Dropbox

Datenschutz und Datensicherheit

Einleitung

Personenbezogene Daten spielen in unserer Gesellschaft und in der Wirtschaft eine große Rolle. Immer mehr Menschen wünschen sich mehr Kontrolle und Klarheit hinsichtlich ihrer personenbezogenen Daten und wie diese von Organisationen genutzt und geschützt werden.

Das Fundament unserer Geschäftsbeziehungen hier bei Dropbox lautet Vertrauen. Das Vertrauen, das Millionen von Menschen weltweit sowohl privat als auch geschäftlich in uns setzen. Wir schätzen dieses Vertrauen und betrachten den Schutz Ihrer personenbezogenen Daten als große Verantwortung.

Unser Versprechen an Sie

Wir verpflichten uns zum Schutz Ihrer personenbezogenen Daten. In den Nutzungsbedingungen von Dropbox finden Sie Angaben zu Ihren Pflichten bei der Nutzung unserer Dienste. In unserer Datenschutzrichtlinie erfahren Sie, wie wir uns für den Schutz der Daten unserer Nutzer einsetzen und Ihre personenbezogenen Daten erfassen, speichern und verwenden, wenn Sie unsere Dienste nutzen. Sollten Sie in Nordamerika (USA, Kanada und Mexiko) ansässig sein, ist Dropbox, Inc. Ihr Serviceprovider.

Bei allen anderen Nutzern agiert Dropbox International Unlimited Company als Verantwortlicher oder Verarbeiter Ihrer personenbezogenen Daten.

Sollten Sie Dropbox Business- oder Dropbox Education-Kunde sein, ist Ihre Organisation der Datenverantwortliche für alle durch die Nutzung von Dropbox Business oder Dropbox Education an Dropbox weitergegebenen Daten. Der Datenverantwortliche bestimmt Zweck und Art der Verarbeitung personenbezogener Daten. Dropbox ist der Auftragsverarbeiter im Namen Ihrer Organisation, wenn Sie Dropbox Business oder Dropbox Education nutzen. In unserer Dropbox Business-Vereinbarung finden sich Angaben zur Datenverarbeitung und zu internationalen Datenübertragungen.

Unsere Erfolgsbilanz: Compliance

Compliance ist eine effektive Möglichkeit, um die Vertrauenswürdigkeit eines Dienstes zu beurteilen. Wir ermutigen zur Überprüfung, ob unsere Sicherheits- und Datenschutzmaßnahmen mit den bekanntesten Normen und Vorschriften (wie ISO 27001, ISO 27017, ISO 27018, HIPPA/HITECH, der deutschen Norm BSI C5 sowie SOC 1, 2 und 3) konform sind und freuen uns über entsprechende Nachfragen.

Außerdem sind wir einer der ersten Clouddienstanbieter, die eine Zertifizierung nach ISO 27018, der international anerkannten Norm für führende Praxis bei Datenschutz und Privatsphäre in der Cloud, erhalten haben. Unsere Maßnahmen werden von unabhängigen Dritten geprüft und in Berichten und Meinungen zusammengefasst. Wann immer möglich, geben wir diese gerne für Sie frei.

Obwohl der Großteil unserer Zertifizierungen und Prüfberichte sich normalerweise auf Dropbox Business und Dropbox Education bezieht, werden die meisten Maßnahmen auch auf Dropbox Basic, Plus und Professional angewandt. Weitere Informationen zu den von uns eingehaltenen Normen sowie dazu, wie wir unsere Maßnahmen prüfen, finden Sie auf unserer Compliance-Webseite.

