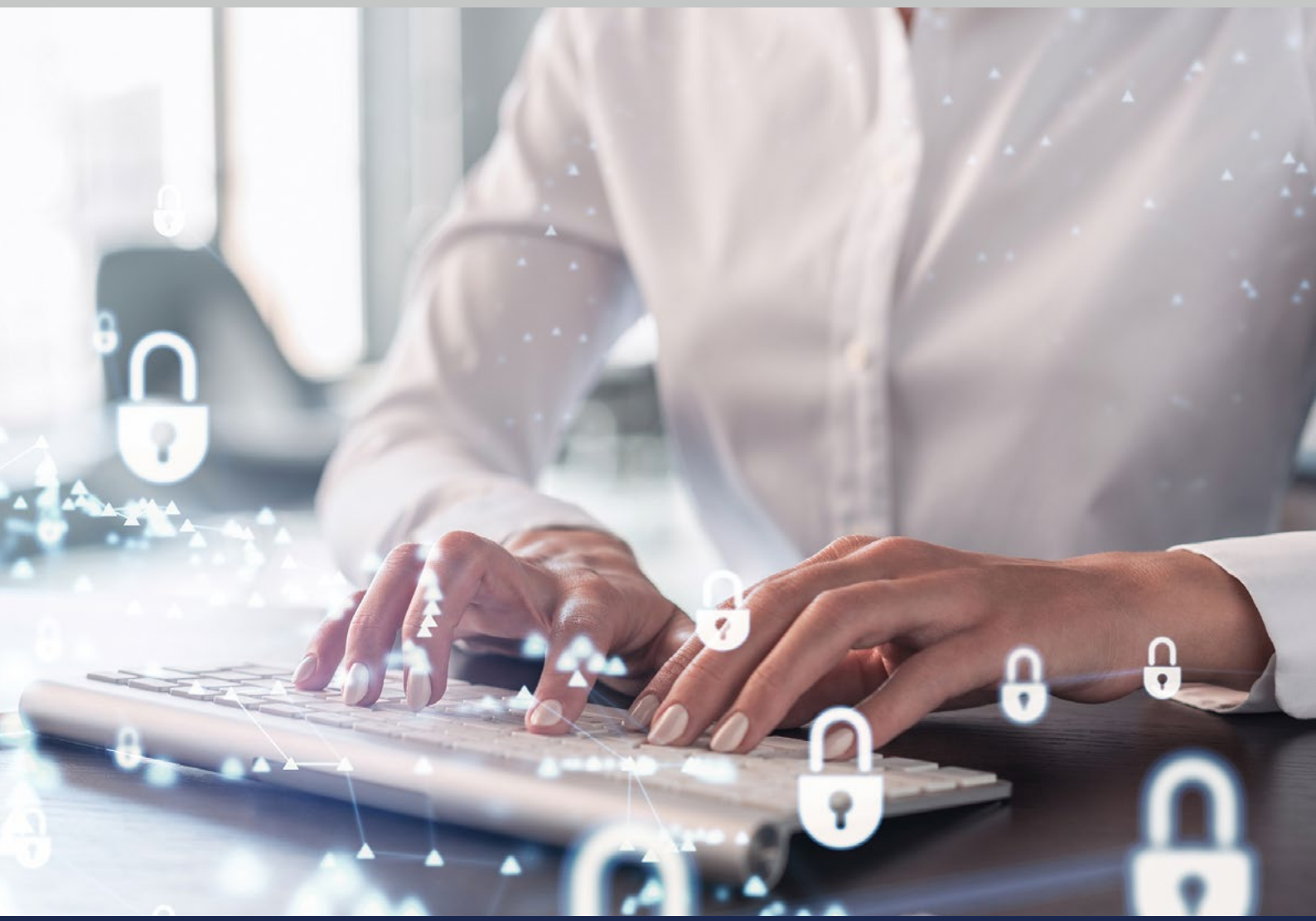
FORUM



Datenschutz-Grundverordnung Teil 2

Betroffenenrechte, Datensicherheit, Web und Sanktionen

Sehr geehrte*r Leser*in,

dieser zweite Teil des Whitepapers zur Datenschutz-Grundverordnung vertieft die praktischen Anforderungen, die sich für Unternehmen im täglichen Umgang mit personenbezogenen Daten ergeben. Nachdem Teil 1 die Grundlagen, den Geltungsbereich und die Datenschutzgrundsätze beleuchtet hat, stehen nun folgende Themen im Mittelpunkt: Betroffenenrechte, Pflichten der Verantwortlichen, Datensicherheit, besondere Anforderungen bei Webseiten und Social Media sowie Haftung und Sanktionen.

Diese aktualisierte Fassung berücksichtigt Entwicklungen bis April 2026 – darunter aktuelle EuGH-Urteile zum Schadensersatz nach Art. 82 DS-GVO, die verschärfte Haltung der Aufsichtsbehörden zu Cookie-Bannern und Dark Patterns sowie die Auswirkungen des EU AI Act auf datenschutzrechtliche Pflichten.

Bitte beachten Sie: Dieses Whitepaper dient der Orientierung und ersetzt keine individuelle Rechtsberatung. Ziehen Sie bei konkreten Fragen stets Ihren oder Ihre Datenschutzbeauftragte*n oder eine Fachkanzlei hinzu.

Wir wünschen Ihnen viel Freude beim Lesen.

Dieses Whitepaper wurde mit Hilfe von Sonnet 4.6 erstellt.

Inhalt

01 Einführung

Die Datenschutz-Grundverordnung wirft immer wieder Fragen auf: Was ist das überhaupt für ein Gesetz? Wen betrifft es? Welche Vorgaben müssen umgesetzt werden? Dieses Whitepaper gibt Ihnen strukturierte Antworten auf diese Fragen und bereitet Sie auf die praktischen Anforderungen des Datenschutzrechts vor.

