

# Informationssicherheit und Datenschutz

## Einleitung

Personenbezogene Daten spielen in der Gesellschaft und der Wirtschaft eine große Rolle. Immer mehr Menschen möchten mehr Kontrolle und Klarheit darüber, wie ihre personenbezogenen Daten von Unternehmen, mit denen sie zusammenarbeiten, verwendet und geschützt werden.

Vertrauen ist das Fundament, auf dem Dropbox Geschäftsbeziehungen zu Millionen von Menschen und Unternehmen weltweit aufbaut. Wir schätzen dieses Vertrauen und nehmen den Schutz Ihrer personenbezogenen Daten sehr ernst.

## Unsere Verpflichtungen Ihnen gegenüber

Wir fühlen uns dem Schutz Ihrer personenbezogenen Daten verpflichtet. Die [Allgemeinen Geschäftsbedingungen](#) von Dropbox beschreiben Ihre Verantwortlichkeiten bei der Nutzung unserer Dienste. Unsere [Datenschutzrichtlinie](#) beschreibt unsere Datenschutzmaßnahmen gegenüber den Nutzern und erklärt, wie wir Ihre personenbezogenen Daten erfassen, verwenden und verarbeiten, wenn Sie unsere Dienste nutzen. Wenn Sie in Nordamerika (Vereinigte Staaten von Amerika, Kanada und Mexiko) wohnen, fungiert Dropbox Inc. als Ihr Diensteanbieter. Für alle anderen Nutzer ist es Dropbox International Unlimited

Company ist der Verantwortliche für Ihre personenbezogenen Daten.

Wenn Sie Dropbox für Unternehmen oder Dropbox Education nutzen, fungiert Ihr Unternehmen als Datenverantwortlicher für alle personenbezogenen Daten, die Dropbox in Verbindung mit Ihrer Nutzung von Dropbox für Unternehmen oder Dropbox Education zur Verfügung gestellt werden. Der Datenverantwortliche bestimmt die Zwecke und Mittel der Verarbeitung personenbezogener Daten.

Dropbox fungiert als Datenverarbeiter und verarbeitet Daten im Namen Ihrer Organisation, wenn Sie Dropbox für Unternehmen oder Dropbox Education verwenden. Unsere [Vereinbarung für Dropbox für Unternehmen](#) umfasst die Verpflichtungen in Zusammenhang mit der Datenverarbeitung und der internationalen Datenübertragung.

## Unsere Erfolge im Bereich Compliance

Anhand der Compliance lässt sich die Vertrauenswürdigkeit eines Dienstes effektiv überprüfen. Wir ermutigen zur Überprüfung, ob unsere Sicherheits- und Datenschutzmaßnahmen mit den bekanntesten Normen und Vorschriften (wie ISO 27001, ISO 27017, ISO 27018, ISO 27701, HIPAA/HITECH sowie SOC 1, 2 und 3) konform sind und freuen uns über entsprechende Nachfragen.

Außerdem sind wir einer der ersten Cloud-Diensteanbieter, die eine Zertifizierung nach ISO 27018, der international anerkannten Norm für führende Praxis bei Datenschutz und Privatsphäre in der Cloud, erhalten haben. Unsere unabhängigen, externen Prüfer testen unsere Kontrolle und stellen ihre Berichte und Urteile zur Verfügung. Diese teilen wir gern mit Ihnen, wenn möglich. Beachten Sie bitte, dass sich unsere Zertifizierungen

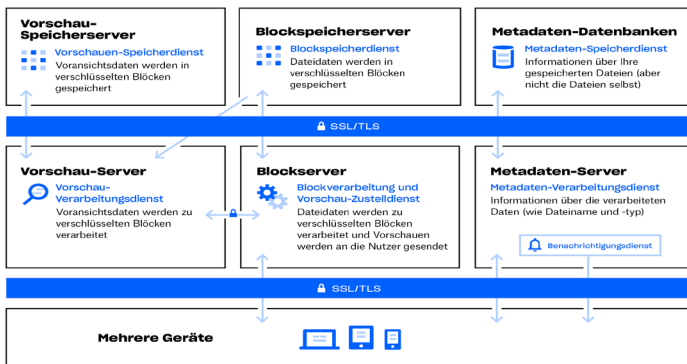
und Berichte zwar meistens auf Dropbox für Unternehmen und Dropbox Education beziehen, dass die Mehrheit unserer Kontrollen jedoch auch für Nutzer von Dropbox Basic, Plus und Professional gilt. Zudem hält sich Dropbox nun auch an die Bestimmungen des EU Cloud Code of Conduct. Weitere Informationen zu den Standards, die wir einhalten, und zur Verifizierung unserer Verfahren finden Sie auf unserer [Compliance-Webseite](#).

