

Die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union (EU), die neue Regeln für den Umgang mit den personenbezogenen Daten von in der EU ansässigen Bürgern sowie für den Schutz dieser Daten aufstellt.

Sie legt neue Pflichten und Haftungen beim Umgang mit personenbezogenen Daten fest und Einzelpersonen erhalten mehr Rechte bei der Erhebung, Verarbeitung und Speicherung ihrer personenbezogenen Daten.

Auswirkungen der DSGVO

Wenn Ihr Unternehmen die Bestimmungen der DSGVO erfüllen muss, sind einige Faktoren zu beachten. Lassen Sie sich unbedingt rechtlich beraten, um über die speziell für Ihr Unternehmen nötigen Anforderungen aufgeklärt zu werden.



1. Ihre Daten verstehen

Um Daten richtig schützen zu können, müssen Sie verstehen, wie sie in Ihrem Unternehmen verarbeitet werden – wie personenbezogene Daten gehandhabt, geteilt, verwendet, archiviert und gelöscht werden. Für die Festlegung Ihrer DSGVO-Unternehmensstrategie ist es besonders wichtig, die Art Ihrer Daten sowie deren Verwendung und Speicherung zu verstehen.

2. Eigentumsrechte und Verantwortlichkeit feststellen

Für die Einhaltung der Datenschutzbestimmungen muss ein verantwortlicher Eigentümer festgelegt werden. Einige Unternehmen sind verpflichtet, einen Datenschutzbeauftragten einzustellen. Die DSGVO hat außerdem ein neues „Verantwortlichkeitsprinzip“ eingeführt, durch das Unternehmen ein Programm zur Einhaltung der Datenschutzbestimmungen befolgen müssen. Unternehmen müssen interne Datenschutzrichtlinien aufstellen und ihre Mitarbeiter schulen.

3. Rechtliche Grundlagen für die Verarbeitung schaffen

Eine weitere Anforderung der DSGVO verpflichtet Unternehmen zur Dokumentation der Rechtsgrundlagen für die unterschiedlichen verarbeiteten personenbezogenen Daten. Wenn Sie zum Beispiel die Einwilligung als Grundlage für die Verarbeitung heranziehen, müssen Sie sich überlegen, wie Sie diese erhalten. Außerdem müssen Sie nachweisen können, wie und wann die Einwilligung erteilt wurde.

4. Die Rechte der Datensubjekte verstehen

Damit Sie angemessene Verfahren einsetzen können, müssen sie zunächst verstehen, welche Rechte Personen in Bezug auf ihre Daten haben. Datensubjekte haben zum Beispiel das Recht, ihre personenbezogenen Daten einzusehen, zu ändern, zu löschen oder sie digital zu exportieren. In manchen Fällen haben Nutzer auch das Recht, automatisierten Entscheidungen und Profiling zu widersprechen.

5. Eingebauten Datenschutz sicherstellen

Eingebauter Datenschutz ist zum ersten Mal vom Gesetz vorgeschrieben. Finden Sie deshalb frühzeitig eine Lösung für die Integration in Ihre Unternehmensprozesse. In manchen Fällen muss eine Datenschutz-Folgenabschätzung durchgeführt werden.

6. Auf Datenschutzverletzungen vorbereitet sein

Für ein stabiles Datenschutzprogramm ist es besonders wichtig, dass Ihre Verhaltensrichtlinien und Prozesse für Datenschutzverletzungen aktuell und erprobt sind. Gemäß DSGVO müssen Datenschutzverletzungen rechtzeitig den zuständigen Behörden gemeldet werden. Denn Strafzahlungen können sowohl für versäumte Berichterstattung als auch Datenschutzverletzungen auferlegt werden.

7. Wichtige Informationen mitteilen

Die Online-Datenschutzrichtlinien und andere Mitteilungen müssen aktuell sein und Datenschutzpraktiken umfassen. Laut den neuen Anforderungen müssen die Rechtsgrundlagen für die Verarbeitung erläutert werden und den Nutzern muss die für Beschwerden zuständige Behörde mitgeteilt werden.

8. Mit Zulieferern zusammenarbeiten

Die DSGVO-Vorschriften betreffen nicht nur die Richtlinien Ihres Unternehmens. Auch Drittanbieter, die für Sie Daten verarbeiten, müssen die geforderten Datenschutzstandards erfüllen. Sie können Ihren Zulieferern folgende Fragen stellen:

- Verfügen Sie über zuverlässige Vorgänge für Netzwerk- und Informationssicherheit sowie Datenschutz und Datensicherheit?
- Erfüllen Sie international anerkannte Standards und überprüfen Sie deren Einhaltung?
- Wie können Sie eine gefestigte Vertrauens- und Sicherheitskultur nachweisen? Wie können Sie uns bei der Datenverwaltung und Erfüllung unserer Pflichten als Verantwortlicher helfen?

Dropbox: Schützt Ihre Daten

Das Fundament unserer Geschäftsbeziehungen lautet Vertrauen. Das Vertrauen, das Millionen von Menschen weltweit sowohl privat als auch geschäftlich in uns setzen.

Wir möchten uns dieses Vertrauens würdig erweisen und betrachten den Schutz Ihrer Daten als eine große Verantwortung. Daher stehen Sicherheit, Compliance und Datenschutz bei der Entwicklung von Dropbox nach wie vor an erster Stelle.

