Europäische Kommission

Die Datenschutz-Grundverordnung: neue Möglichkeiten, neue Pflichten

Was jedes Unternehmen über die Datenschutz-Grundverordnung der EU wissen muss

Justiz und Verbraucher

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2018

Print	ISBN 978-92-79-79420-9	doi:10.2838/54937	DS-01-18-082-DE-C
PDF	ISBN 978-92-79-79439-1	doi:10.2838/191560	DS-01-18-082-DE-N

INHALTSVERZEICHNIS

KAPITEL 1

EINE GESCHÄFTSMÖGLICHKEIT

Die Datenschutz-Grundverordnung regelt die Verarbeitung und Verwaltung personenbezogener Daten durch Unternehmen. Die ab 25. Mai 2018 für alle Unternehmen und Organisationen (d. h. Krankenhäuser, öffentliche Verwaltungen usw.) geltende Verordnung stellt die größte Änderung der EU-Datenschutzvorschriften seit mehr als 20 Jahren dar.

Die Datenschutz-Grundverordnung gibt nicht nur Bürgern mehr Kontrolle über die Verwendung ihrer personenbezogenen Daten, sondern bringt auch eine bedeutende Straffung des Regelungsumfelds für Unternehmen mit sich, indem ein einheitlicher Rahmen für die Datenschutzgesetzgebung in der gesamten EU festgelegt wird. Mit anderen Worten: Statt eigener Datenschutzvorschriften in jedem Land unterliegt nun die ganze EU einer einzigen Verordnung. Entsprechend müssen Unternehmen, die in verschiedenen Ländern tätig sind, nicht mehr mehrere – häufig unterschiedliche – Vorschriften einhalten. Stattdessen müssen sie nur noch der Datenschutz-Grundverordnung entsprechen, um ihre Dienstleistungen in der gesamten EU anbieten zu können.

Wie Ihr Unternehmen von der Datenschutz-Grundverordnung profitieren kann

- **Eine Union, ein Gesetz:** Einheitliche Vorschriften vereinfachen Geschäftstätigkeiten in der EU und senken die Kosten für Unternehmen.
- **Verfahren der Zusammenarbeit und Kohärenz:** In den meisten Fällen haben Unternehmen nur mit einer Datenschutzbehörde zu tun.
- **Europäische Regeln auf europäischem Boden:** Außerhalb der EU ansässige Unternehmen, die natürlichen Personen in der EU Waren und Dienstleistungen anbieten, müssen dieselben Regeln anwenden wie europäische Unternehmen.
- **Risikobasierter Ansatz:** Die Datenschutz-Grundverordnung verhindert aufwendige, pauschale Pflichten und sieht stattdessen auf die jeweiligen Risiken zugeschnittene Pflichten vor.
- **Innovationsfreundliche Regeln:** Die Datenschutz-Grundverordnung ist technologieneutral.

Es dreht sich alles um Vertrauen

Der Schutz personenbezogener Daten ist Menschen wichtig. Darum bringen sie digitalen Umgebungen nach wie vor wenig Vertrauen entgegen. Eine Eurobarometer-Umfrage stellt fest:

- Acht von zehn Befragten haben das Gefühl, nicht die vollständige Kontrolle über ihre personenbezogenen Daten zu haben;
- sechs von zehn Befragten geben an, Online-Unternehmen nicht zu vertrauen;
- mehr als 90 % der Europäer wünschen sich dieselben Datenschutzvorschriften in allen EU-Ländern.

„Unternehmen, die personenbezogene Daten nicht angemessen schützen, laufen Gefahr, das Vertrauen der Verbraucher zu verlieren. Doch genau dieses Vertrauen ist entscheidend, um Menschen dazu zu bewegen, neue Produkte und Dienstleistungen zu verwenden.“

Die Datenschutz-Grundverordnung ist für Ihr Unternehmen eine neue Möglichkeit, das Vertrauen der Verbraucher durch eine risikobasierte Verwaltung personenbezogener Daten zu stärken.

KAPITEL 2

DIE DATENSCHUTZ-GRUNDVERORDNUNG VERSTEHEN

Gilt die Datenschutz-Grundverordnung für mich?

Zusammenfassend gilt die Datenschutz-Grundverordnung für ***alle*** Unternehmen, die

personenbezogene Daten automatisiert oder **manuell verarbeiten** (sofern die Daten nach bestimmten Kriterien geordnet sind).

Auch wenn Ihr Unternehmen Daten nur im Auftrag anderer Unternehmen verarbeitet, müssen Sie trotzdem die Vorschriften einhalten.

Die Datenschutz-Grundverordnung gilt, wenn

- Ihr Unternehmen personenbezogene Daten verarbeitet und in der EU ansässig ist, ungeachtet dessen, wo die Datenverarbeitung tatsächlich stattfindet; oder
- Ihr Unternehmen außerhalb der EU ansässig ist, aber Personen in der EU Waren oder Dienstleistungen anbietet oder das Verhalten dieser Personen beobachtet.