# Dropbox-Architektur: Schutz Ihrer personenbezogenen Daten

Bei Dropbox sind wir überzeugt, dass der Schutz Ihrer personenbezogenen Daten mit der Sicherheit Ihrer Daten beginnt. Darum wurde Dropbox mit verschiedenen Schutzebenen erstellt, einschließlich sicherem Datentransfer, Verschlüsselung sowie Steuerelementen auf Anwendungsebene, die über eine skalierbare, sichere Infrastruktur verteilt werden.

## Unsere Infrastruktur: Dateien

Die Dateinfrastruktur von Dropbox besteht aus den im Diagramm unten abgebildeten Bestandteilen.



## Blockspeicherserver

Die Inhalte der Nutzerdateien werden in verschlüsselten Blöcken auf den Blockspeicherservern gespeichert. Vor der Übertragung unterteilt der Dropbox-Client die Dateien in Dateiblocke, um sie auf die Speicherung vorzubereiten. Die Blockspeicherserver nutzen das Content-Addressable Storage(CAS)-Speicherverfahren. Dabei wird jeder verschlüsselte Dateiblock anhand seines Hash-Wertes abgerufen.

## Vorschau-Server

Die Vorschau-Server sind für das Erstellen von Dateivorschauen verantwortlich. Vorschauen sind Abbildungen einer Nutzerdatei in einem für die schnelle Anzeige auf dem Endnutzergesetz besser geeigneten Dateiformat. Vorschau-Server rufen Dateiblocke aus dem Blockspeicherserver ab, um Vorschauen zu erstellen. Wird eine Dateivorschau angefordert, rufen die Vorschau-Server die zwischengespeicherte Vorschau aus den Vorschau-Speicherservern ab und übermitteln sie an die Blockserver. Vorschauen werden Nutzern letztlich von Blockservern bereitgestellt.

## Vorschau-Speicherserver

Zwischengespeicherte Vorschauen werden verschlüsselt auf den Vorschau-Speicherservern gespeichert.

## Benachrichtigungsdienst

Für die Überprüfung auf Änderungen an Dropbox-Konten wird ein separater Dienst eingesetzt. Hier werden keine Dateien oder Metadaten gespeichert bzw. übertragen. Jeder Client stellt eine Long-Poll-Verbindung zum Benachrichtigungsdienst her und befindet sich danach in Warteposition. Wenn Änderungen an Dateien in Dropbox vorgenommen werden, teilt der Benachrichtigungsdienst diese Änderung dem/den relevanten Client(s) mit, indem die Long-Poll-Verbindung aufgehoben wird. Durch das Aufheben dieser Verbindung wird dem Client signalisiert, dass er eine sichere Verbindung zu Metadatenservern herstellen muss, um alle Änderungen synchronisieren zu können.

## Metadaten-Server

Grundinformationen über Nutzerdaten, sogenannte Metadaten, werden in einem speziell dafür vorgesehenen Speicherdienst aufbewahrt und dienen als Index für die Daten in den Nutzerkonten. Metadaten umfassen grundlegende Konto- und Nutzerinformationen wie die E-Mail-Adressen und Namen der einzelnen Nutzer sowie die Namen ihrer Geräte. Dazu gehören auch Grundinformationen über Dateien wie Dateiname und -format, durch die Features wie Versionsverlauf, Wiederherstellung und Synchronisierung unterstützt werden.