Da die Thematik komplex ist und sich ständig weiterentwickelt, empfehlen wir, dieses Dokument regelmäßig auf den aktuellen Stand zu bringen und bei konkreten Rechtsfragen stets den oder die Datenschutzbeauftragte hinzuzuziehen.

02 Was ist die Datenschutz-Grundverordnung?

Cookies, Datenschutzerklärungen, Einwilligungen, Auftragsverarbeitung – die datenschutzrechtlichen Anforderungen stellen viele Unternehmen vor große Herausforderungen. Was hat es nun genau mit der Datenschutz-Grundverordnung auf sich?

Bei der DS-GVO handelt es sich um eine EU-Verordnung, die die Speicherung und Verarbeitung personenbezogener Daten durch verbindliche Verhaltensregeln EU-weit vereinheitlicht. In Deutschland hat sie das alte Bundesdatenschutzgesetz (BDSG) ablöst. Im Englischen spricht man von der „General Data Protection Regulation“ (GDPR).

Ihr zentrales Ziel ist es, das Recht auf informationelle Selbstbestimmung zu stärken: Jede Person soll selbst über ihre Daten und deren Verarbeitung bestimmen können.

Die DS-GVO gilt verbindlich und unmittelbar in allen EU-Mitgliedstaaten. Eine Umsetzung in nationales Recht ist nicht erforderlich. Allerdings existieren über 60 Öffnungsklauseln, die es den Mitgliedstaaten erlauben, unter bestimmten Voraussetzungen eigene Regelungen zu treffen. In Deutschland trat daher zeitgleich das neue BDSG (BDSG-neu) in Kraft.

