

AMERICAN EXPRESS

Datenschutz-Grundverordnung (DSGVO) der EU

2018

A vertical decorative border on the left side of the slide, featuring a repeating pattern of the American Express logo, including the words "AMERICAN EXPRESS" and "SERVICE" in a stylized, ornate font.

Die Bedeutung des Datenschutzes bei American Express

American Express verarbeitet jeden Tag eine große Menge an personenbezogenen Daten, die für sein Geschäft von entscheidender Bedeutung sind. Ein Versäumnis bei der ordnungsgemäßen Verarbeitung dieser Daten kann sich nachteilig auf die Marke American Express und unsere Wettbewerbsposition auswirken oder, schlimmer noch, dem Einzelnen schaden.

Als Mitglied des American Express-Teams sind Kollegen und Auftragnehmer persönlich dafür verantwortlich, sich über die Anwendung der American Express-Grundsätze zum Schutz der Daten und der Privatsphäre auf alle von uns verarbeiteten personenbezogenen Daten sowie über die Einhaltung der geltenden Gesetze und Vorschriften zu informieren.

Der Schutz der Privatsphäre unserer Kunden und Kollegen ist mehr als die Sicherung der Daten, die wir über sie erheben. Der Schutz der Privatsphäre bedeutet, Überraschungen zu begrenzen und Einzelpersonen die Wahl zu geben, wie wir ihre personenbezogenen Daten erheben, nutzen und weitergeben.

A vertical decorative border on the left side of the slide, featuring a repeating pattern of the American Express logo and the words "SERVICE", "AMER", "EXPRESS", and "WO".

Über diesen Kurs

Dieser Kurs soll das Bewusstsein für die jüngsten Änderungen der Datenschutzgesetze in der Europäischen Union schärfen, die sich auf die Geschäftstätigkeit von American Express auswirken.

Er deckt Folgendes ab:

- Zweck und Geltungsbereich der Datenschutz-Grundverordnung (bekannt als DSGVO)
- Schlüsseldefinitionen einschließlich personenbezogener Daten und besonderer Datenkategorien
- Die Grundsätze der Verordnung, die für die Erhebung, Nutzung und Speicherung personenbezogener Daten gelten
- Rechte, die Einzelpersonen im Rahmen der DSGVO ausüben können
- Anforderungen für die Meldung von Datenverstößen
- Folgenabschätzungen zum Datenschutz
- Wie Sie mehr Informationen erhalten und wen Sie für Hilfe kontaktieren können

Datenschutz-Grundverordnung

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung) trat am 25. Mai 2018 in allen 28 Mitgliedstaaten der Europäischen Union in Kraft. Kurz darauf trat sie auch in den EWR-Staaten Norwegen, Island und Liechtenstein in Kraft.

Sie hob ein Flickwerk nationaler Datenschutzgesetze auf der Grundlage einer EU-Richtlinie von 1995 auf und ersetzte sie durch ein einziges gemeinsames Regelwerk für die Verarbeitung personenbezogener Daten.

Sie gilt für jede Person oder Organisation, die Daten verarbeitet und:

- in der Europäischen Union ansässig ist (wie z. B. unsere American Express Rechtspersonen der EU); oder
- anderswo niedergelassen ist, aber Waren und Dienstleistungen für Einzelpersonen in der EU anbietet; oder
- anderswo niedergelassen ist, jedoch das Verhalten von Personen in der EU überwacht.

Entscheidend ist, dass sie die Befugnisse der Regulierungsbehörden stärkte und Strafen von bis zu 4 % des weltweiten Jahresumsatzes bei Nichteinhaltung einführte.





Wichtige Begriffe

Personenbezogene Daten

Informationen über eine identifizierte oder identifizierbare lebende Person. Dies sollte breit ausgelegt werden und umfasst alle Informationen, die verbunden werden können, um eine Person zu identifizieren. Dazu gehören eindeutige Identifikatoren wie Name und Kontonummer, aber auch Online-Kennungen wie Geräte-ID und IP-Adresse.