## Datenbanken für Metadaten

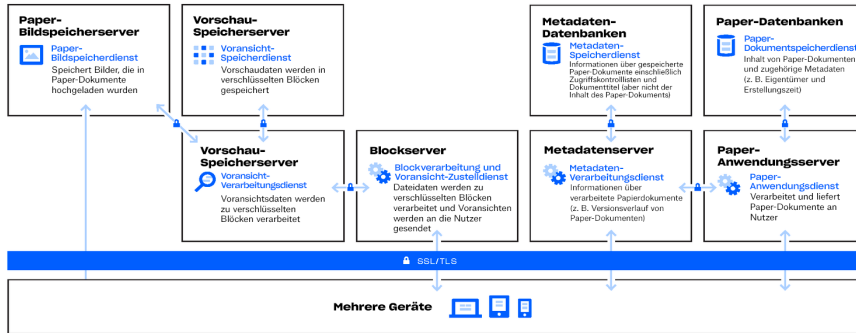
Dateimetadaten werden in einem MySQL-basierten Datenbankdienst gespeichert und nach Bedarf fragmentiert und repliziert, um Leistungs- und Hochverfügbarkeitsanforderungen zu erfüllen.

## Blockserver

Dropbox bietet einen einzigartigen Sicherheitsmechanismus, der über die herkömmliche Verschlüsselung zum Schutz von Nutzerdaten hinausgeht. Blockserver verarbeiten Dateien aus den Dropbox-Apps, indem sie jede Datei in einzelne Blöcke aufteilen, jeden Dateiblock mithilfe einer starken Chiffre verschlüsseln und nur Blöcke synchronisieren, die zwischen einzelnen Dateiversionen verändert wurden. Wenn eine Dropbox-App eine neue Datei oder Änderungen an einer vorhandenen Datei erkennt, informiert die Anwendung die Blockserver über die Änderung. Dann werden die neuen oder veränderten Dateiblocke verarbeitet und an die Speicherserver übertragen.

## Unsere Infrastruktur: Paper

Dropbox Paper (Paper) ist ein Feature des Dropbox-Produkts. Paper nutzt jedoch eine überwiegend eindeutige Auswahl an Systemen innerhalb der Dropbox-Infrastruktur. Die Infrastruktur von Paper besteht aus den im Diagramm unten abgebildeten Bestandteilen.



### Paper-Anwendungsserver

Die Anwendungsserver von Paper verarbeiten Nutzeranfragen, geben den Output bearbeiteter Paper-Dokumente an den Nutzer zurück und versenden Benachrichtigungen. Paper-Anwendungsserver schreiben von Nutzern eingehende Bearbeitungen in die Paper-Datenbanken, wo sie dauerhaft gespeichert werden. Die Kommunikation der Paper-Anwendungsserver mit den Paper-Datenbanken wird stark verschlüsselt.

### Paper-Datenbanken

Die Inhalte von Paper-Dokumenten sowie gewisse Metadaten darüber werden verschlüsselt und in den Paper-Datenbanken dauerhaft gespeichert. Zu den gespeicherten Daten gehören Informationen über das jeweilige Paper-Dokument (zum Beispiel der Titel, Freigaben und Berechtigungen, Projekt- und Dateizuordnungen usw.) und Inhalte des Paper-Dokuments selbst, wie zum Beispiel Kommentare und Aufgaben. Die Paper-Datenbanken werden nach Bedarf fragmentiert und repliziert, um Leistungs- und Hochverfügbarkeitsanforderungen zu erfüllen.

### Paper-Bildspeicherserver

In Paper-Dokumente eingefügte Abbildungen werden auf den Paper-Bildservern gespeichert und im Ruhezustand verschlüsselt. Bilddaten, die von der Paper-Anwendung an die Paper-Bildserver übermittelt werden und umgekehrt, werden in einer verschlüsselten Sitzung übertragen.

### Vorschau-Server

Die Vorschau-Server erstellen sowohl von Bildern, die in Paper-Dokumente eingefügt werden, als auch von Hyperlinks in Paper-Dokumenten Vorschauen. Wenn Bilder in Paper-Dokumente eingefügt werden, rufen die Vorschau-Server die auf den Paper-Bildspeicherservern gespeicherten Bilddaten über eine verschlüsselte Verbindung ab. Wenn Hyperlinks in Paper-Dokumente eingebettet werden, rufen die Vorschau-Server die Bilddaten ab und erstellen mit der vom Quelllink vorgegebenen Verschlüsselung eine Bildvorschau. Vorschauen werden Nutzern letztlich von Blockservern bereitgestellt.

### Vorschau-Speicherserver

Paper verwendet für die Speicherung der zwischengespeicherten Bildvorschau dieselben im Dropbox-Infrastrukturdiagramm beschriebenen Vorschau-Speicherserver. Zwischengespeicherte Vorschaublöcke werden verschlüsselt auf den Vorschau-Speicherservern gespeichert.