Beispiele für Öffnungsklauseln

- Datenschutzbeauftragte (Art. 37 Abs. 4 DS-GVO): Möglichkeit zur nationalen Regelung der Bestellpflicht
- Meinungs- und Informationsfreiheit (Art. 85 DS-GVO): Abweichungen zum Ausgleich mit der Meinungsfreiheit
- Beschäftigtendatenschutz (Art. 88 DS-GVO): Nationale Regelungen zum Schutz von Arbeitnehmer*innen

Ziele der DS-GVO

Die DS-GVO verfolgt mehrere Ziele gleichzeitig:

- Einheitlicher Datenschutzstandard in der gesamten EU
- Stärkung der Grundrechte natürlicher Personen, insbesondere des Rechts auf informationelle Selbstbestimmung
- Mehr Kontrolle für Bürger*innen über die Verwendung ihrer persönlichen Daten
- Größere Verantwortung für Unternehmen beim Umgang mit personenbezogenen Daten
- Beschleunigung der Meldepflicht bei Datenpannen und Datenlecks
- Förderung eines effektiven europäischen Binnenmarkts

Geltungsbereich

Nur natürliche Personen können „Betroffene“ im Sinne der DS-GVO und damit Rechteinhaber sein. Unternehmen als juristische Personen sind nicht direkt geschützt, wohl aber die Daten der natürlichen Personen, die in ihnen tätig sind oder mit ihnen in Verbindung stehen.

Rechtliche Grundlage: *Art. 1 Abs. 2 DS-GVO: „Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.“*

Gemäß Art. 2 Abs. 1 DS-GVO gilt die Verordnung 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.“

ⓘ Hinweis: Nicht umfasst sind lediglich unsortierte analoge Datensammlungen, z. B. unstrukturierte Notizzettel. Alle anderen Datensammlungen – auch strukturierte Aktenordner – fallen grundsätzlich in den Anwendungsbereich.

Was sind personenbezogene Daten?

Gemäß Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten „Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen." Das umfasst:

- Namen, Anschriften, Telefonnummern
- E-Mail-Adressen und Online-Kennungen
- IP-Adressen und Standortdaten
- Kennummern, die einer Person zugeordnet werden können

Anonymisierte Daten fallen nicht in den Anwendungsbereich – sofern eine Re-Identifizierung wirklich ausgeschlossen ist. Pseudonymisierte Daten hingegen bleiben personenbezogen.

Besondere Kategorien personenbezogener Daten

Einige Datenkategorien sind besonders sensibel und genießen erhöhten Schutz (Art. 9 DS-GVO):

- Rassische und ethnische Herkunft
- Politische Meinungen, religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische und biometrische Daten zur eindeutigen Identifizierung
- Gesundheitsdaten
- Daten zum Sexualleben und zur sexuellen Orientierung

Die Verarbeitung dieser Daten ist grundsätzlich untersagt. Ausnahmen sind in Art. 9 Abs. 2 DS-GVO geregelt, z. B. bei ausdrücklicher Einwilligung, arbeitsrechtlicher Verpflichtung oder medizinischer Notwendigkeit.

ⓘ Hinweis: Bei der Verarbeitung besonderer Kategorien personenbezogener Daten ist stets zu prüfen, ob eine Datenschutz-Folgeabschätzung (DSFA) gemäß Art. 35 DS-GVO erforderlich ist.

Neu / Aktuell: Biometrische Daten – darunter z. B. Gesichtserkennung oder Fingerabdruckscans – sind im Kontext des EU AI Act (in Kraft seit August 2024) besonders reguliert. Hochrisiko-KI-Systeme, die biometrische Daten verarbeiten, unterliegen zusätzlichen Anforderungen und müssen in der EU-Datenbank registriert werden.

Wer ist für die Umsetzung verantwortlich?

Die Pflichten der DS-GVO richten sich an den sogenannten „Verantwortlichen" (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."

Verantwortliche sind beispielsweise:

- Ein Arbeitgeber für die Verarbeitung von Daten über seine Beschäftigten
- Ein Händler für die Daten seiner Kund*innen
- Ein Webseitenbetreiber für die Nutzerdaten seiner Plattform

ⓘ Hinweis: Datenschutzbeauftragte sind nie die Verantwortlichen! Sie haben ausschließlich beratende und unterstützende Funktion.