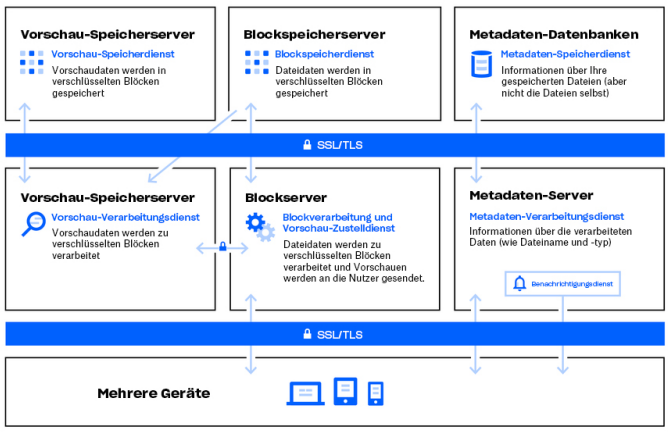
Dropbox

Gut geschützt dank Dropbox-Architektur: Ihre personenbezogenen Daten

Wir sind der Überzeugung, dass der Schutz Ihrer personenbezogenen Daten mit der Geheimhaltung Ihrer allgemeinen Daten beginnt. Aus diesem Grund verfügt Dropbox über verschiedene Schutzebenen, einschließlich sicherem Datentransfer, Verschlüsselung und Steuerelementen auf Anwendungsebene, die über eine skalierbare, sichere Infrastruktur verteilt werden.

Unsere Infrastruktur: Dateien

Die Dropbox-Dateiinfrastruktur setzt sich aus den unten in der Darstellung abgebildeten Komponenten zusammen.



Metadatenserver

Bestimmte, grundlegende Informationen zu Nutzerdaten (die sogenannten Metadaten) werden in einem separaten Speicher hinterlegt und sind eine Art Index für die Daten aus verschiedenen Nutzerkonten. Zu Metadaten zählen grundlegende Konto- und Nutzerinformationen wie E-Mail-Adresse, Name und Gerätenamen. Außerdem umfassen die Metadaten auch grundlegende Informationen zu Dateien – darunter Dateinamen und -typen, die dabei helfen, Funktionen wie den Versionsverlauf, die Datenwiederherstellung und die Synchronisation zu unterstützen.

Metadaten-Datenbanken

Dateimetadaten werden in einem MySQL-basierten Datenbankdienst gespeichert und bei Bedarf gesplittet und kopiert, um Anforderungen an Leistungsfähigkeit und Hochverfügbarkeit zu erfüllen.

Blockserver

Dropbox verfügt über einen einzigartigen Schutzmechanismus, der über herkömmliche Verschlüsselung für den Schutz von Nutzerdaten hinausgeht. Blockserver verarbeiten Dateien der Dropbox-Anwendungen, indem sie jede Datei in Blöcke unterteilen, diese jeweils mit einem starken Schlüssel verschlüsseln und nur die Blöcke synchronisieren, die von der einen zur nächsten Dateiversion geändert wurden. Wenn eine Dropbox-Anwendung eine neue Datei oder Änderungen an einer bereits bestehenden Datei erkennt, informiert die Anwendung die Blockserver über diese Änderunge. Die neuen oder geänderten Dateiblöcke werden verarbeitet und an den Speicherserver übertragen.

Blockspeicherserver

Die eigentlichen Inhalte von Nutzerdateien werden mithilfe von Blockspeicherservern in Blöcken verschlüsselt. Vor der Übertragung teilt der Dropbox-Client Dateien in Dateiblöcke auf, um sie auf die Speicherung vorzubereiten. Die Blockspeicherserver agieren dabei als CAS-System (Content-Addressable Storage), wobei jeder verschlüsselte Dateiblock jeweils nach seinem Hash-Wert abgerufen wird.

Vorschauserver

Vorschauserver stellen Vorschauen von Dateien bereit. Bei einer Vorschau handelt es sich um eine Ausgabe einer Nutzerdatei in einem anderen Dateiformat, das sich für die Darstellung auf dem Endgerät eines Nutzers besser eignet. Vorschauserver rufen Dateiblöcke von den Speicherservern ab, um Vorschauen zu generieren. Wird eine Vorschau angefordert, rufen die Vorschauserver die zwischengespeicherte Vorschau aus dem Vorschauserver ab und übermitteln sie an die Blockserver. Schließlich wird die Vorschau dem Nutzer über die Blockserver bereitgestellt.