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen. Dazu zählen unter anderem:

- Name,
- Anschrift und Telefonnummer,
- Ort,
- Gesundheitsdaten,
- Einkommens- und Bankdaten,
- kulturelle Vorlieben
- ... und so weiter.

Personenbezogene Daten, die anonymisiert oder pseudonymisiert wurden, aber dennoch zur erneuten Identifizierung einer Person genutzt werden können, fallen ebenfalls in den Anwendungsbereich der Datenschutz-Grundverordnung. Personenbezogene Daten, die unwiderruflich auf eine Weise anonymisiert wurden, dass die Person nicht mehr identifizierbar ist, gelten jedoch nicht als personenbezogene Daten und werden entsprechend nicht durch die Datenschutz-Grundverordnung geregelt.

Zudem ist die Datenschutz-Grundverordnung technologieneutral, d. h., sie schützt personenbezogene Daten ungeachtet der verwendeten Techniken und der Art und Weise der Speicherung der personenbezogenen Daten. Ob Ihr Unternehmen nun personenbezogene Daten mittels eines komplexen IT-Systems oder über papierbasierte Akten verarbeitet und speichert – in beiden Fällen unterliegen Sie der Datenschutz-Grundverordnung.

„Ob Ihr Unternehmen nun personenbezogene Daten mittels eines komplexen IT-Systems oder über papierbasierte Akten verarbeitet und speichert – in beiden Fällen unterliegen Sie der Datenschutz-Grundverordnung.“

Bei besonderen (sensiblen) Kategorien personenbezogener Daten ist besondere Vorsicht geboten

Umfassen die von Ihnen erhobenen personenbezogenen Daten Informationen über die Gesundheit, Rasse, sexuelle Orientierung, Religion, politischen Überzeugungen oder Gewerkschaftszugehörigkeit einer Person, so gelten diese Daten als sensibel. Ihr Unternehmen darf diese Daten nur unter bestimmten Bedingungen verarbeiten und Sie müssen unter Umständen zusätzliche Garantien, z. B. in Form einer Verschlüsselung, umsetzen.

Was gilt als Verarbeitung personenbezogener Daten?

Gemäß Datenschutz-Grundverordnung fallen Handlungen wie das Erheben, die Verwendung und das Löschen personenbezogener Daten unter die Definition der Verarbeitung personenbezogener Daten.

Lassen Sie Ihre Geschäftsräume per Video überwachen? Konsultieren Sie eine personenbezogene Daten enthaltende Datenbank zu geschäftlichen Zwecken? Versenden Sie E-Mails zu Werbezwecken? Löschen Sie (digitale) Mitarbeiterakten oder schreddern Sie Dokumente? Oder veröffentlichen Sie Fotos von Personen auf Ihrer Website oder auf Social-Media-Kanälen?

Haben Sie auch nur eine dieser Fragen mit „Ja“ beantwortet, verarbeitet Ihr Unternehmen zweifellos personenbezogene Daten.

Wie trägt die Datenschutz-Grundverordnung zur Kostensenkung bei?

Die Datenschutz-Grundverordnung trägt den Bedürfnissen von Unternehmen Rechnung. Ziel der Verordnung ist es unter anderem, Verwaltungsauflagen zu beseitigen, um Kosten zu senken und den Verwaltungsaufwand zu minimieren:

- **Keine vorherigen Meldungen mehr**: Durch die Reform werden die meisten vorherigen Meldungen bei Aufsichtsbehörden abgeschafft, sodass auch die damit verbundenen Kosten entfallen.
- **Datenschutzbeauftragte**: Unternehmen müssen vor allem dann einen Datenschutzbeauftragten ernennen, wenn ihre Kerntätigkeiten die Verarbeitung sensibler Daten in großem Umfang bzw. die regelmäßige systematische Überwachung von Personen in großem Umfang umfassen. Öffentliche Verwaltungen sind verpflichtet, einen Datenschutzbeauftragten zu ernennen.
- **Datenschutz-Folgenabschätzungen**: Unternehmen sind nur dann verpflichtet, eine Datenschutz-Folgenabschätzung durchzuführen, wenn eine vorgeschlagene Datenverarbeitungstätigkeit ein hohes Risiko für die Rechte und Freiheiten von Personen mit sich bringt.
- **Führen von Verzeichnissen**: Unternehmen mit weniger als 250 Mitarbeitern müssen keine Verzeichnisse führen, es sei denn, die Datenverarbeitung erfolgt nicht nur gelegentlich oder betrifft sensible Daten.