Gemeinsame Verantwortlichkeit (Art. 26 DS-GVO)

Wenn mehrere Unternehmen gemeinsam über Zweck und Mittel einer Verarbeitung entscheiden, liegt gemeinsame Verantwortlichkeit vor. Dies ist z. B. bei gemeinsamen Plattformen, Logistikketten oder Marketing-Kooperationen der Fall. Entscheidend ist die Mitbestimmungsmöglichkeit über die Verarbeitungszwecke.

Ein bekanntes Beispiel aus der EuGH-Rechtsprechung: Betreiber von Facebook-Fanpages sind gemeinsam verantwortlich mit Meta, da sie durch die Nutzung der Fanpage die Datenerhebung durch Facebook erst ermöglichen.

Neu / Aktuell: Der EuGH hat in neueren Entscheidungen (u. a. C-446/21 – Maximilian Schrems gegen Meta, 2023) die gemeinsame Verantwortlichkeit und die Anforderungen an die Einwilligung bei sozialen Netzwerken weiter präzisiert. Unternehmen, die Social-Media-Plugins oder externe Tracking-Dienste einsetzen, sollten ihre Datenschutzerklärungen und Einwilligungsmechanismen regelmäßig überprüfen.

03 Auftragsverarbeitung

Eine Auftragsverarbeitung liegt vor, wenn personenbezogene Daten durch einen Auftragsverarbeiter im Auftrag und auf Weisung des Verantwortlichen verarbeitet werden (Art. 28 und 29 DS-GVO). Der Auftragsverarbeiter handelt nicht eigenständig, sondern ist an die Weisungen des Verantwortlichen gebunden.

Der Verantwortliche bleibt datenschutzrechtlich „Herr der Daten“ und hat dafür zu sorgen, dass der Auftragsverarbeiter die Anforderungen der DS-GVO erfüllt und geeignete technische sowie organisatorische Maßnahmen (TOM) ergreift.

Typische Beispiele für Auftragsverarbeitungsverhältnisse

- Lohn- und Gehaltsabrechnung durch Rechenzentren
- Cloud-Computing ohne inhaltlichen Datenzugriff des Anbieters
- Werbeadressenverarbeitung in einem Lettershop
- Callcenter-Dienstleistungen ohne eigene Entscheidungsspielräume
- Auslagerung der E-Mail-Verwaltung oder Betreuung von Kontaktformularen
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten
- Backup-Sicherheitsspeicherung und Archivierung
- Datentägerentsorger
- IT-Fernwartung und externer Support, wenn Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann
- Sicherheitsdienste, die Besucher*innendaten erfassen

Auftragsverarbeitungsvertrag

Vor Beginn der Verarbeitung muss ein Vertrag abgeschlossen werden, der die Mindestanforderungen des Art. 28 Abs. 3 DS-GVO erfüllt. Hierbei können individuelle Regelungen getroffen oder die von der EU-Kommission verabschiedeten Standardvertragsklauseln (SCC) verwendet werden.

Ein zentraler Bestandteil des Vertrags ist die Darstellung der technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DS-GVO. Diese sind regelmäßig zu überprüfen.

Neu / Aktuell: Die EU-Kommission hat im Juni 2021 aktualisierte Standardvertragsklauseln (SCC) veröffentlicht, die seit dem 27. September 2021 verbindlich gelten. Ältere SCC-Versionen dürfen seit dem 27. Dezember 2022 nicht mehr für neue Verträge verwendet werden. Prüfen Sie, ob Ihre bestehenden Auftragsverarbeitungsverträge auf die aktuellen Klauseln aktualisiert wurden.

Subunternehmer-Einsatz

Möchte ein Auftragsverarbeiter Subunternehmen beauftragen, benötigt er hierfür die vorherige Genehmigung des Verantwortlichen (Art. 28 Abs. 2 DS-GVO). Nachträgliche Änderungen beim Subunternehmereinsatz müssen ebenfalls vorab mitgeteilt werden. Der Verantwortliche kann Einspruch erheben.