Vorschau-Speicherserver

Zwischengespeicherte Vorschauen werden in verschlüsselter Form auf Vorschau-Speicherservern hinterlegt.

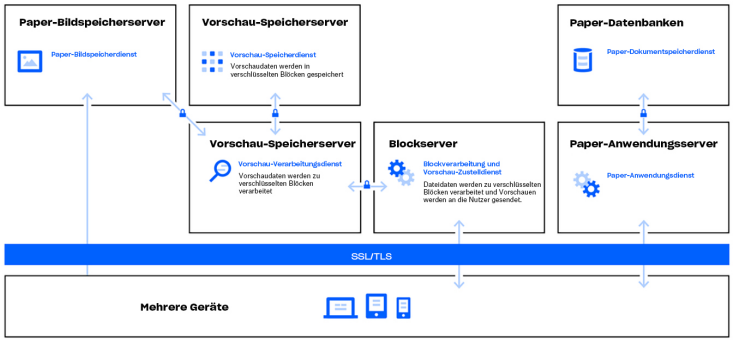
Benachrichtigungsdienst

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 über Long Polling eine Verbindung zum Benachrichtigungsdienst her und befindet sich danach in Warteposition. Wenn Änderungen an Dateien in Dropbox vorgenommen werden, signalisiert der Benachrichtigungsdienst diese Änderung an die relevanten Clients, indem die Long-Poll-Verbindung aufgehoben wird. Durch das Aufheben dieser Verbindung wird ein Signal an den Client abgegeben, der eine sichere Verbindung zu den Metadatenservern herstellen muss, um alle Änderungen synchronisieren zu können.

Dropbox

Unsere Infrastruktur: Paper

Dropbox Paper (Paper) ist eine Funktion der Dropbox-Suite, nutzt jedoch größtenteils unabhängige Systeme der Dropbox-Infrastrukturumgebung. Die Infrastruktur von Paper setzt sich aus den unten dargestellten Komponenten zusammen.



Paper-Anwendungsserver

Die Paper-Anwendungsserver verarbeiten Nutzeranforderungen, zeigen Nutzern ihre Änderungen in den von ihnen bearbeiteten Paper-Dokumenten an und führen Benachrichtigungsdienste aus. Paper-Anwendungsserver schreiben von Nutzern vorgenommene Änderungen in die Paper-Datenbanken, wo sie in einem persistenten Speicher gespeichert werden. Kommunikationssitzungen zwischen den Paper-Anwendungsservern und Paper-Datenbanken werden mit einem starken Schlüssel verschlüsselt.

Paper-Datenbanken

Die tatsächlichen Inhalte der Paper-Dokumente von Nutzern werden zusammen mit bestimmten Metadaten zu diesen Paper-Dokumenten verschlüsselt und persistent in den Paper-Datenbanken gespeichert. Dazu gehören Informationen zu einem Paper-Dokument (z. B. Titel, Freigabe- und Berechtigungsdaten, Projekt- und Ordnerverknüpfungen usw.) aber auch zum Inhalt selbst, wie Kommentare und Aufgaben. Die Paper-Datenbanken werden nach Bedarf fragmentiert und repliziert, um Leistungs- und Hochverfügbarkeitsanforderungen zu erfüllen.

Paper-Bildspeicherserver

Bilder, die in Paper-Dokumente hochgeladen werden, werden gespeichert und auf den Paper-Bildservern verschlüsselt aufbewahrt. Die Übertragung von Bilddaten zwischen der Paper-Anwendung und den Paper-Bildservern geschieht im Rahmen einer verschlüsselten Sitzung.