„Ziel der Verordnung ist es, Verwaltungsauflagen zu beseitigen, um Kosten zu senken und den Verwaltungsaufwand zu minimieren.“

KAPITEL 3

IHRE PFLICHTEN IM RAHMEN DER DATENSCHUTZ-GRUNDVERORDNUNG

Die Datenschutz-Grundverordnung schafft in Bezug auf die Datenverarbeitung direkte Pflichten für Unternehmen auf EU-Ebene. Gemäß Datenschutz-Grundverordnung können Unternehmen personenbezogene Daten nur unter bestimmten Bedingungen verarbeiten. So sollte die Verarbeitung zum Beispiel fair und rechtmäßig sein, für einen festgelegten, rechtmäßigen Zweck erfolgen und sich auf die zur Erfüllung dieses Zwecks erforderlichen Daten beschränken. Sie muss sich außerdem auf eine der folgenden Rechtsgrundlagen stützen.

- Die **Einwilligung** der betroffenen Person;
- eine **Verpflichtung aus einem Vertrag** zwischen Ihnen und der Person;
- die Erfüllung einer **rechtlichen Verpflichtung**;
- der Schutz **lebenswichtiger Interessen** der Person;
- die Wahrnehmung einer **Aufgabe, die im öffentlichen Interesse liegt**;
- die **berechtigten Interessen** Ihres Unternehmens, jedoch nur, nachdem sichergestellt wurde, dass die Grundrechte und Grundfreiheiten der betroffenen Person bei der Datenverarbeitung nicht ernsthaft beeinträchtigt werden. Wenn die Rechte der Person Ihre Interessen überwiegen, dürfen Sie die Daten nicht verarbeiten.

Im Fokus: die Einwilligung zur Verwendung personenbezogener Daten einholen

Die Datenschutz-Grundverordnung wendet strenge Regeln für die auf Einwilligung beruhende Datenverarbeitung an. Der Zweck dieser Regeln besteht darin, sicherzustellen, dass Personen verstehen, in was sie einwilligen. Daher sollte die Einwilligung **freiwillig, für den konkreten Fall, in informierter Weise** in klarer und **unmissverständlich** erteilt und in klarer und einfacher Sprache eingeholt werden. Außerdem sollte sie durch eine **bestätigende Handlung** erfolgen, zum Beispiel durch das Anklicken eines Kästchens im Internet oder die Unterzeichnung eines Formulars.

Wenn Sie auf der Grundlage einer Einwilligung personenbezogene Daten verarbeiten, die ein **Kind** betreffen, ist die Einwilligung der Eltern notwendig. Da jedoch die Altersgrenze je nach Land zwischen 13 und 16 Jahren variiert, sollten Sie die nationale Gesetzgebung beachten.

Beachten Sie: Wenn eine Person der Verarbeitung ihrer personenbezogenen Daten zustimmt, können Sie die Daten nur für jene Zwecke verarbeiten, zu denen die Einwilligung erfolgt ist. Sie müssen ihr außerdem die Möglichkeit geben, die Einwilligung zu widerrufen.

Ermittlung Ihrer Rolle und Verantwortung

Nachdem Sie festgestellt haben, dass die Datenschutz-Grundverordnung für Ihr Unternehmen gilt und dass Sie personenbezogene Daten verarbeiten, müssen Sie in einem zweiten Schritt Ihre Rolle ermitteln.

In den Datenschutzvorschriften wird zwischen dem Verantwortlichen und dem Auftragsverarbeiter unterschieden, die jeweils unterschiedliche Pflichten haben. Während der Verantwortliche den Zweck der und die Mittel zur Verarbeitung der personenbezogenen Daten festlegt, verarbeitet der Auftragsverarbeiter die personenbezogenen Daten lediglich im Auftrag des Verantwortlichen. Allerdings bedeutet das nicht, dass der Auftragsverarbeiter sich einfach hinter dem Verantwortlichen verstecken kann.

Die Datenschutz-Grundverordnung verlangt von Verantwortlichen, dass sie nur Auftragsverarbeiter beauftragen, die hinreichende Garantien bieten. Diese Garantien sind in einem schriftlichen Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter festzuhalten. Außerdem muss der Vertrag eine Reihe von zwingenden Bestimmungen enthalten, unter anderem eine Klausel, die vorsieht, dass der Auftragsverarbeiter personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten wird.

Pflichten, die Rechte von Personen schützen

Die Datenschutz-Grundverordnung enthält eine Reihe von Pflichten zum Schutz des Rechts von Personen, die Kontrolle über ihre eigenen personenbezogenen Daten zu übernehmen.

Ihre Pflicht: Bereitstellung transparenter Informationen

Unternehmen müssen Personen darüber informieren, wer was aus welchem Grund verarbeitet. Diese Informationen müssen mindestens folgende Aspekte beinhalten:

- wer Sie sind;
- warum Sie die Daten verarbeiten;
- welche Rechtsgrundlage besteht;
- wer die Daten erhält (sofern zutreffend).