Betroffene Person

Die Person, auf die sich die Daten beziehen. Dies kann ein Kollege, Interessent, Kartenmitglied, Händler, wirtschaftlicher Eigentümer oder jede andere Person sein, über die wir Daten besitzen.

Besondere Kategorien personenbezogener Daten

Personenbezogene Daten, die die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten über das Sexualleben oder die sexuelle Orientierung einer Person offenbaren, unterliegen zusätzlichen Beschränkungen.

A vertical decorative border on the left side of the page featuring a repeating pattern of the American Express logo, including the words "SERVICE", "AMERICAN EXPRESS", and "WORLDWIDE".

Wichtige Begriffe

Datenverantwortlicher

Die Person oder Organisation, die über den Zweck und die Art und Weise der Verarbeitung personenbezogener Daten entscheidet. In fast allen Fällen ist American Express der Verantwortliche für die von uns verarbeiteten Daten.

Auftragsverarbeiter von Daten

Eine Person oder Organisation, die personenbezogene Daten unter Anleitung des für die Verarbeitung Verantwortlichen verarbeitet. Anbieter, die personenbezogene Daten im Auftrag von American Express verarbeiten, sind unsere Auftragsverarbeiter.

Internationale Übermittlung

Übermittlung personenbezogener Daten aus der EU an einen anderen Ort oder Zugriff auf Daten innerhalb der EU von einem anderen Ort aus. Für internationale Übermittlungen innerhalb der American Express Gruppe gelten die von unserer Aufsichtsbehörde genehmigten Binding Corporate Rules (verbindliche interne Datenschutzvorschriften). Andere internationale Übermittlungen unterliegen zusätzlichen gesetzlichen Anforderungen.



Datenschutzgrundsätze der DSGVO

Personenbezogene Daten müssen:

1. **rechtmäßig, fair und transparent** in Bezug auf die betroffene Person verarbeitet werden

Die Datenverarbeitung muss auf einer rechtmäßigen Grundlage erfolgen, wie z. B.:

- Einwilligung der betroffenen Person,
- Ausführung des Vertrages,
- gesetzliche Verpflichtung oder
- die berechtigten Interessen des für die Verarbeitung Verantwortlichen

2. für **bestimmte, ausdrückliche und rechtmäßige Zwecke** erhoben und nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken unvereinbar ist

Bekanntmachungen und andere Angaben müssen die Zwecke, für die die Daten genutzt werden sollen, deutlich machen, und wir müssen sicherstellen, dass die Daten nicht für andere Zwecke verwendet werden.

3. **angemessen, sachdienlich und beschränkt auf das, was** für die Zwecke, für die sie verarbeitet werden, erforderlich ist

Wir sollten nur die Daten erheben, die wir für jeden Zweck benötigen.



Datenschutzgrundsätze der DSGVO

Personenbezogene Daten müssen:

4. genau sein und, wo nötig, auf dem neuesten Stand gehalten werden

Die Daten müssen zum Zeitpunkt der Erhebung oder Erstverarbeitung korrekt sein. Wir müssen sicherstellen, dass insbesondere die Kundendaten aktuell sind, um eine unbefugte Offenlegung zu verhindern.

5. in einer Form aufbewahrt werden, die eine Identifizierung der betroffenen Personen **nicht länger als** für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, erforderlich ist

Wir bewahren personenbezogene Daten so lange auf, wie es für die Beziehung zwischen uns und dem Einzelnen notwendig ist. Wir werden die Daten in Übereinstimmung mit unseren Aufbewahrungsfristen aufbewahren, die unseren gesetzlichen Verpflichtungen entsprechen. Nach Ablauf der Aufbewahrungsfrist werden personenbezogene Daten anonymisiert oder gelöscht.