Vorschauserver

Die Vorschauserver stellen Bildvorschauen sowohl für Bilder, die in Paper-Dokumente hochgeladen werden, als auch für in Paper-Dokumente eingebettete Hyperlinks bereit. Für in Paper-Dokumente hochgeladene Bilder rufen die Vorschauserver über einen verschlüsselten Kanal auf den Paper-Bildspeicherservern hinterlegte Daten ab. Für in Paper-Dokumente eingebettete Hyperlinks rufen die Vorschauserver die Bilddaten wie im Quelllink definiert ab und geben die Vorschau aus. Schließlich wird die Vorschau dem Nutzer über die Blockserver bereitgestellt.

Vorschau-Speicherserver

Paper arbeitet für die Zwischenspeicherung von Bildvorschauen mit den gleichen Vorschau-Speicherservern, die auch im Dropbox-Infrastrukturdiagramm erläutert wurden. Zwischengespeicherte Vorschaublöcke werden in verschlüsselter Form auf Vorschau-Speicherservern hinterlegt.

Dropbox

Dropbox-Steuerungen: interne Praxis

Wir ergreifen umfassende Maßnahmen, um unsere Infrastruktur, unser Netzwerk und unsere Anwendungen zu schützen. Einige der von uns genutzten Sicherheitsmaßnahmen sind Verschlüsselung von Daten im Ruhezustand, Verschlüsselung während der Übermittlung und die dauerhafte Löschung von Dateien.
Außerdem bieten wir umfangreiche Datenschutz- und Sicherheitsschulungen für all unsere Mitarbeiter an, um eine Firmenkultur zu schaffen, in der Vertrauenswürdigkeit oberste Priorität genießt. Weitere Angaben zu unseren Steuerungen finden Sie unten:

Schulung

Zum Schutz der personenbezogenen Daten unserer Nutzer gehören unter anderem auch der Aufbau und die Förderung eines Sicherheits- und Datenschutzbewusstseins. Mitarbeiter von Dropbox sind verpflichtet, Sicherheitsvorschriften (darunter auch einer Datenschutzrichtlinie für Nutzer) zuzustimmen, bevor sie Zugriff auf unsere Systeme erhalten. Nur Mitarbeiter mit entsprechenden Zuständigkeitsbereichen erhalten bei Bedarf Zugang zu diesen Systemen.
Unsere Mitarbeiter nehmen zudem jährlich an verpflichtenden Sicherheits- und Datenschutzschulungen teil.

Verschlüsselung von übermittelten Daten

Damit Dateidaten auch bei der Übermittlung von einem Dropbox-Client (aktuell Desktop, Mobilgerät, API oder Web) an die Front-End-Server von Dropbox geschützt sind, wird eine verschlüsselte Verbindung aufgebaut, um eine sichere Bereitstellung zu gewährleisten. Gleichzeitig wird auch eine verschlüsselte Verbindung hergestellt, um Daten aus Paper-Dokumenten bei der Übertragung von einem Paper-Client (aktuell Mobilgerät, API oder Web) an den gehosteten Dienst zu schützen. Diese Verbindungen werden mit Secure Sockets Layer (SSL)/Transport Layer Security (TLS) verschlüsselt, um einen sicheren Tunnel einzurichten, der durch eine Advanced Encryption Standard-Verschlüsselung (AES) mit mindestens 128 Bit geschützt ist.

Verschlüsselung von gespeicherten Daten

Von Nutzern hochgeladene Dateien werden in Form mehrerer unterschiedlicher Dateiblöcke auf den Dropbox-Speicherservern hinterlegt. Jeder Block wird nach AES (Advanced Encryption Standard) mit 256 Bit verschlüsselt. Nur Dateiblöcke, die zwischen den Prüfungen geändert wurden, werden synchronisiert. Ähnlich werden auch Daten aus Paper-Dokumenten in Paper-Datenbanken in Ruhe mit 256 Bit Advanced Encryption Standard (AES) verschlüsselt.