04 Übermittlung an Drittländer

Länder außerhalb der EU bzw. des Europäischen Wirtschaftsraums (EWR) bezeichnet die DS-GVO als Drittländer. Bei der Übermittlung personenbezogener Daten dorthin gelten über die allgemeinen DS-GVO-Anforderungen hinaus die spezifischen Vorschriften der Art. 45 ff. DS-GVO.

Praxisbeispiel: Personenbezogene Daten werden bei einem ausländischen Cloud-Anbieter (z. B. in den USA) gespeichert.

Möglichkeiten für rechtskonforme Drittlandtransfers

- Angemessenheitsbeschluss der EU-Kommission (Art. 45 DS-GVO): Das Datenschutzniveau im Drittland entspricht dem europäischen Standard.
- Geeignete Garantien (Art. 46 DS-GVO): z. B. Standardvertragsklauseln (SCC), Binding Corporate Rules (BCR) oder genehmigte Verhaltensregeln
- Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO): z. B. ausdrückliche Einwilligung, Vertragserfüllung oder lebenswichtige Interessen

Neu / Aktuell: Nach dem Schrems-II-Urteil des EuGH (C-311/18, 2020) wurde der EU-U.S. Privacy Shield für ungültig erklärt. Seit Juli 2023 gilt der EU-U.S. Data Privacy Framework (DPF) als neuer Angemessenheitsbeschluss für zertifizierte US-Unternehmen. Dennoch bleibt die politische Stabilität des DPF unsicher. Es empfiehlt sich, Drittlandtransfers vorsorglich zusätzlich auf aktualisierte Standardvertragsklauseln (SCC, Fassung 2021) zu stützen und eine Transfer Impact Assessment (TIA) durchzuführen.

Hinweis: Grundsätzlich gilt: Vor jedem Datentransfer in ein Drittland muss geprüft werden, ob eine der o. g. Rechtsgrundlagen vorliegt. Im Zweifel ist der oder die Datenschutzbeauftragte hinzuzuziehen.

05 Grundsätze der DS-GVO (Art. 5)

In Art. 5 DS-GVO sind die wesentlichen Grundsätze für den Umgang mit personenbezogenen Daten festgelegt. Sie bilden das Fundament jeder datenschutzkonformen Verarbeitung.

Rechtmäßigkeit

Grundsätzlich ist die Verarbeitung personenbezogener Daten verboten – es sei denn, es liegt eine der in Art. 6 DS-GVO genannten Rechtsgrundlagen vor („Verarbeitungsverbot mit Erlaubnisvorbehalt“). Die wichtigsten Rechtsgrundlagen sind:

- Einwilligung der betroffenen Person (Art. 6 Abs. 1 a) DS-GVO)
- Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen (Art. 6 Abs. 1 b) DS-GVO)
- Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 c) DS-GVO)
- Wahrung berechtigter Interessen (Art. 6 Abs. 1 f) DS-GVO) – sofern keine überwiegenden Interessen der betroffenen Person entgegenstehen

Verarbeitung nach Treu und Glauben

Die Verarbeitung muss fair und redlich erfolgen. Betroffene Personen müssen in der Lage sein, von der Verarbeitung zu erfahren und vollständig darüber informiert zu werden.

Transparenz

Alle Informationen über die Datenverarbeitung müssen leicht zugänglich, verständlich und in klarer Sprache abgefasst sein. Betroffene müssen wissen, wer ihre Daten zu welchem Zweck verarbeitet.

Zweckbindung

Daten dürfen nur zu bestimmten, eindeutigen und legitimen Zwecken erhoben und verarbeitet werden. Eine spätere Weiterverarbeitung für einen anderen Zweck ist nur zulässig, wenn der neue Zweck mit dem ursprünglichen vereinbar ist oder eine neue Rechtsgrundlage vorliegt (Art. 6 Abs. 4 DS-GVO).