In einigen Fällen müssen auch folgende Angaben gemacht werden:

- die Kontaktdaten des Datenschutzbeauftragten;
- das berechtigte Interesse (wenn ein berechtigtes Interesse die Rechtsgrundlage für die Verarbeitung ist);
- die Grundlage für die Übermittlung der Daten in ein Land außerhalb der EU;
- wie lange die Daten gespeichert werden;
- die Datenschutzrechte der Person (d. h. Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit usw.);
- wie die Einwilligung widerrufen werden kann (wenn eine Einwilligung die Rechtsgrundlage für die Verarbeitung ist);
- ob eine gesetzliche oder vertragliche Verpflichtung zur Bereitstellung der Daten besteht;
- im Falle einer automatisierten Entscheidungsfindung: Informationen über die Logik, Tragweite und Auswirkungen der Entscheidung.

„Unternehmen müssen Personen darüber informieren, wer was aus welchem Grund verarbeitet.“

Ihre Pflicht: Auskunftsrecht und Recht auf Datenübertragbarkeit

Personen haben das Recht auf unentgeltliche Auskunft über ihre personenbezogenen Daten in einem zugänglichen Format. Wenn Sie einen entsprechenden Antrag erhalten, müssen Sie

- der Person mitteilen, ob Sie ihre personenbezogenen Daten verarbeiten;
- sie über die Verarbeitung informieren (etwa über die Zwecke der Verarbeitung, die Kategorien der betreffenden personenbezogenen Daten, die Empfänger ihrer Daten usw.);
- eine Kopie der verarbeiteten personenbezogenen Daten zur Verfügung stellen.

Außerdem können Personen, sofern die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht, verlangen, dass ihre personenbezogenen Daten zurückgegeben oder an ein anderes Unternehmen übermittelt werden. Dies wird Recht auf Datenübertragbarkeit genannt. Die Daten sollten in einem gängigen und maschinenlesbaren Format bereitgestellt werden.

Auch wenn diese beiden Rechte eng miteinander verbunden sind, handelt es sich dennoch um zwei verschiedene Rechte. Aus diesem Grund müssen Sie sicherstellen, dass die beiden Rechte klar differenziert werden, und die Person entsprechend informieren.

Ihre Pflicht: Recht auf Löschung (Recht auf Vergessenwerden)

Unter bestimmten Umständen kann eine Person vom Verantwortlichen die Löschung ihrer personenbezogenen Daten verlangen, zum Beispiel wenn die Daten nicht mehr zur Erfüllung des Verarbeitungszwecks benötigt werden. Ihr Unternehmen ist jedoch nicht verpflichtet, einem solchen Ersuchen nachzukommen, wenn

- die Verarbeitung zur Wahrung des Rechts auf freie Meinungsäußerung und Informationsfreiheit notwendig ist;
- Sie die personenbezogenen Daten aufbewahren müssen, um eine rechtliche Verpflichtung einzuhalten;
- andere Gründe des öffentlichen Interesses vorliegen – zum Beispiel, wenn Sie die personenbezogenen Daten zu Zwecken der öffentlichen Gesundheit oder zu wissenschaftlichen oder historischen Forschungszwecken aufbewahren müssen;
- Sie die personenbezogenen Daten aufbewahren müssen, um einen Rechtsanspruch geltend zu machen.

Ihre Pflicht: Recht auf Berichtigung und auf Widerspruch

Wenn eine Person der Ansicht ist, ihre personenbezogenen Daten seien falsch, unvollständig oder unrichtig, hat sie das Recht, sie unverzüglich berichtigen oder vervollständigen zu lassen.

Personen können der Verarbeitung ihrer personenbezogenen Daten für eine bestimmte Verwendung auch jederzeit widersprechen, wenn Ihr Unternehmen die Daten auf der Grundlage Ihres berechtigten Interesses oder zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe verarbeitet. Sofern Ihr berechtigtes Interesse das Interesse der Person nicht überwiegt, müssen Sie die Verarbeitung der personenbezogenen Daten beenden. Ebenso kann eine Person verlangen, dass die Verarbeitung ihrer personenbezogenen Daten eingeschränkt wird, während ermittelt wird, ob Ihr berechtigtes Interesse das Interesse der Person überwiegt. Im Falle von Direktwerbung sind Sie jedoch stets verpflichtet, die Verarbeitung personenbezogener Daten auf Antrag einer Person zu beenden.

Vorsicht bei automatisierter Entscheidungsfindung und Profiling

Personen haben das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden. Für diese Regel existieren jedoch einige Ausnahmen, zum Beispiel, wenn die Person der automatisierten Entscheidung ausdrücklich zugestimmt hat. Außer wenn die automatisierte Entscheidung auf einem Gesetz beruht, muss Ihr Unternehmen

- die Person über die automatisierte Entscheidungsfindung informieren;
- der Person das Recht geben, die automatisierte Entscheidung von einer Person überprüfen zu lassen;
- der Person die Möglichkeit geben, die automatisierte Entscheidung anzufechten.

