die Schwerpunktbereiche Datenschutz, IT-Sicherheit und IT-Recht.

Jetzt anfragen:
contact@morgenstern-privacy.com

03. Auftragsverarbeitung

Eine Auftragsverarbeitung liegt vor, wenn personenbezogene Daten durch einen Auftragsverarbeiter im Auftrag des Verantwortlichen weisungsgebunden verarbeitet werden (vgl. Art. 28 und Art. 29 DS-GVO).

- Er führt daher die Verarbeitung für den Auftraggeber nicht als Dritter i. S. d. Art. 4 Nr. 10 DS- GVO durch. Es besteht vielmehr zwischen dem auftragserteilenden Verantwortlichen und seinem Auftragsverarbeiter ein „Innenverhältnis". Die Verarbeitung durch den Auftragsverarbeiter wird deshalb grundsätzlich dem Verantwortlichen zugerechnet.

Der Verantwortliche hat dafür Sorge zu tragen, dass der Auftragsverarbeiter die Anforderungen der DS-GVO an den Schutz der Rechte von Betroffenen gewährleistet und geeignete technische und organisatorische Maßnahmen ergreift.

Zu empfehlen sind Folgekontrollen zur Überprüfung der technischen und organisatorischen Maßnahmen beim Auftragsverarbeiter!

Beispiele für Auftragsverarbeitungsverhältnisse:

- Datenverarbeitungstechnische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren
- Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist
- Werbeadressenverarbeitung in einem Lettershop
- Verarbeitung von Kundendaten durch ein Callcenter ohne wesentliche eigene Entscheidungsspielräume
- Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Webseiten (z.B. Betreuung von Kontaktformularen oder Nutzer*innenanfragen)
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten
- Auslagerung der Backup-Sicherheitsspeicherung und anderer Archivierungen
- Datenträgerentsorgung durch Dienstleister
- Prüfung oder Wartung (z.B. Fernwartung, externer Support) automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann
- Sicherheitsdienste, die an der Pforte Anlieferer- und Besucher*innendaten erheben
- externe Personen, Dienstleister, usw., die im Auftrag Messwerte in Mietwohnungen (Heizung, Strom, Wasser etc.) ablesen und/oder erfassen bzw. verarbeiten

Weitere Informationen dazu, wann insbesondere ein Auftragsverarbeitungsvertrag abzuschließen ist und welche Ausnahmen es gibt, sind in unserem **FAQ zur DS-GVO** zu finden.

Auftragsverarbeitungsvertrag

Der Verantwortliche hat vor Beginn der Datenverarbeitung mit dem Auftragsverarbeiter einen Vertrag abzuschließen, der die Mindestanforderungen des Art. 28 Abs. 3 S. 1 und 2 DS-GVO erfüllt.

Hierfür können sowohl individuelle Regelungen getroffen als auch von der EU-Kommission oder von der zuständigen Aufsichtsbehörde verabschiedete Standardvertragsklauseln verwendet werden. Ein wichtiger Bestandteil des Vertrages ist die Darstellung der erforderlichen Maßnahmen zur Sicherheit in der Verarbeitung (nach Art. 32 DS-GVO).

Subunternehmer-Einsatz

Will sich der Auftragsverarbeiter zur Erbringung der vereinbarten Dienstleistung Subunternehmen als weiterer Auftragsverarbeiter bedienen, benötigt er hierfür die vorherige (schriftliche oder elektronische) Genehmigung durch den Verantwortlichen (Art. 28 Abs. 2 DS-GVO). Wenn später weitere Subunternehmen eingesetzt werden sollen, ist das dem Verantwortlichen ebenfalls im Voraus mitzuteilen.

Dieser kann gegen die geplante Einbeziehung eines Subunternehmens Einspruch erheben. Falls keine Einigung erreicht wird, hat der Verantwortliche die Unterbeauftragung per Weisung zu unterbinden oder die Auftragsverarbeitung zu beenden.