6. in einer Weise verarbeitet werden, die eine **angemessene Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor versehentlichem Verlust, Vernichtung oder Beschädigung durch geeignete technische oder organisatorische Maßnahmen

Wir verarbeiten Daten in Übereinstimmung mit den American Express Information Security Standards, um deren Vertraulichkeit, Integrität und Zugänglichkeit zu gewährleisten.



Persönliche Rechte

Zugangsrecht

Die Datenschutz-Grundverordnung gibt Einzelpersonen ein Recht auf Zugang zu den personenbezogenen Daten, die American Express über sie besitzt. Wenn sie uns einen Antrag auf Zugang stellen, haben sie das Recht, darüber informiert zu werden, ob wir Daten über sie gespeichert haben. Wenn dies der Fall ist, haben sie auch das Recht, Kopien ihrer personenbezogenen Daten, die über sie bei uns gespeichert sind, zu erhalten, sowie Informationen darüber, wie diese Daten gespeichert und verarbeitet werden.

Recht auf Berichtigung

Personen haben das Recht auf Richtigkeit, Aktualität und Vollständigkeit der bei American Express gespeicherten personenbezogenen Daten. Zum Beispiel sind die wahrscheinlichsten Situationen, in denen Personen die Berichtigung personenbezogener Daten verlangen würden:

- wenn eine Einzelperson die Richtigkeit der personenbezogenen Daten, die für eine nachteilige Kontoentscheidung verwendet werden, wie z. B. eine reduzierte Kreditlinie, in Frage stellt;
- wenn eine Einzelperson personenbezogene Daten herausfordert, die der Kreditauskunftei gemeldet werden;
- wenn eine Einzelperson einen falsch geschriebenen Namen korrigieren oder Informationen wie die Rechnungsadresse aktualisieren möchte.

A vertical decorative border on the left side of the slide, featuring a repeating pattern of the American Express logo and the words "SERVICE", "AMERICAN EXPRESS", and "WORLDWIDE".

Persönliche Rechte

Recht auf Löschung („Recht, vergessen zu werden“):

Einzelpersonen können American Express auffordern, personenbezogene oder kontobezogene Daten zu löschen, und wir werden dies tun, es sei denn, wir sind verpflichtet, diese Daten für vertragliche, rechtliche oder behördliche Zwecke aufzubewahren.

Recht auf Einspruch

Es gibt drei Arten der Verarbeitung, die von Einzelpersonen beanstandet werden können:

- Einzelpersonen haben das Recht, der Verarbeitung auf der Grundlage der berechtigten Interessen von American Express zu widersprechen, z. B. um Rechtsansprüche zu begründen, auszuüben oder zu verteidigen, Betrug zu verhindern und/oder unsere Produkte oder Dienstleistungen zu verbessern.
- Einzelpersonen können auch Einwände gegen die Verarbeitung zum Zwecke der Einladung zu Umfragen und Fokusgruppen erheben.
- Einzelpersonen haben das Recht, dem Direktmarketing zu widersprechen. Sobald Einzelpersonen Widerspruch einlegen, müssen wir die Verarbeitung personenbezogener Daten für das Direktmarketing unabhängig vom Grund sofort einstellen.



Persönliche Rechte

Recht auf Beschränkung

Einzelpersonen können die Richtigkeit der Daten von American Express in Frage stellen. American Express ist verpflichtet, die Verarbeitung der Daten bis zum Abschluss der Untersuchung zu überprüfen und zu beschränken.

Recht auf Datenübertragbarkeit

Die Datenübertragbarkeit ist ein neues Recht, das von der DSGVO eingeführt wurde.

Das Recht auf Datenübertragbarkeit gewährt Einzelpersonen das Recht, ihre eigenen personenbezogenen Daten, die sie American Express zur Verfügung gestellt haben, zu erhalten und wiederzuverwenden. Es erlaubt ihnen auch, personenbezogene Daten einfach und sicher von American Express zu einem anderen Verantwortlichen zu übertragen, ohne die Benutzerfreundlichkeit zu beeinträchtigen.