Dauerhafte Löschung von Dateien und Paper-Dokumenten

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

Zugriffsanforderungen auf personenbezogene Daten

Möchten Nutzer über die in Dropbox gespeicherten Dateien und Paper-Dokumente hinaus auf weitere personenbezogene Daten zugreifen, können sie sich auf der Webseite anmelden und zu ihren Kontoseiten navigieren. Auf der Kontoseite finden sich Daten wie Name und E-Mail-Adresse, die mit dem Konto verknüpft sind. Nutzer können außerdem die IP-Adressen der Verbindungssitzungen, Computer und Mobilgeräte sowie die mit ihrem Konto verbundenen Apps prüfen. Angaben hierzu finden Sie auf den Seiten über Sicherheit und verbundene Apps.

Dropbox-Nutzer haben auch die Möglichkeit, Zugriff auf personenbezogene Daten oder die Löschung von personenbezogenen Daten zu fordern, die Dropbox unter Umständen zu ihnen erfasst hat.
Weitere Informationen hierzu finden Sie im Dropbox-Hilfecenter.

Datenschutz-Governance bei Dropbox

Unser Privacy Program-Team ist für das Dropbox-Datenschutzprogramm verantwortlich, es setzt unsere wichtigsten Datenschutzinitiativen um und fördert Datenschutz durch Integration in unseren Datenlebenszyklus. Das Dropbox-Datenschutzprogramm wird zudem von verschiedenen, bereichsübergreifenden Teams für Rechtsfragen unterstützt. Diese Teams verfügen über die zusätzlichen Erfahrungen, die für Durchführung und Überwachung der Tagesaufgaben im Rahmen des Datenschutzprogramms notwendig sind.

Das DPO-Team arbeitet separat von den anderen Datenschutzabteilungen, dient als Anlaufstelle für Compliance und Überwachung und unterstützt den Datenschutzbeauftragten unmittelbar bei der Ausübung seiner Pflichten. Der Datenschutzbeauftragte (Data Protection Officer, DPO) ist unser lokaler Vertreter in der EU und unter der E-Mail-Adresse privacy@dropbox.com erreichbar.

Dropbox

Richtlinien zu behördlichen Auskunftsanfragen

Uns ist bewusst, dass Nutzer von uns erwarten, dass wir die uns anvertrauten Daten sicher aufbewahren. Wie die meisten Onlinedienste erhalten wir manchmal Auskunftsanfragen von Ämtern und Behörden zu bestimmten Nutzern.

Die unten aufgeführten Prinzipien beschreiben, wie wir mit solchen Auskunftsanfragen von Regierungen umgehen.

Auskunft nur bei transparenten Anfragen

Onlinedienste sollten die Anzahl und Arten behördlicher Anfragen, die sie erhalten, veröffentlichen und Nutzer benachrichtigen dürfen, wenn Auskünfte über sie eingeholt werden.

Transparenz dieser Art hilft Nutzern, Vorfälle und Muster behördlicher Übergriffe besser zu verstehen und darauf zu reagieren. Wir werden weiterhin detaillierte Informationen über diese Anforderungen veröffentlichen und uns für das Recht auf die umfassendere Bereitstellung dieser Informationen einsetzen.

Abwehr zu allgemeiner Anfragen

Behördliche Auskunftsanfragen sollten sich auf die Informationen beschränken, die tatsächlich nötig sind, und klar auf konkrete Nutzer und rechtmäßige Untersuchungen zielen. Pauschale und zu weit gefasste Anfragen lehnen wir ab.

Bereitstellung vertrauenswürdiger Dienste

Regierungen sollten niemals einen heimlichen Zugang zu Onlinediensten installieren 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 Handlungen illegal sind.

Schutz aller Nutzer

Gesetze, die Menschen unterschiedlichen Schutz auf der Grundlage ihres Wohnorts oder ihrer Staatsbürgerschaft gewähren, sind veraltet und werden dem weltumspannenden Wesen von Onlinediensten nicht gerecht. Wir kämpfen auch weiterhin für die Überarbeitung dieser Regelungen.

Diese Prinzipien sowie unseren jährlich veröffentlichten Transparenzbericht finden Sie öffentlich zugänglich auf der Dropbox-Webseite: https://www.dropbox.com/transparency.