Wenn etwa eine Bank die Entscheidung automatisiert, ob sie einer bestimmten Person ein Darlehen gewährt, sollte diese Person über die automatisierte Entscheidung informiert werden und die Möglichkeit erhalten, die Entscheidung anzufechten und ein menschliches Eingreifen zu verlangen.

Risikobasierte Pflichten

Zusätzlich zu den Pflichten, die den Schutz persönlicher Rechte gewährleisten sollen, enthält die Datenschutz-Grundverordnung eine Reihe von Pflichten, deren Anwendung von den jeweiligen Risiken abhängt.

Ihre Pflicht: Ernennung eines Datenschutzbeauftragten

Ein Datenschutzbeauftragter ist dafür zuständig, Ihre Einhaltung der Datenschutz-Grundverordnung zu überwachen. Eine der zentralen Aufgaben des Datenschutzbeauftragten besteht darin, Mitarbeiter, die die eigentliche Verarbeitung personenbezogener Daten durchführen, über ihre Pflichten zu informieren und sie zu beraten. Der Datenschutzbeauftragte arbeitet außerdem mit der Datenschutzbehörde zusammen und fungiert als Kontaktstelle für die Datenschutzbehörde und betroffene Personen.

Ihr Unternehmen ist zur Ernennung eines Datenschutzbeauftragten verpflichtet, wenn

- Sie regelmäßig oder systematisch Personen überwachen oder besondere Kategorien von Daten verarbeiten;
- diese Verarbeitung eine Ihrer Kerntätigkeiten darstellt und
- es sich um eine Verarbeitung in großem Umfang handelt.

Wenn Sie zum Beispiel personenbezogene Daten verarbeiten, um ausgehend von dem Online-Verhalten von Menschen zielgerichtete Werbung über Suchmaschinen zu schalten, sind Sie gemäß Datenschutz-Grundverordnung verpflichtet, einen Datenschutzbeauftragten zu ernennen. Wenn Sie Ihren Kunden jedoch nur einmal im Jahr Werbematerial senden, benötigen Sie keinen Datenschutzbeauftragten. Auch wenn Sie als Arzt Gesundheitsdaten über Ihre Patienten erheben, ist wahrscheinlich kein Datenschutzbeauftragter notwendig. Wenn Sie allerdings für ein Krankenhaus personenbezogene Daten zu Genetik und Gesundheit verarbeiten, ist ein Datenschutzbeauftragter Pflicht.

Ihre Pflicht: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Die Datenschutz-Grundverordnung führt zwei neue Grundsätze ein: Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen.

Der **Datenschutz durch Technikgestaltung** sorgt dafür, dass Unternehmen den Datenschutz schon frühzeitig berücksichtigen, wenn sie neue Methoden der Verarbeitung personenbezogener Daten planen. Gemäß diesem Grundsatz muss ein Verantwortlicher alle erforderlichen technischen und organisatorischen Maßnahmen treffen, um die Datenschutzgrundsätze umzusetzen und die Rechte natürlicher Personen zu schützen. Zu diesen Maßnahmen könnte zum Beispiel der Einsatz von Pseudonymisierung zählen.

Der Datenschutz durch Technikgestaltung minimiert Risiken für die Privatsphäre und stärkt das Vertrauen. Indem der Datenschutz bei der Entwicklung neuer Waren oder Dienstleistungen in den Vordergrund rückt, können potenzielle Datenschutzprobleme frühzeitig vermieden werden. Zudem trägt dieses Verfahren zur Sensibilisierung für das Thema Datenschutz in allen Abteilungen und auf allen Ebenen eines Unternehmens bei.

Der **Datenschutz durch datenschutzfreundliche Voreinstellungen** bedingt, dass Ihr Unternehmen stets die datenschutzfreundlichste Voreinstellung wählt. Sind zum Beispiel zwei Datenschutzeinstellungen möglich, von denen eine den Zugriff auf personenbezogene Daten durch Unbefugte verhindert, so ist letztere als Voreinstellung zu verwenden.

„Der Datenschutz durch Technikgestaltung minimiert Risiken für die Privatsphäre und stärkt das Vertrauen.“

„Der Datenschutz durch datenschutzfreundliche Voreinstellungen bedingt, dass Ihr Unternehmen stets die datenschutzfreundlichste Voreinstellung wählt.“

Ihre Pflicht: ordnungsgemäße Meldung von Datenschutzverletzungen

Eine Datenschutzverletzung liegt vor, wenn personenbezogene Daten, für die Sie verantwortlich sind, unbeabsichtigt oder unrechtmäßig gegenüber unbefugten Empfängern offengelegt werden, vorübergehend nicht verfügbar sind oder geändert werden.