# Dropbox-Kontrollen: Unsere internen Verfahren

Wir ergreifen umfassende Maßnahmen zum Schutz unserer Infrastruktur, unseres Netzwerks und unserer Anwendungen. Zu den Sicherheitsmaßnahmen, die wir getroffen haben, gehören die Verschlüsselung im Ruhezustand, die Verschlüsselung bei der Übertragung und die dauerhafte Löschung von Dateien. Außerdem bieten wir allen unseren Mitarbeitern robuste Datenschutz- und Sicherheitsschulungen an, um eine Kultur zu schaffen, in der Vertrauenswürdigkeit Priorität hat. Hier erfahren Sie mehr über einige unserer Kontrollen:

## Schulung

Zum Schutz der personenbezogenen Daten unserer Nutzer gehört auch, ein Datenschutz- und Sicherheitsbewusstsein in unserer Kultur zu entwickeln. Dropbox-Mitarbeiter müssen der Einhaltung von Sicherheitsrichtlinien zustimmen, einschließlich unserer Datenschutzrichtlinie, bevor sie Systemzugriff erhalten. Nur Mitarbeiter mit einem spezifischen Bedarf erhalten Zugang zu Systemen. Die Mitarbeiter nehmen außerdem jedes Jahr an obligatorischen Sicherheits- und Datenschutzbildungen teil.

## Verschlüsselung bei der Übertragung

Für Dateidaten, die zwischen einem Dropbox-Client (derzeit Desktop, Mobilgerät, API oder online) und den Front-End-Servern von Dropbox übertragen werden, wird eine verschlüsselte Verbindung ausgehandelt, um ihre sichere Zustellung zu gewährleisten. Genauso wird eine verschlüsselte Verbindung genutzt, um Paper-Dokumente bei der Übertragung zwischen einem Paper-Client (Mobilgerät, API oder online) und dem gehosteten Dienst zu schützen. Dropbox verwendet für die Datenübertragung Secure Sockets Layer (SSL)/Transport Layer Security (TLS) und richtet einen sicheren Tunnel ein, der durch eine Advanced Encryption Standard-Verschlüsselung (AES) mit mindestens 128 Bit geschützt ist.

## Verschlüsselung im Ruhezustand

Dateien, die der Nutzer hochlädt, werden als diskrete Dateiblöcke auf den Speicherservern von Dropbox gespeichert. Jeder Block wird nach Advanced Encryption Standard (AES) mit 256 Bit verschlüsselt.

Nur Dateiblöcke, die seit der letzten Dateiversion geändert wurden, werden synchronisiert. Genauso werden Paper-Dokumentdaten, die in Paper-Datenbanken gespeichert werden, im Ruhezustand nach AES mit 256 Bit verschlüsselt.

## Endgültiges Löschen von Dateien und Paper-Dokumenten

Wenn ein Dropbox-Nutzer oder ein Administrator eines Teams von Dropbox für Unternehmen oder Dropbox Education eine Datei für die endgültige Löschung markiert, wird ein entsprechender Prozess ausgelöst, um die Datei dauerhaft zu entfernen. Wenn ein Nutzer oder Administrator eines Teams von Dropbox für Unternehmen oder Dropbox Education ein Paper-Dokument für die endgültige Löschung markiert, wird ein ähnlicher Prozess ausgelöst, um die Paper-Dokument- und Bilddaten dauerhaft zu entfernen.

## Private Anfrage nach Datenzugriff

Nutzer können sich auf der Website anmelden und ihre [Kontoseiten](#) aufrufen, um Zugriff auf personenbezogene Daten zu erhalten, die über die in Dropbox gespeicherten Dateien und Paper-Dokumente hinausgehen. Die Kontoseite zeigt unter anderem den Namen und die E-Mail-Adresse, die mit dem Konto verknüpft sind. Nutzer können sich hier auch die IP-Adressen von Sitzungen ansehen und auf den Seiten für [Sicherheit](#) und [verknüpfte Apps](#) nachprüfen, welche Computer, Mobilgeräte und Apps mit ihren Konten verknüpft sind.

Außerdem können Dropbox-Nutzer Zugriff auf andere von uns gesammelte personenbezogene Daten oder deren Löschung beantragen. Weitere Informationen hierzu finden Sie im [Dropbox-Hilfocenter](#).