04. Übermittlung an Drittländer

Länder außerhalb der EU bzw. des EWR werden in der DS-GVO als Drittländer bezeichnet. In der Praxis wird auch von „Drittstaaten“ gesprochen.

Bei der Übermittlung der personenbezogenen Daten an Drittländer oder an internationale Organisationen, sind zusätzlich zu den allgemeinen Anforderungen der DS-GVO, die du nun kennengelernt hast, die in Art. 45 ff. DS-GVO geregelten spezifischen Anforderungen einzuhalten. Dies gilt auch bei einer Weiterübermittlung der personenbezogenen Daten durch die empfangende Stelle im Drittland.

Praxis-Beispiel: Personenbezogene Daten werden bei einem ausländischen Cloud-Anbieter gespeichert.

Die DS-GVO sieht für Datentransfers in Drittländer folgende Möglichkeiten vor:

- *Feststellung der Angemessenheit des Datenschutzniveaus im Drittland durch die EU-Kommission (Art. 45 DS-GVO)*

Ein angemessenes Datenschutzniveau = dem in der DS-GVO gewährten Schutzniveau gleichwertig

- *Vorliegen geeigneter Garantien (Art. 46 DS-GVO)*
  - *Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, Art. 46 Abs. 2 b), Art. 47 DS-GVO)*
  - *Standarddatenschutzklauseln der Kommission oder einer Aufsichtsbehörde (Art. 46 Abs. 2 c) und d) DS-GVO)*
  - *Genehmigte Verhaltensregeln und genehmigter Zertifizierungsmechanismus (Art. 46 Abs. 2 e) und f) DS-GVO)*
  - *Einzeln ausgehandelte Vertragsklauseln (Art. 46 Abs. 3 a) DS-GVO)*

- *Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO) (weder Angemessenheitsbeschluss noch Garantien liegen vor)*
  - *Einwilligung (Art. 49 Abs. 1 Abs. 1 a) DS-GVO)*
  - *Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 Abs. 1 b) und c) DS-GVO)*
  - *Wichtige Gründe des öffentlichen Interesses (Art. 49 Abs. 1 Abs. 1 d) DS-GVO)*
  - *Verfolgung von Rechtsansprüchen (Art. 49 Abs. 1 Abs. 1 e) DS-GVO)*
  - *Schutz lebenswichtiger Interessen (Art. 49 Abs. 1 Abs. 1 f) DS-GVO)*
  - *Wahrung zwingender berechtigter Interessen (Art. 49 Abs. 1 Abs. 2 S. 1) DS-GVO)*

05. Grundsätze

In Art. 5 der DS-GVO sind wesentliche Aussagen darüber zu finden, wie personenbezogene Daten zu behandeln sind und wann sie überhaupt erhoben, abgefragt, gespeichert und verarbeitet werden dürfen.

Rechtmäßigkeit

Grundsätzlich ist die Verarbeitung personenbezogener Daten verboten. Die DS-GVO definiert Ausnahmen, für die eine Verarbeitung dennoch zulässig ist: „Verarbeitungsverbot mit Erlaubnisvorbehalt“.

Jede Verarbeitung personenbezogener Daten stellt einen Eingriff in die Privatsphäre dar. Daher benötigst du für jede Verarbeitungstätigkeit eine zulässige Rechtsgrundlage.

Art. 6 DS-GVO benennt unter anderem diese Rechtsgrundlagen:

- Einwilligung der betroffenen Person
- (Vor-)Vertragliches Verhältnis
- Rechtliche Verpflichtung
- Wahrung berechtigter Interessen

Verarbeitung nach Treu und Glauben

Die Verarbeitung nach Treu und Glauben gemäß Art. 5 Abs. 1 a) DS-GVO ist rechtlich schwerer zu fassen und lässt sich im Allgemeinen nur am konkreten Einzelfall unter Berücksichtigung aller Umstände beurteilen. Hierbei geht es meist um die Frage, ob ein bestimmtes Verhalten als redlich bzw. anständig angesehen werden kann. Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß sowie umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei Ihnen erhoben werden.