Weitere Angaben zu unseren Steuerungen und unserem Ansatz für den Schutz Ihrer personenbezogenen Daten finden Sie in unserem Whitepaper Sicherheit in Dropbox Business.

Externe Unternehmen, die für Dropbox arbeiten oder mit uns zusammenarbeiten

Dropbox verwaltet die Mehrheit der Aktivitäten, die für die Bereitstellung seiner Dienste notwendig sind, selbst. Manchmal beauftragen wir jedoch vertrauenswürdige Dritte in Bezug auf unsere Dienste (beispielsweise Anbieter von Kundensupport und IT-Diensten). Diese Dritten erhalten lediglich Zugang zu Informationen, um in unserem Namen Aufgaben zu übernehmen. Dabei arbeiten sie mit unserer Datenschutzrichtlinie konform und wir sind nach wie vor verantwortlich für die Verarbeitung Ihrer Daten gemäß unseren Anweisungen.

Alle Drittanbieter werden einer strengen Prüfung unterzogen, zu der unter anderem Sicherheitsprüfungen und regelmäßige Vertragsprüfungen zählen, um zu gewährleisten, dass sie unsere Datenschutzversprechen einhalten können.

Internationale Datentransfers

Dropbox stützt sich beim internationalen Transfer personenbezogener Daten von der EU in die USA auf eine Vielzahl rechtlicher Mechanismen. Wir sind sowohl nach EU-U.S. als auch Swiss-U.S. Privacy Shield zertifiziert.

Diese Zertifizierungen gelten für Erfassung, Nutzung und Speicherung personenbezogener Daten sowie deren Übermittlung von der EU oder Schweiz in die USA. Neben diesen Datenschutzschildbestimmungen erfüllt Dropbox ebenfalls strenge vertragliche Ansprüche rund um den Schutz seiner Dienste und deckt internationale Datenübermittlungen durch EU-Modellvertragsklauseln ab.

Dropbox

DSGVO: die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung, kurz DSGVO, ist eine EU-Verordnung, die ein rechtliches Rahmenwerk für den Schutz personenbezogener Daten für EU-Bürger etabliert.

Die DSGVO ist die wichtigste EU-Datenschutzregelung seit der Datenschutzverordnung von 1995 und viele in Europa tätige Unternehmen – darunter auch Dropbox – haben umfangreiche Mittel in ihre DSGVO-Konformität investiert.

Die DSGVO dient der Harmonisierung der Datenschutzgesetze in Europa und bringt sie auf Höhe der rapiden technologischen Entwicklungen der letzten beiden Jahrzehnte.

Sie baut auf älteren rechtlichen Rahmenbedingungen auf, darunter auch die EU-Datenschutzrichtlinie, und führt neue Pflichten und Haftungsgründe für Organisationen, die personenbezogene Daten verarbeiten, ein. Außerdem erhalten Privatpersonen neue Rechte hinsichtlich ihrer personenbezogenen Daten. Organisationen, die ihren Sitz in der EU haben, aber auch Organisationen, die mit Daten von EU-Bürgern arbeiten, müssen die Vorgaben der DSGVO einhalten.

Die DSGVO-Vorbereitung von Dropbox

Dropbox hat sich der DSGVO-Konformität verschrieben. Unser Unternehmen baut seit seiner Gründung auf einem Fundament aus Datenschutz und Sicherheit auf und auch mit unserem Wachstum haben wir unsere Verantwortung für den Schutz und die Verarbeitung der uns von unseren Nutzern anvertrauten Daten nicht aus dem Blick verloren. Dropbox ist aktuellen Compliance-Anforderungen seit Jahren voraus – wie oben beschrieben waren wir einer der ersten Clouddienstanbieter, die nach der Norm ISO 27018 für Business-Nutzer zertifiziert wurden. Dank dieses stabilen Fundaments sieht Dropbox die Konformität mit der DSGVO einfach als Weiterentwicklung bestehender Maßnahmen und Steuerungen an. Sie repräsentiert laufende, sich weiterentwickelnde Initiativen, die gewährleisten sollen, dass die Daten unserer Nutzer immer sicher sind.