## Datenschutz-Governance bei Dropbox

Das Datenschutzteam ist für das Dropbox-Datenschutzprogramm verantwortlich. Es setzt unsere wichtigsten Datenschutzinitiativen um und setzt sich für den Datenschutz ein, indem es den Grundsatz des Datenschutzes durch Technikgestaltung in unseren Datenlebenszyklus integriert. Das Dropbox-Datenschutzprogramm wird darüber hinaus von mehreren funktionsübergreifenden untergeordneten Rechtsteams unterstützt. Diese stellen das zusätzliche Fachwissen bereit, das für den Betrieb und die Überwachung der täglichen Aufgaben im Rahmen des Datenschutzprogramms erforderlich ist.

Das Team der Datenschutzbeauftragten arbeitet getrennt von den anderen Datenschutzfunktionen und dient der Einhaltung und Überwachung des Datenschutzes. Es unterstützt zudem den Datenschutzbeauftragten direkt bei der Ausführung seiner Aufgaben. Der Datenschutzbeauftragte (DSB) kann kontaktiert werden unter [privacy@dropbox.com](mailto:privacy@dropbox.com).



## Richtlinien zu behördlichen Anfragen

Wir verstehen, dass Nutzer, die uns ihre personenbezogenen Daten anvertrauen, einen vertraulichen Umgang mit diesen Daten erwarten. Wie die meisten Onlinedienste erhält auch Dropbox zuweilen Anfragen von Regierungen, in denen um Informationen zu ihren Nutzern gebeten wird.

Diese Grundsätze beschreiben, wie wir mit Auskunftersuchen durch Regierungsstellen umgehen.

### Transparenz

Wir sind der Ansicht, dass es Onlinediensten gestattet sein sollte, die Anzahl und die Art der erhaltenen behördlichen Anfragen zu veröffentlichen und Personen darüber zu informieren, wenn Angaben zu ihnen angefragt wurden. Diese Art der Transparenz stärkt die Position von Nutzern, indem sie dabei unterstützt werden, Fälle und Muster von

Eingriffen durch Regierungen besser zu verstehen. Wir werden weiterhin detaillierte Informationen zu diesen Anfragen veröffentlichen und uns für das Recht auf die Weitergabe weiterer derart wichtiger Informationen einsetzen.

### Widerstand gegen zu breit gefasste Anfragen

Auskunftersuchen durch Regierungen sollten begrenzt sein bzgl. der nachgefragten Information und sich auf spezifische Personen und rechtmäßige Untersuchungen beschränken. Dropbox wird sich gegen pauschale und zu breit gefasste Anfragen wehren.

### Bereitstellung vertrauenswürdiger Dienste

Regierungen sollten niemals Hintertüren in Onlinedienste implementieren oder in die Infrastruktur eindringen, um Nutzerdaten zu erlangen. Wir arbeiten auch weiterhin daran, unsere Systeme zu schützen und die Gesetzgebung zu ändern, um klar darauf hinzuweisen, dass solche Aktivitäten illegal sind.

### Schutz für alle Nutzer

Gesetze, durch die Menschen unterschiedlichen Schutz genießen, abhängig davon, wo sie leben oder welche Staatsbürgerschaft sie haben, sind veraltet und spiegeln nicht den globalen Charakter von Onlinediensten wider. Wir werden uns weiterhin für eine Änderung dieser Gesetze einsetzen.

Diese Grundsätze und unser alljährlicher Transparenzbericht sind unter der folgenden Adresse auf der Dropbox-Website öffentlich zugänglich: <https://www.dropbox.com/transparency>.

Weitere Informationen zu unseren Kontrollen und darüber, wie wir Ihre personenbezogenen Daten schützen, entnehmen Sie bitte unserem [Whitepaper zur Sicherheit in Dropbox für Unternehmen](#).

## Andere, die für und mit Dropbox arbeiten

Dropbox verwaltet den Großteil der Aktivitäten, die zur Bereitstellung unserer Dienste erforderlich sind, selbst. Wir arbeiten in diesem Zusammenhang jedoch auch mit vertrauten Dritten zusammen (zum Beispiel für Kundendienst und IT). Diese Dritten greifen nur unter Einhaltung unserer [Datenschutzrichtlinie](#) auf Ihre Informationen zu, um ihre Aufgaben in unserem Auftrag zu erfüllen, und wir bleiben verantwortlich dafür, wie sie Ihre Informationen gemäß unseren Anweisungen behandeln.