American Express kann Kartenmitglieder an MYCA verweisen, wo sie Kontoauszüge für einen Zeitraum von bis zu sieben Jahren einsehen können. Kartenmitglieder können ihre Kontoauszüge im PDF-Format herunterladen, speichern und ausdrucken.

A decorative vertical border on the left side of the slide featuring a repeating pattern of the American Express logo, including the words "SERVICE", "AMERICAN EXPRESS", and "AMER".

Benachrichtigung bei Datenverstößen

Datenverantwortliche müssen Verstöße, die ein Risiko für die betroffenen Personen darstellen, der nationalen Datenschutzbehörde melden. Diese Mitteilung muss innerhalb von **72 Stunden** nachdem der Verantwortliche Kenntnis vom Verstoß erlangt, erfolgen.

Im Falle von Verstößen, die ein hohes Risiko für Einzelpersonen darstellen, muss der für die Verarbeitung Verantwortliche auch Informationen über den Verstoß an die betroffenen Personen weitergeben.

Enterprise Incident Response Programm (EIRP)

Melden Sie alle potenziellen oder bestätigten Datensicherheitsvorfälle sofort an EIRP, indem Sie das auf der EIRP-Homepage auf The Square verlinkte Aufnahmeformular verwenden. Sie können sich auch an EIRP wenden, indem Sie innerhalb der USA unter (888) 732-3750 oder international unter (602) 537-3021 anrufen.

Bitte beachten Sie diese Richtlinien:

- Behandeln Sie den Vorfall vertraulich. Teilen Sie keine Details mit anderen, weder intern noch extern.
- Sprechen Sie nicht mit den Medien. Verweisen Sie alle Medienanfragen, die Sie erhalten, unverzüglich an American Express Public Affairs.

A decorative vertical border on the left side of the slide, featuring a repeating pattern of the American Express logo and the words "SERVICE", "AMERICAN EXPRESS", and "WORLDWIDE".

Folgenabschätzung für den Datenschutz

Wenn die Verarbeitung personenbezogener Daten zu einem **hohen Risiko** für die Rechte und Freiheiten von Personen führen kann, muss der Verantwortliche vor der Verarbeitung eine **Folgenabschätzung** der vorgeschlagenen Tätigkeit auf den Schutz personenbezogener Daten vornehmen.

Eine einzige Bewertung kann sich auf eine Reihe ähnlicher Verarbeitungsvorgänge beziehen, die ein ähnlich hohes Risiko darstellen.

Zu den Arten der Verarbeitung, die eine Datenschutzfolgenabschätzung (Data Protection Impact Assessment, DPIA) erfordern, gehören:

- systematische und umfassende Bewertung der persönlichen Aspekte, die auf einer automatisierten Verarbeitung, einschließlich Profiling, basiert;
- Verarbeitung von besonderen Datenkategorien in großem Umfang;
- systematische Überwachung im großen Stil.

American Express hat diese Anforderungen in seine Methodik zur Bewertung des Datenschutzes integriert, und Global Privacy wird Sie darüber informieren, ob zusätzlich zu den Standard-Fragebögen zur Bewertung des Datenschutzes (RAQs) eine DPIA erforderlich ist.



Ergreifen globaler Datenschutzmaßnahmen

Wenn Sie Fragen zum Datenschutz haben oder um Rat fragen möchten, wenden Sie sich bitte an **Global Privacy** über das Global Privacy Portal auf The Square:

[Globales Datenschutzportal](#)

Auf dem Portal können Sie auf Datenschutzstandards und -richtlinien zugreifen, eine Anfrage stellen oder eine Datenschutz-Folgenabschätzung initiieren.

Global Privacy beauftragt GCO und den Geschäftsbereich/Market Compliance je nach Bedarf zu unterstützen.

Wenn Sie eine Beschwerde zum Datenschutz einreichen, Bedenken äußern oder andere Rechte ausüben möchten, können Sie sich an unseren **EU-Datenschutzbeauftragten** wenden: DPO-Europe@aexp.com.