Transparenz

Der Grundsatz der Transparenz nach Art. 5 Abs. 1 a) DS-GVO soll insbesondere gewährleisten, dass die betroffene Person im engeren Sinne ihre Betroffenenrechte und im weiteren Sinne generell ihr Recht auf informationelle Selbstbestimmung wahrnehmen kann. Nur wenn die betroffene Person Kenntnis über die Verarbeitung hat, kann sie ihre diesbezüglichen Rechte geltend machen.

Das Prinzip der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst sind. Betroffen sind insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung sowie weitere Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten. Darüber hinaus stehen die Rechte der Betroffenen im Vordergrund, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffenden personenbezogenen Daten verarbeitet werden.

Zweckbindung

Daten dürfen nur zu bestimmten Zwecken verarbeitet werden. Der Zweck muss stets hinreichend bestimmt, eindeutig und legitim sein. Wichtig ist die Festlegung bereits vor der Erhebung der Daten, um die Transparenz zu wahren. So können betroffene Personen besser abschätzen, wer welche Daten über sie erhält. Es können mehrere Zwecke zugleich festgelegt werden.

Der Zweck kann auch geändert werden; dann muss der Sekundärzweck allerdings mit dem Primärzweck vereinbar sein (Art. 6 Abs. 4 DS-GVO), ansonsten ist eine neue Rechtsgrundlage erforderlich. Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Art. 89 Abs. 1 DS-GVO nicht als unvereinbar mit den ursprünglichen Zwecken.

Datenminimierung

Diese Regel besagt, dass die Verarbeitung personenbezogener Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss.

Somit dürfen nur solche Daten erhoben und verarbeitet werden, die für den konkreten Erhebungszweck von direkter Relevanz und für dessen Erfüllung erforderlich sind.

Die Datenverarbeitung ist stets auf das für die Zwecke notwendige Maß zu beschränken.

Datenrichtigkeit

Ferner müssen die Daten auf dem neuesten Stand sein, wenn es der Zweck der Datenverarbeitung erfordert.
Erforderlich ist es z.B. bei einer Speicherung von Zutrittsberechtigungen oder sonstigen Berechtigungen der betroffenen Person oder wenn Entscheidungen mit Rechtswirkungen davon abhängen (z. B. alter Negativvermerk bei der Schufa).

E-Learning zum Datenschutz

Professionell. Flexibel. Individualisierbar.

Die wirksame Vermittlung von Datenschutzthemen ist anspruchsvoll. Sie erfordert ein hohes Maß an Verständlichkeit, Transfer, Bezug zu realen Arbeitssituationen und Einstellung auf die Zielgruppe. Pflichtschulungen sind oft unbeliebt, weil sie diese und andere Kriterien nicht erfüllen.

Unsere E-Learnings ändern das. Verständlichkeit, Überschaubarkeit, Struktur, Anschaulichkeit und Beispiele stehen bei uns an erster Stelle. Datenschutz-Schulung kann angenehm und wirkungsvoll sein. Das sollen unsere E-Learnings zeigen.

Lektionen und Kapitel sorgen für inhaltliche Struktur und sinnvolle Input-Portionierung.

Die Schulungsinhalte im Datenschutz umfassen die grundlegenden Kenntnisse der DS-GVO, einschließlich dem Umgang mit personenbezogenen Daten und den damit verbundenen Risiken. Komplexe und abstrakte rechtliche Inhalte werden durch praxisnahe Beispiele verständlich und auch für Personen ohne Vorkenntnisse greifbar. Dadurch wird sichergestellt, dass deinen Mitarbeitenden die notwendigen Kenntnisse im Datenschutz für ihren Alltag vermittelt werden.

Ein Ziel unserer E-Learnings ist der Abbau von Unsicherheit, Stress und Überforderungsgefühlen im Zusammenhang mit dem Thema Datenschutz. Eine Lernerfreundliche Grundhaltung und Gestaltung sind dafür essenziell. Selbstgezeichnete Bilder verleihen unseren E-Learnings eine ganz persönliche Note und tragen zum guten Lerngefühl bei.