Dropbox hat schon bereits kurz nach der Verabschiedung der DSGVO im Jahr 2016 mit den Vorbereitungen begonnen. Als Erstes haben wir ein funktionsübergreifendes Team aus Datenschutzfachleuten gebildet, das aus Rechtsberatern, Schutz- und Compliance-Experten sowie Produkt- und Infrastrukturingenieuren besteht. Im Anschluss hat unser Team eine umfangreiche Beurteilung unser aktuellen Sicherheits- und Datenschutzmaßnahmen unter Berücksichtigung der DSGVO-Vorgaben durchgeführt.

Im nächsten Schritt fanden eine Überprüfung der Verarbeitungsaktivitäten für personenbezogene Daten und die Verfolgung des Lebenszyklus dieser Daten in unseren Systemen statt. Diese Maßnahmen werden manchmal auch als Datenzuordnungen und Datenschutz-Folgenabschätzungen bezeichnet.

Seither bauen wir weiter auf bestehenden internen Prozessen und Vorgängen auf, um die Einhaltung der Rechenschaftspflichten laut DSGVO zu erfüllen. Das ist extrem wichtig, da die DSGVO ein besonderes Augenmerk auf die personenbezogene Daten betreffenden Dokumentations-entscheidungen und -praktiken legt.

Dropbox

Stärkung unserer Nutzer durch die DSGVO

Dropbox bietet Funktionen für Kontrolle und Transparenz, mit deren Hilfe Sie Ihrer Datenschutzverpflichtung und damit auch den Vorgaben der DSGVO leichter nachkommen können. Die DSGVO-Compliance in Ihrer Organisation beschränkt sich natürlich nicht darauf, die Geschäftsbeziehung zu Ihren Auftragnehmern (wie Dropbox) anzupassen. Unsere Funktionen können Sie zwar dabei unterstützen, Ihre Pflichten wahrzunehmen, sie alleine garantieren jedoch noch keine Compliance. Für eine DSGVO-Compliance muss breiter angelegt darüber nachgedacht werden, wie Daten sich in Ihrer Organisation bewegen und geschützt werden. Jede Organisation sollte eigene Maßnahmen ergreifen, um ihre Compliance zu gewährleisten, und ihre Lieferanten dabei als wichtige Partner betrachten.

Datenminimierung

Ein wichtiger Bestandteil der DSGVO-Anforderungen des eingebauten Datenschutzes ist es, dass Organisationen ihre Dienste so datenarm wie möglich gestalten. Das bedeutet, dass jederzeit ein guter Überblick und umfassende Kontrolle über die Daten in einer Organisation besteht, was wiederum bei deren Verwaltung unterstützt. Das Admin-Dashboard von Dropbox Business ist ein nützliches Tool hierfür: Es ermöglicht Ihnen, Teamaktivitäten zu überwachen, verbundene Geräte anzuzeigen und Freigabeaktivitäten zu prüfen. Wir bemühen uns, die Grundsätze des eingebauten Datenschutzes auch in neue Produkte und Funktionen einzubetten.

Datenschutz und -wiederherstellung

Der Schutz verlorener Geräte, der Versionsverlauf und die Dateiwiederherstellung können dabei helfen, sich vor versehentlichem Verlust, Schädigung oder Vernichtung personenbezogener Daten zu schützen. Außerdem unterstützen diese Funktionen bei der Möglichkeit, den Zugang zu und die Verfügbarkeit von personenbezogenen Daten nach einem Vorfall schnell wiederherzustellen. Auch die Zwei-Faktor-Authentifizierung ist eine wichtige Maßnahme, mit der wir den Schutz Ihrer Daten fördern möchten.