Es ist entscheidend, dass Unternehmen geeignete technische und organisatorische Maßnahmen treffen, um Datenschutzverletzungen zu vermeiden. Stellt jedoch eine eingetretene Datenschutzverletzung ein Risiko für die Rechte und Freiheiten von Personen dar, sollten Sie Ihre Datenschutzbehörde innerhalb von 72 Stunden informieren, nachdem Sie von der Verletzung erfahren.

Abhängig davon, ob eine Datenschutzverletzung ein *hohes* Risiko darstellt, sind Unternehmen unter Umständen überdies verpflichtet, alle von der Datenschutzverletzung betroffenen Personen zu informieren.

Sie übermitteln personenbezogene Daten nach außerhalb der EU?

Die Datenschutz-Grundverordnung gilt für den Europäischen Wirtschaftsraum (EWR), der alle EU-Länder sowie Island, Liechtenstein und Norwegen umfasst. Werden personenbezogene Daten in Länder außerhalb des EWR übermittelt, sollte der von der Datenschutz-Grundverordnung gebotene Schutz mit den Daten reisen. Um Daten ins Ausland zu exportieren, müssen Unternehmen also sicherstellen, dass bestimmte Garantien bestehen.

Die Datenschutz-Grundverordnung bietet ein breit gefächertes Instrumentarium mit Mechanismen, um Daten in Drittländer zu übermitteln. Gemäß Datenschutz-Grundverordnung sind diese Übermittlungen unter den folgenden Voraussetzungen zulässig:

1. Die EU erachtet den durch das jeweilige Land vorgesehenen Schutz als angemessen; oder
2. Ihr Unternehmen trifft beispielsweise die notwendigen Maßnahmen, um geeignete Garantien zu bieten, etwa durch die Aufnahme bestimmter Klauseln in den Vertrag, den Sie mit dem nicht in Europa ansässigen Importeur der personenbezogenen Daten geschlossen haben; oder
3. Ihr Unternehmen stützt sich beispielsweise auf bestimmte Gründe für die Übermittlung (sogenannte „Ausnahmen“) wie die Einwilligung der jeweiligen Person.

Weitere Informationen über die Regeln für internationale Datenübermittlungen finden Sie in der Mitteilung der Europäischen Kommission über den Austausch und Schutz personenbezogener Daten in einer globalisierten Welt: http://eur-lex.europa.eu/legal-content/de/TXT/HTML/?uri=CELEX:52017DC0007

Müssen Sie eine Datenschutz-Folgenabschätzung durchführen?

Die Durchführung einer Datenschutz-Folgenabschätzung ist immer dann verpflichtend, wenn die beabsichtigte Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen würde. Dies kann zum Beispiel zutreffen, wenn neue Technologien zum Einsatz kommen.

Gemäß Datenschutz-Grundverordnung besteht mindestens ein hohes Risiko, wenn

- automatisierte Verarbeitung und Profiling-Mechanismen eingesetzt werden, um Personen systematisch und eingehend zu bewerten;
- ein öffentlich zugänglicher Bereich systematisch und weiträumig überwacht wird (z. B. durch Videoüberwachung);
- in großem Umfang sensible Daten (z. B. Gesundheitsdaten) verarbeitet werden.

Der Zweck der Datenschutz-Folgenabschätzung besteht darin, potenzielle Risiken für die Rechte und Freiheiten natürlicher Personen vor Beginn der Verarbeitung personenbezogener Daten und vor Entstehung des Risikos zu ermitteln. Indem Risiken bereits im Vorfeld eingedämmt werden, können Schäden verhindert und Kosten minimiert werden.

Falls die in der Datenschutz-Folgenabschätzung angegebenen Maßnahmen nicht alle ermittelten hohen Risiken beseitigen, muss vor der beabsichtigten Datenverarbeitung die Datenschutzbehörde konsultiert werden.

„Die Durchführung einer Datenschutz-Folgenabschätzung ist immer dann verpflichtend, wenn die beabsichtigte Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen würde.“

Was Sie tun müssen

Beantwortung von Anträgen

Erhält Ihr Unternehmen einen Antrag einer Person, die ihre Rechte ausüben möchte, sollten Sie unverzüglich, in jedem Fall aber innerhalb eines Monats ab Eingang des Antrags, darauf antworten. Die Frist zur Beantwortung kann allerdings im Fall von komplexen oder mehrfachen Anträgen um zwei Monate verlängert werden, sofern der Antragsteller über diese Fristverlängerung in Kenntnis gesetzt wird. Zudem müssen Anträge **unentgeltlich** bearbeitet werden. Wird ein Antrag abgewiesen, müssen Sie die Person über die Gründe dafür und über ihr Recht unterrichten, Beschwerde bei der Datenschutzbehörde einzulegen.

Weisen Sie nach, dass Sie die Vorschriften einhalten, indem Sie Verzeichnisse führen!