ⓘ Hinweis: Ausnahmen gelten für Archivzwecke im öffentlichen Interesse, wissenschaftliche Forschung und Statistik (Art. 89 Abs. 1 DS-GVO).

Datenminimierung

Es dürfen nur die Daten erhoben und verarbeitet werden, die für den konkreten Zweck tatsächlich erforderlich sind. Die Verarbeitung ist auf das notwendige Maß zu beschränken.

Datenrichtigkeit

Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Dies ist besonders relevant bei Berechtigungen, Bonitätsdaten oder medizinischen Angaben.

Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für den Verarbeitungszweck erforderlich ist. Danach müssen sie gelöscht oder anonymisiert werden. Eine Datenspeicherung „auf Vorrat“ ist grundsätzlich unzulässig.

Neu / Aktuell: Aktuelle EuGH-Rechtsprechung (u. a. C-200/23, 2024) bestätigt, dass eine unzulässig lange Datenspeicherung über die Speicherfrist hinaus einen immateriellen Schaden begründen kann, der zu Schadensersatzansprüchen führt (Art. 82 DS-GVO). Löschkonzepte sind daher keine optionale Maßnahme, sondern Pflicht.

Integrität und Vertraulichkeit

Personenbezogene Daten müssen durch geeignete technische und organisatorische Maßnahmen (TOM) geschützt werden – gegen unbefugten Zugriff, Verlust, Zerstörung oder Schädigung (Art. 32 DS-GVO). Der Maßstab richtet sich nach dem aktuellen Stand der Technik und dem Risikoniveau.

Rechenschaftspflicht

Verantwortliche müssen nicht nur die DS-GVO einhalten, sondern dies auch nachweisen können. Dazu gehören u. a. ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO), dokumentierte Datenschutzrichtlinien und nachweisliche Schulungsmaßnahmen.

Rechtliche Grundlage: *Art. 5 Abs. 2 DS-GVO: „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können."*

06 Marktortprinzip und räumlicher Anwendungsbereich

Ein wichtiges Merkmal der DS-GVO ist das sogenannte Marktortprinzip: Die europäischen Datenschutzvorgaben gelten nicht nur für Unternehmen mit Sitz in der EU, sondern für alle Unternehmen weltweit, die Waren oder Dienstleistungen innerhalb der EU anbieten oder das Verhalten von EU-Bürger*innen beobachten.

Drittländische Unternehmen ohne EU-Niederlassung sind verpflichtet, einen bestellten Vertreter in der EU zu benennen.

ⓘ *Hinweis: Entscheidend ist nicht, wo ein Produkt hergestellt wurde, sondern ob es innerhalb des europäischen Binnenmarkts angeboten wird. Auch Kleinunternehmen sind den Regelungen der DS-GVO vollumfänglich unterworfen.*

Ausblick: Teil 2 dieses Whitepapers

Dieser erste Teil hat Ihnen die Grundlagen der DS-GVO vermittelt: ihren Zweck, ihren Geltungsbereich, die zentralen Grundsätze sowie die Anforderungen an Auftragsverarbeitung und Drittlandtransfers.

Im zweiten Teil erwartet Sie unter anderem:

- Betroffenenrechte: Auskunft, Löschung, Datenübertragbarkeit und mehr
- Datensicherheit: Technische und organisatorische Maßnahmen (TOM) und Meldepflichten bei Datenpannen
- Webseiten und Cookies: Anforderungen an Cookie-Banner, Einwilligungen und Tracking
- Sanktionen: Bußgelder, Schadensersatz und aktuelle Behördenentscheidungen
- KI und Datenschutz: Anforderungen aus DS-GVO und EU AI Act

Das FORUM Institut für Management bietet regelmäßig Seminare und Zertifikatslehrgänge zu den Themen Datenschutz, Compliance und Datensicherheit an. Wir laden Sie herzlich ein, sich über unser aktuelles Seminarprogramm zu informieren.

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. 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 unverbindlich testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

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

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