Dokumentation

Außerdem werden Organisationen durch die DSGVO eingehender dazu verpflichtet, detaillierte Aufzeichnungen über ihre Verarbeitungsvorgänge zu führen. Unsere Prüfungs- und Aktivitätsprotokolle helfen Ihnen dabei, Ihre Verarbeitungsvorgänge besser zu verstehen und so Ihre Aufzeichnungen zu vervollständigen.

Zugriffsverwaltung

Im Admin-Dashboard von Dropbox Business können Sie den Zugriff von Teammitgliedern auf Dateien, Ordner und Paper-Dokumente problemlos verwalten. Mit der Linkberechtigungsfunktion können Sie freigegebene Dateilinks mit einem Kennwort schützen, Gültigkeitsdauern für einen temporären Zugriff festlegen und den Zugriff auf Ihre Mitarbeiter beschränken. Sollten sich die Zuständigkeitsbereiche von Nutzern ändern, können Sie mithilfe der Kontoübertragung Dateien und Eigentumsrechte an Paper-Dokumenten problemlos von einem Nutzer an einen anderen übergeben.

Administratoren haben zudem die Möglichkeit, den Zugriff eines Nutzers auf sein Konto zu sperren und die Daten ihrer Organisation zu schützen, ohne dazu die Nutzerdaten oder Freigabebeziehungen löschen zu müssen. Und zu guter Letzt erlaubt es Ihnen das Remote-Löschen, Dateien und Paper-Dokumente von verlorenen oder gestohlenen Geräten zu entfernen.

EU-Infrastruktur

Zwar müssen Daten laut DSGVO nicht zwangsweise in der EU gehostet werden, dennoch bietet Dropbox qualifizierten Nutzern von Dropbox Business und Dropbox Education die Möglichkeit, ihre Dateien (Blöcke) in der EU zu speichern. EU-basierte Dateispeicher werden über die Infrastruktur von Amazon Web Services (AWS) bereitgestellt. Möchten Sie mehr über unsere EU-Infrastruktur erfahren, wenden Sie sich an unser Vertriebsteam.

Dropbox

Gemeinsam für den Schutz Ihrer Daten

Dropbox arbeitet aktiv mit seinen Nutzern zusammen, um deren personenbezogene Daten zu schützen. Wir ergreifen umfangreiche Maßnahmen, um unsere Infrastruktur, unser Netzwerk und unsere Anwendungen zu schützen und um unsere Mitarbeiter in den Bereichen Sicherheit und Datenschutz zu unterweisen, und der Aufbau einer Kultur mit Vertrauenswürdig-keit als oberster Priorität ist uns wichtig. Des Weiteren unterziehen wir unsere Systeme und Praktiken rigorosen Prüfungen und Tests durch unabhängige Dritte.

Doch auch die Nutzer selbst spielen beim Schutz ihrer personenbezogenen Daten eine große Rolle. Dropbox ermöglicht es Ihnen, Ihr Konto so zu konfigurieren, nutzen und überwachen, dass die Datenschutz-, Sicherheits- und Compliance-Anforderungen Ihrer Organisation erfüllt werden. In unserem Leitfaden zur gemeinsamen Verantwortung erfahren Sie, was wir tun, um Ihre Daten zu schützen, und was Sie tun können, um Transparenz und Kontrolle Ihrer personenbezogenen Daten zu gewährleisten.

Zusammenfassung

Jeden Tag schenken Millionen Nutzer Dropbox ihr Vertrauen. Damit wir diesem Vertrauen auch würdig sind, bauen wir Dropbox auf dem Fundament Sicherheit und Datenschutz auch in Zukunft weiter aus. Unsere Verpflichtung gegenüber unseren Nutzern, ihre personenbezogenen Daten zu schützen, steht im Mittelpunkt all unserer Entscheidungen. Wenden Sie sich für weitere Informationen per E-Mail an privacy@dropbox.com. Weitere Informationen zur DSGVO finden Sie außerdem in unserem DSGVO-Guidance-Center.