Einer der wesentlichen Grundsätze der Datenschutz-Grundverordnung lautet, dass sichergestellt sein muss, dass Unternehmen ihre Einhaltung der Vorschriften nachweisen können. Das bedeutet, dass Sie belegen können müssen, dass Ihr Unternehmen die Datenschutz-Grundverordnung einhält und alle geltenden Pflichten erfüllt – insbesondere auf Anfrage oder bei Prüfungen durch die Datenschutzbehörde.

Eine Möglichkeit, das zu tun, besteht in der Führung detaillierter Verzeichnisse, die u. a. folgende Punkte enthalten:

- Name und Kontaktdaten Ihres an einer Datenverarbeitung beteiligten Unternehmens;
- Grund bzw. Gründe für die Verarbeitung personenbezogener Daten;
- Beschreibung der Kategorien von Personen, die personenbezogene Daten bereitstellen;
- Kategorien der Organisationen, die personenbezogene Daten erhalten;
- Übermittlung personenbezogener Daten in ein anderes Land oder an eine andere Organisation;
- Speicherfristen für die personenbezogenen Daten;
- Beschreibung der Sicherheitsmaßnahmen, die bei der Verarbeitung personenbezogener Daten genutzt werden.

Zusätzlich sollte Ihr Unternehmen Verfahren und Leitlinien schriftlich festhalten – und regelmäßig aktualisieren –, über die auch Ihre Mitarbeiter informiert werden.

KAPITEL 4

BEREIT FÜR DIE DATENSCHUTZ-GRUNDVERORDNUNG?

Bei der Verarbeitung personenbezogener Daten sind jetzt Sie am Ball. Gemäß der Datenschutz-Grundverordnung müssen Sie in einem ersten Schritt Ihre aktuellen Datenverarbeitungstätigkeiten skizzieren und eine Neubewertung Ihrer internen Geschäftsprozesse vornehmen. Insbesondere müssen Sie

- ermitteln, über welche Daten Sie verfügen und zu welchem Zweck und auf welcher Rechtsgrundlage Sie diese nutzen;
- alle bestehenden, insbesondere zwischen Verantwortlichen und Auftragsverarbeitern geschlossenen Verträge überprüfen;
- alle verfügbaren Möglichkeiten für internationale Übermittlungen prüfen; und
- die übergeordnete Führungsstruktur in Ihrem Unternehmen überprüfen (d. h. prüfen, welche technologischen und organisatorischen Maßnahmen getroffen wurden); dazu gehört auch die Überlegung, ob Sie einen Datenschutzbeauftragten ernennen müssen oder möchten.

Von grundlegender Bedeutung in diesem Prozess ist es, sicherzustellen, dass die oberste Führungsebene Ihres Unternehmens an diesen Prüfungen beteiligt ist, Informationen bereitstellt und regelmäßig auf den neuesten Stand gebracht und zu Änderungen der Datenschutzrichtlinien befragt wird.

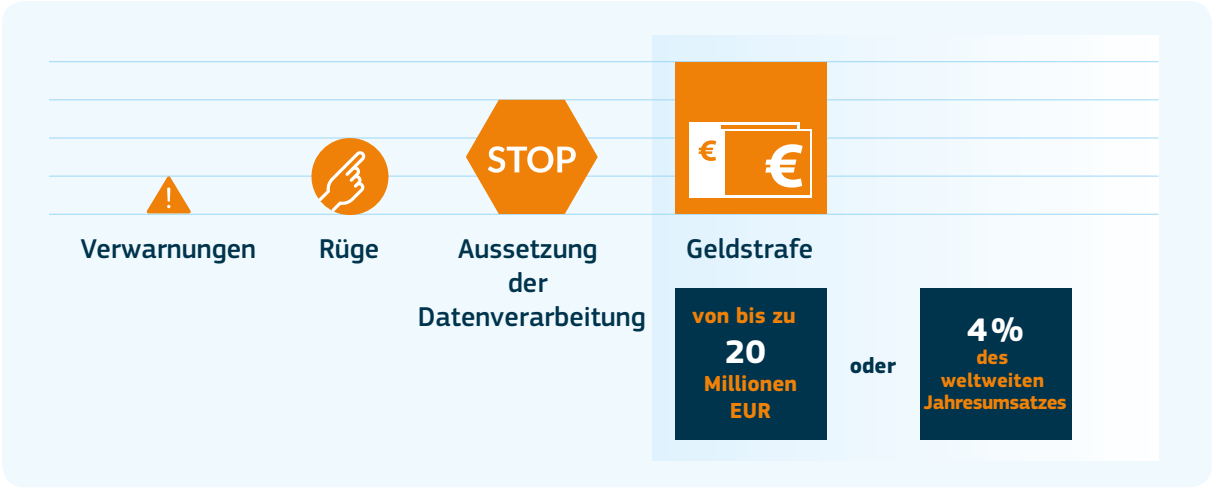
Sie verarbeiten Daten in mehr als einem Land?