Jede Drittpartei durchläuft ein strenges Überprüfungsverfahren, einschließlich Sicherheits- und Datenschutzprüfungen sowie regelmäßiger vertraglicher Überprüfungen, um ihre Fähigkeit zur Erfüllung unserer Datenschutzverpflichtungen sicherzustellen. Basierend auf diesem Überprüfungsprozess bestätigt Dropbox, dass sich seine vertrauenswürdigen externen Partner dazu verpflichtet haben, die geltenden EU-Datenschutzgesetze in Verbindung mit der Verarbeitung personenbezogener Daten im Namen von Dropbox einzuhalten. Kunden können die vertrauenswürdigen Dritten von Dropbox anzeigen, indem sie die ISO 27001- und

27018-Zertifizierungen von Dropbox und unter Anwendung entsprechender Vertraulichkeitsverpflichtungen den SOC 2 Typ II-Bericht von Dropbox einsehen. Insbesondere können Kunden die vertrauenswürdigen Dritten von Dropbox anzeigen, indem sie die Kontrollen und Auditergebnisse von Dropbox hinsichtlich der Trust Services-Kriterien P6.1, P6.4 und CC.9.2 des SOC 2 Typ II-Berichts prüfen.

## Internationale Datenübertragungen

Wenn Sie Daten aus der Europäischen Union, dem Europäischen Wirtschaftsraum oder der Schweiz übertragen, nutzt Dropbox verschiedene rechtliche Mechanismen, wie zum Beispiel Verträge mit unseren Kunden und Partnerunternehmen, Standardvertragsklauseln sowie ggf. die Angemessenheitsentscheidungen der Europäischen Kommission hinsichtlich bestimmter Länder.

Dropbox erfüllt die vom US-Handelsministerium festgelegten EU-US und Swiss-US Privacy Shield-Abkommen

zum Schutz der Privatsphäre hinsichtlich der Erfassung, Verwendung und Aufbewahrung von personenbezogenen Daten, die aus der Europäischen Union, dem Europäischen Wirtschaftsraum, dem Vereinigten Königreich und der Schweiz in die Vereinigten Staaten übermittelt werden; allerdings stützt sich Dropbox nicht auf das EU-US Privacy Shield- oder das Swiss-US Privacy Shield-Abkommen als rechtliche Grundlage für die Übermittlung personenbezogener Daten. Die Privacy Shield-Zertifizierung von

Dropbox finden Sie unter [www.privacyshield.gov/list](http://www.privacyshield.gov/list). Mehr über Privacy Shield erfahren Sie unter [www.privacyshield.gov](http://www.privacyshield.gov).

Beschwerden und Streitigkeiten in Zusammenhang mit unserer Privacy Shield-Compliance werden von JAMS, einer unabhängigen Drittpartei, untersucht und gelöst. Um mehr zu erfahren, lesen Sie bitte unsere [Datenschutzrichtlinie](#).

## DSGVO: die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-Verordnung, die neue rechtliche Rahmenbedingungen zum Schutz der personenbezogenen Daten von in der EU ansässigen Personen schafft. Die DSGVO ist die wichtigste europäische Rechtsvorschrift seit der EU-Datenschutzrichtlinie von 1995, und wie viele in Europa tätige Unternehmen hat auch Dropbox stark in die DSGVO-

Compliance investiert. Die DSGVO soll das Datenschutzrecht in Europa vereinheitlichen und mit den schnellen technologischen Veränderungen der vergangenen zwei Jahrzehnte in Einklang bringen. Sie baut auf vergangenen rechtlichen Rahmenbedingungen der EU auf, einschließlich der EU-Datenschutzrichtlinie, führt eine Reihe neuer Bestimmungen und Verantwortlichkeiten für

Organisationen ein, die personenbezogene Daten ihrer Kunden handhaben, und schafft mehr Rechte für den Nutzer in Bezug auf seine personenbezogenen Daten. Organisationen, die in der EU ansässig sind, sowie Organisationen, die personenbezogene Daten von in der EU ansässigen Personen verarbeiten, sind verpflichtet, die DSGVO einzuhalten.