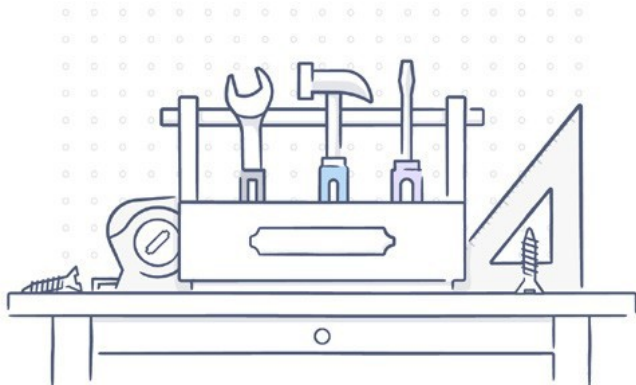
Sicherheit: Schutz und Kontrolle

Schutz: Architektur- Informationssicherheit

Dropbox wurde mit einer sicheren verteilten Infrastruktur entwickelt. Sie umfasst mehrere Sicherheitsebenen wie sichere Datenübertragung, Verschlüsselung, Netzwerkkonfiguration und Steuerelemente auf Anwendungsebene, die über eine skalierbare und sichere Infrastruktur verteilt sind. Unsere zuverlässige Informationssicherheitsverwaltung bewertet Risiken und trägt bei Dropbox zu einer Sicherheitskultur bei. Wir überprüfen und aktualisieren unsere Richtlinien regelmäßig, bieten unseren Mitarbeitern Sicherheitsschulungen, testen Anwendungs- und Netzwerksicherheitstest (einschließlich Penetrationstest), führen Risikobewertungen durch und stellen die Einhaltung der Sicherheitsrichtlinien sicher. Umfassende Informationen finden Sie in unserem White-Paper [Sicherheit in Dropbox Business](#).

Kontrolle: IT-Administratoren unterstützen

Dropbox bietet die [Kontroll- und Analysefunktionen](#), die IT-Administratoren benötigen. Damit verwalten Sie Ihre Compliance-Verpflichtungen einfacher. Mit unserem Admin-Dashboard können Sie die Team-Aktivität beobachten, verbundene Geräte anzeigen und Freigabeaktivitäten überprüfen. Sie können Gruppen erstellen, um Teammitgliedern einen einfachen Zugriff auf bestimmte Ordner zu ermöglichen. Außerdem können Sie mit dem Teamordner-Manager Team-Ordner, einschließlich Synchro-Management, anzeigen und kontrollieren. Mit der Linkberechtigungsfunktion können Sie freigegebene Links mit einem Kennwort schützen, Gültigkeitsdauern für einen temporären Zugriff festlegen und den Zugriff auf Ihre Mitarbeiter beschränken. Mit unserem Kontoübertragungstool können Sie Dateien bei veränderten Verantwortlichkeiten einfach von einem Nutzer zum anderen übertragen. Durch Remote-Löschen können Sie Dateien von verlorenen oder gestohlenen Geräten löschen.



Compliance: Vertrauen ist gut, Kontrolle ist besser

Compliance ist eine effektive Möglichkeit, um die Vertrauenswürdigkeit eines Dienstes zu beurteilen. Wir empfehlen Ihnen, ja, erwarten sogar von Ihnen, dass Sie sich von [der Konformität](#) unserer Sicherheitsmaßnahmen mit den allgemein anerkannten [Standards und Vorschriften](#) wie ISO 27001, 27017, 27018 und SOC 1, 2, und 3 überzeugen. Auditoren unabhängiger Unternehmen prüfen unsere Kontrollsysteme und erstellen Berichte und Gutachten, die wir Ihnen wann immer möglich bereitstellen. Weitere Informationen über die von uns eingehaltenen Standards und über die Überprüfung unserer Sicherheitsmaßnahmen finden Sie auf unserer [Compliance-Webseite](#).

Datenschutz: Unsere Verantwortung

Es sind Ihre Daten und egal, ob es sich um geschäftliche oder persönliche Informationen handelt, wir wollen Ihr Vertrauen nicht enttäuschen und stellen jederzeit den Schutz Ihrer Daten sicher. In unserer [Datenschutzrichtlinie](#) wird der Umgang und der Schutz Ihrer Informationen umfassend beschrieben. Wir veröffentlichen einen [Transparenzbericht](#) und unsere [Grundsätze](#) bei behördlichen Auskunftsanfragen. Damit wollen wir zeigen, wie oft wir Anfragen erhalten, bewerten und beantworten. Außerdem setzen wir uns für strengere Datenschutzgesetze ein.

Zusammen arbeiten wir an der Sicherheit Ihrer Daten

Dropbox arbeitet mit seinen Unternehmenskunden zusammen, um ihre Daten zu schützen. Wir schützen unsere Infrastruktur, unser Netzwerk und unsere Anwendungen umfassend; schulen unsere Mitarbeiter hinsichtlich Sicherheits- und Datenschutzmaßnahmen; fördern eine Kultur, bei der Vertrauenswürdigkeit das Wichtigste ist und unterziehen unsere Systeme und Maßnahmen strengsten Tests und Audits durch unabhängige Prüfer. Auch Kunden sind maßgeblich am Schutz und der Sicherheit ihrer Teams und Daten beteiligt. Mit Dropbox können Sie Ihr Konto so konfigurieren, verwenden und überwachen, dass Ihr Unternehmen die Sicherheits-, Datenschutz- und Compliance-Vorgaben erfüllt. In unserem [Leitfaden zur gemeinsamen Verantwortung](#) erfahren Sie, wie wir Ihr Konto schützen und wie Sie den Überblick und die Kontrolle über Ihre Team-Daten behalten.

Der Inhalt dieses Leitfadens soll den Informationszugriff erleichtern und stellt keine Rechtsberatung dar. Die Leser sollten bei Bedarf eine individuelle Rechtsberatung einholen.