Für die grenzüberschreitende Verarbeitung ist unter Umständen nicht Ihre nationale Datenschutzbehörde, sondern eine Aufsichtsbehörde in einem anderen Land zuständig. In der Regel handelt es sich dabei um die Datenschutzbehörde des Landes, in dem Ihr Unternehmen seinen Hauptsitz hat (an dem Entscheidungen über die Mittel und Zwecke der Verarbeitung getroffen werden).

Die Risiken der Nichteinhaltung

Eine Nichteinhaltung der Datenschutz-Grundverordnung kann empfindliche Geldbußen nach sich ziehen – bei bestimmten Verstößen bis zu 20 Millionen Euro oder 4 % des weltweiten Umsatzes Ihres Unternehmens. Die Datenschutzbehörde kann Unternehmen zusätzliche Abhilfemaßnahmen auferlegen, indem sie zum Beispiel die Beendigung der Verarbeitung personenbezogener Daten anordnet. Sie sollten auch berücksichtigen, dass eine Nichteinhaltung Ihren Ruf schädigen könnte.

Offensichtlich sind die Kosten der Nichteinhaltung der Datenschutz-Grundverordnung viel höher als jegliche Investitionen, die zu ihrer Einhaltung getätigt werden.



Fragen? Bedenken? Wenden Sie sich bitte an Ihre nationale Datenschutzbehörde.

Nationale Datenschutzbehörde online suchen

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

WICHTIGER HINWEIS

Die Informationen und Hinweise in dieser Broschüre dienen einem besseren Verständnis der EU-Datenschutzvorschriften.

Sie gelten ausschließlich als Orientierungshilfe. Nur der Wortlaut der Datenschutz-Grundverordnung ist rechtsverbindlich. Demzufolge begründet ausschließlich die Datenschutz-Grundverordnung Rechte und Pflichten für die betroffenen Personen. Diese Orientierungshilfe begründet weder durchsetzbare Rechte noch Ansprüche.

Die verbindliche Auslegung des EU-Rechts fällt in die ausschließliche Zuständigkeit des Gerichtshofs der Europäischen Union. Die in dieser Orientierungshilfe geäußerten Ansichten lassen den Standpunkt, den die Kommission gegebenenfalls vor dem Gerichtshof vertreten wird, unberührt.

Weder die Europäische Kommission noch irgendeine andere Person, die in deren Auftrag handelt, ist für die Nutzung der in der Broschüre enthaltenen Informationen verantwortlich.

Diese Broschüre stellt den aktuellen Stand zum Zeitpunkt ihrer Ausarbeitung dar. Sie sollte als „dynamisches Dokument“ erachtet werden, das laufender Verbesserung unterliegt. Die Inhalte können daher jederzeit ohne Vorankündigung geändert werden.

Informationen über die EU

Im Internet

Auf dem Europa-Portal finden Sie Informationen über die Europäische Union in allen Amtssprachen: https://europa.eu/european-union/index_de

EU-Bookshop

Beim können Sie – zum Teil kostenlos – EU-Veröffentlichungen herunterladen oder bestellen: https://publications.europa.eu/bookshop. Wünschen Sie mehrere Exemplare einer kostenlosen Veröffentlichung, wenden Sie sich an Europe Direct oder das Informationsbüro in Ihrer Nähe (siehe https://europa.eu/european-union/contact_de).

Informationen zum EU-Recht

Informationen zum EU-Recht, darunter alle EU-Rechtsvorschriften seit 1952 in sämtlichen Amtssprachen, finden Sie in EUR-Lex: http://eur-lex.europa.eu

Offene Daten der EU

Über ihr Offenes Datenportal (http://data.europa.eu/euodp/de) stellt die EU Datensätze zur Verfügung. Die Daten können zu gewerblichen und nichtgewerblichen Zwecken kostenfrei heruntergeladen werden.

Die Datenschutz-Grundverordnung regelt die Verarbeitung und Verwaltung personenbezogener Daten durch Unternehmen. Mit dem Inkrafttreten einheitlicher europäischer Vorschriften zum Schutz personenbezogener Daten muss Ihr Unternehmen nun vorrangig ein einziges Datenschutzgesetz einhalten, wenn es in der EU Waren und Dienstleistungen anbietet.

Durch die Vereinfachung des Regelungsumfelds für Unternehmen bietet die Datenschutz-Grundverordnung eine neue Möglichkeit für Ihr Unternehmen, die Verwaltung personenbezogener Daten zu verbessern und in der Folge das Vertrauen der Verbraucher in Ihr Unternehmen zu stärken.

In dieser Broschüre sind die Pflichten herausgestellt, die Ihr Unternehmen gemäß Datenschutz-Grundverordnung hat.

europa.eu/dataprotection/de

Amt für Veröffentlichungen