## Dropbox auf dem Weg zur DSGVO-Compliance

Dropbox verspricht, die DSGVO zu befolgen. Unser Unternehmen legte von Anfang an sehr viel Wert auf Datenschutz und Sicherheit. Auch in unserem Wachstum hat der Umgang mit den Daten, die unsere Kunden uns anvertrauen, sowie deren Schutz weiterhin Priorität. Dropbox ist schon in der Vergangenheit ein Vorreiter in Sachen Compliance gewesen. Wie bereits erwähnt, gehörten wir zu den ersten Anbietern von Cloud-Diensten, die für ihre Kunden die Zertifizierung nach ISO 27018 erwarben. Vor diesem Hintergrund sieht Dropbox die DSGVO-Compliance als Weiterentwicklung unserer vorhandenen Verfahren und Kontrollen, die eine kontinuierliche, sich weiter entwickelnde Reihe von Initiativen zur Gewährleistung des ununterbrochenen Schutzes der personenbezogenen Daten unserer Nutzer darstellen. Für Dropbox begann der Weg zur DSGVO-Compliance bereits mit dem Beschluss der Verordnung im Jahr 2016.

Zuerst stellten wir ein bereichsübergreifendes Team von Spezialisten auf dem Gebiet des Datenschutzes zusammen, bestehend aus Rechtsberatern, Sicherheits- und Compliance-Experten sowie Produkt- und Infrastrukturtechnikern. Dieses Team evaluierte unsere bestehenden Sicherheits- und Datenschutzverfahren im Hinblick auf die Anforderungen der DSGVO.

Im nächsten Schritt prüften wir, wie personenbezogene Daten verarbeitet wurden, und verfolgten den Lebenszyklus personenbezogener Daten in unseren Systemen. Diese Verfahren kennt man zum Teil als Datenmapping und Datenschutz-Folgenabschätzung.

Seitdem bauen wir unsere vorhandenen internen Vorgänge und Verfahren weiter aus, um dem Grundsatz der Rechenschaftspflicht gemäß DSGVO

nachzukommen. Dies umfasst auch die Aufbewahrung von Datensätzen zur Verarbeitung in Übereinstimmung mit Artikel 30 der DSGVO. Das ist besonders wichtig, da laut DSGVO verstärkt Wert darauf gelegt wird, dass Entscheidungen und Verfahrensweisen in Zusammenhang mit personenbezogenen Daten dokumentiert werden.

# Nutzer auf dem Weg zur DSGVO unterstützen

Dropbox enthält Funktionen für Kontrolle und Transparenz, mit denen Sie Ihre Datenschutzpflichten, einschließlich der Voraussetzungen für die DSGVO-Compliance, leichter erfüllen können. Natürlich steht und fällt die DSGVO-Compliance in Ihrer Organisation nicht allein mit der Beziehung zu Ihren Auftragnehmern, zum Beispiel Dropbox. Unsere Funktionen können Ihnen zwar helfen, Ihre Verpflichtungen zu verwalten, aber sie können für sich genommen nicht die Compliance gewährleisten. Die DSGVO-Compliance erfordert eine umfassendere Betrachtung von Datenflüssen und den Maßnahmen zum Datenschutz in Ihrer Organisation. Jede Organisation sollte für sich Schritte unternehmen, um die Compliance zu gewährleisten. Ihre Auftragnehmer können auf diesem Weg wichtige Partner sein.

## Datenminimierung

Die DSGVO-Voraussetzung des Datenschutzes durch Technikgestaltung verlangt unter anderem, dass Organisationen bei der Gestaltung ihrer Dienste auf Datenminimierung achten. Das bedeutet, dass Transparenz und gute Kontrolle der Daten innerhalb Ihrer Organisation nötig sind, um sie verwalten zu können. Das Dropbox-Admin-Dashboard ist ein nützliches Tool, das Ihnen hilft, Team-Aktivitäten zu überwachen, verknüpfte Geräte einzusehen und Freigabeaktivitäten zu protokollieren. Wir arbeiten daran, die Grundsätze des Datenschutzes durch Technikgestaltung in neue Produkte und Features zu integrieren.