Ein wichtiger Teil von Lernprozessen sind Fragen. Bei uns wechseln sich Input und Fragen zur Wiederholung und zum Nachdenken ab. Am Ende jeder Lektion gibt es einen kleinen Abschlusstest. Zur Fortsetzung und zum Abschließen von Lektionen müssen die Fragen richtig beantwortet werden.

Jeder Kurs, jedes Paket und jedes Konzept soll individuell zu dir und deinen Ansprüchen passen!

Branchen- und firmenspezifische Gestaltung

In der MORGENSTERN E-Learning-Manufaktur werden E-Learnings nach Kundenwünschen erstellt. Anpassungen für einzelne Branchen sind dabei genauso möglich wie individuelle Formate für Firmen, Abteilungen oder bestimmte Zielgruppen. Die Menge der Lektionen und der inhaltliche Zuschnitt sind flexibel gestaltbar.

Je mehr wir über Bedürfnisse und Kontextbedingungen wissen, umso genauer sind die Inhalte und umso mehr finden sich die Mitarbeitenden darin wieder.

Die Lernenden ernst nehmen, individuelle Bedarfe und Besonderheiten verstehen und in E-Learnings umsetzen. Das ist unsere Antwort auf die Bedeutung des Themas Datenschutz.

Jetzt kostenlosen Probezugang sichern!

Mit unserem E-Learning-Demo bekommst du einen Eindruck davon, wie wir unsere E-Learnings gestalten. Du erhältst einen kostenfreien Einblick in…

- den Aufbau von Lektionen
- die Wissensabfragen
- die optische Gestaltung
- die Lernerfahrung

Speicherbegrenzung

Nach der in Art. 5 Abs. 1 e) DS-GVO normierten Speicherbegrenzung dürfen personenbezogene Daten nur in einer Form gespeichert werden, die die Identifizierung der Person nur so lange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist.

- Sobald die Speicherung personenbezogener Daten für den Verarbeitungszweck also nicht mehr erforderlich ist, müssen die personenbezogenen Daten gelöscht oder die Identifizierung der betroffenen Person aufgehoben werden. Ausnahmen ergeben sich beispielsweise für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke.

Eine Datenverarbeitung auf Verdacht oder Vorrat ist grundsätzlich unzulässig („Verbot der Vorratsdatenspeicherung").

Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. Diese werden insbesondere in Art. 32 DS-GVO konkretisiert.

Die Integrität der Daten muss durch technisch-organisatorische Sicherheitsmaßnahmen gewährleistet werden, die ein angemessenes Schutzniveau bieten. Dabei spielt der Stand der Technik ebenso eine Rolle wie das Risiko und die Schwere einer möglichen Verletzung von Betroffenenrechten und -freiheiten.

Rechenschaftspflicht

Die Rechtmäßigkeit der Verarbeitung nach Art. 5 Abs. 1 a) DS-GVO wird grundsätzlich in Art. 6 DS- GVO näher konkretisiert. Die Verarbeitung von personenbezogenen Daten ist demnach rechtmäßig, wenn eine der in Art. 6 Abs. 1 a) bis f) DS-GVO genannten Voraussetzungen vorliegt.

Nun weißt du schon eine Menge über die Datenschutz-Grundverordnung. Das ist aber noch nicht alles. Denn im zweiten Teil unseres Whitepapers geht es weiter. Dort erfährst du dann beispielsweise alles über die Betroffenenrechte, die Datensicherheit oder den besonderen Handlungsbedarf bei Webseiten und Cookies. Und hast du dich nicht auch schon mal gefragt, welche Sanktionen bei Verstößen in Frage kommen? Der zweite Teil kommt nächsten Monat.

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.

FORUM · Institut für Management GmbH · Postfach 10 50 60 · 69040 Heidelberg · Germany
Tel. +49 6221 500-500 · Fax +49 6221 500-555 · www.forum-institut.de