## Datenschutz und -wiederherstellung

Schutz abhandengekommener Geräte, Versionsverlauf und Dateiwiederherstellung können helfen, dem unbeabsichtigten Verlust oder der Vernichtung personenbezogener Daten vorzubeugen und im Notfall den Zugriff auf personenbezogene Daten zügig wiederherzustellen. Eine weitere wichtige Maßnahme, die wir zum Schutz Ihrer Daten unterstützen, ist die zweistufige Überprüfung.

## Protokollierung

Die DSGVO verpflichtet Organisationen außerdem verstärkt, ihre Verarbeitungsaktivitäten ausführlich zu protokollieren. Unsere Audit- und Aktivitätsprotokolle helfen Ihnen, Ihre Verarbeitungsvorgänge besser zu verstehen, um die eigene Protokollierung zu erleichtern.

## Zugriffsverwaltung

Im Admin-Dashboard von Dropbox für Unternehmen können Sie den Zugriff von Teammitgliedern auf Dateien, Ordner und Paper-Dokumente bequem verwalten. Mit unseren Berechtigungsoptionen für freigegebene Links können Sie diese durch Passwörter schützen, durch Festlegen einer Gültigkeitsdauer den Zugriff zeitlich begrenzen oder nur Mitarbeitern Ihrer Organisation erlauben, darauf zuzugreifen. Sollten sich die Verantwortlichkeiten einmal ändern, können Sie unser Tool für die Kontenübertragung verwenden, um Dateien und das Eigentumsrecht an Paper-Dokumenten von einem Nutzer auf einen anderen zu übertragen.

Administratoren können den Zugriff von Nutzern auf ihr Konto sperren, dabei jedoch deren Daten und Freigabebeziehungen sichern, um Unternehmensinformationen zu schützen. Mit der Funktion Remote-Löschen können Sie schließlich alle Dateien und Paper-Dokumente von Geräten entfernen, die abhandengekommen sind oder gestohlen wurden.

## EU-Infrastruktur

Die DSGVO verlangt in den meisten Fällen nicht, dass personenbezogene Daten nur in der Europäischen Union gespeichert werden. Dennoch bietet Dropbox qualifizierten Kunden von Dropbox für Unternehmen und Dropbox Education an, Daten (Blöcke) in der EU zu speichern. Die Datenspeicherung in der EU beruht auf der Infrastruktur von Amazon Web Services (AWS). Wenn Sie mehr über unsere EU-Infrastruktur erfahren möchten, [wenden Sie sich bitte an unser Vertriebsteam](#).

# Zusammenarbeiten, um Ihre personenbezogenen Daten zu schützen

Dropbox arbeitet mit seinen Nutzern eng zusammen, um ihre personenbezogenen Daten zu schützen. Wir ergreifen umfassende Maßnahmen, um unsere Infrastruktur, unser Netzwerk und unsere Anwendungen zu schützen. Wir schulen Mitarbeiter in Sicherheits- und Datenschutzfragen und bauen eine Sicherheitskultur auf, in der Vertrauen höchste Priorität hat.

Darüber hinaus lassen wir gründliche Tests und Überprüfungen von unabhängigen Dritten an unseren Systemen vornehmen.

Aber auch die Nutzer spielen eine Schlüsselrolle beim Schutz ihrer persönlichen Daten.

Dropbox ermöglicht es Ihnen, Ihr Konto so zu konfigurieren, zu verwenden und zu überwachen, dass es den Anforderungen Ihrer Organisation entspricht, was

Datenschutz, Sicherheit und Compliance angeht. Unser [Leitfaden zur gemeinsamen Verantwortung](#) kann Ihnen dabei helfen, mehr darüber zu erfahren, was wir tun, um Ihr Konto sicher zu halten, und was Sie tun können, um die Sichtbarkeit und Kontrolle in Bezug auf Ihre persönlichen Daten zu erhalten.

## Zusammenfassung

Täglich setzen Millionen von Nutzern ihr Vertrauen in Dropbox. Das bedeutet uns sehr viel, und deshalb haben Sicherheit und Datenschutz bei der Weiterentwicklung von Dropbox nach wie vor oberste Priorität. Bei jeder Entscheidung, die wir treffen, steht der Schutz der personenbezogenen Daten unserer Nutzer an erster Stelle. Wenn Sie gern mehr darüber erfahren möchten, schreiben Sie bitte eine E-Mail an [privacy@dropbox.com](mailto:privacy@dropbox.com). Weitere Informationen zur DSGVO finden Sie in unserem [DSGVO-Guidance-Center](#).