Dropbox

Informations-sicherheit und Datenschutz

Einleitung

Personenbezogene Daten spielen in der heutigen Gesellschaft ebenso wie in der Wirtschaft eine große Rolle. Kontrolle und Klarheit in Bezug auf die Verarbeitung und den Schutz personenbezogener Daten durch Organisationen nehmen einen immer höheren Stellenwert ein. Gleichzeitig wächst der Bedarf an eindeutigen Richtlinien, an denen sich Organisationen orientieren können, um personenbezogene Daten zu schützen.

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 schützen Ihre personenbezogenen Daten. In den Allgemeinen Geschäftsbedingungen von Dropbox werden Ihre Verantwortlichkeiten erläutert, wenn Sie unsere Dienste nutzen. Unsere Datenschutzrichtlinien beinhalten unser Datenschutzversprechen an die Nutzer und erklären Ihnen, wie wir Ihre personenbezogenen Daten sammeln, nutzen und verarbeiten, wenn Sie unsere Dienste nutzen. Sofern Sie in der Europäischen Union (EU) ansässig sind, werden Ihre personenbezogenen Daten von Dropbox International Unlimited Company in Irland kontrolliert.

Ihre Organisation ist als Nutzer von Dropbox Business oder Dropbox Education für jegliche personenbezogenen Daten verantwortlich, auf die Dropbox in Verbindung mit Ihrer Dropbox Business- oder Dropbox Education-Nutzung zugreift. Der Verantwortliche bestimmt, zu welchem Zweck und in welcher Weise personenbezogene Daten verarbeitet werden. Wenn Sie Dropbox Business oder Dropbox Education nutzen, handelt Dropbox als Auftragsverarbeiter für Ihre Organisation. Unsere Geschäftsvereinbarung beinhaltet auch Verpflichtungen in Bezug auf Datenverarbeitung und internationale Datenübertragung.

Unsere Erfolge im Bereich Compliance

Anhand der Compliance lässt sich die Vertrauenswürdigkeit eines Dienstes effektiv überprüfen. Wir lassen unsere Sicherheits- und Datenschutzverfahren gern überprüfen und stellen Nachweise zur Verfügung, dass sie den gemeinhin anerkannten Standards und Regelungen wie ISO 27001, ISO 27017, ISO 27018, dem deutschen C5-Anforderungskatalog des BSI sowie SOC 1, 2 und 3 entsprechen. So waren wir zum Beispiel einer der ersten Clouddienstanbieter mit ISO 27018-Zertifizierung. Das ist die weltweit anerkannte Norm für führende Datenschutz- und Informationssicherheitsverfahren in der Cloud. 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 Business und Dropbox Education beziehen, dass die Mehrheit unserer Kontrollen jedoch auch für Nutzer von Dropbox Basic, Plus und Professional gilt. Weitere Informationen zu den Standards, die wir einhalten, und zur Verifizierung unserer Verfahren finden Sie auf unserer Compliance-Webseite.

Wenn Sie weitere Details über die Sicherheitsfunktionen und -richtlinien von Dropbox erfahren möchten, lesen Sie bitte das Dropbox Business-Whitepaper zur Sicherheit oder kontaktieren Sie sales@dropbox.com

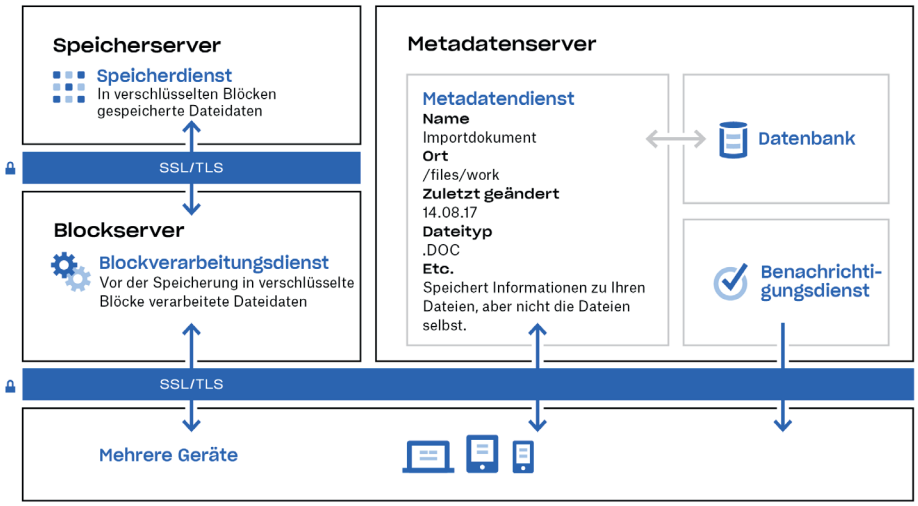
Dropbox

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 Dateiinfrastruktur von Dropbox besteht aus den im Diagramm unten abgebildeten Bestandteilen.



Blockserver

Dropbox bietet einen einzigartigen Sicherheitsmechanismus, der über die herkömmliche Verschlüsselung zum Schutz von Nutzerdaten hinausgeht. Blockserver verarbeiten die Dateien der Dropbox-Anwendungen, indem sie jede Datei in Blöcke unterteilen, jeden Block mit einem starken Schlüssel schützen und nur die veränderten Blöcke synchronisieren. Wenn eine Dropbox-Anwendung eine neue Datei oder Änderungen an einer vorhandenen Datei erkennt, informiert die Anwendung die Blockserver über die Änderung. Daraufhin werden die neuen oder veränderten Dateiblöcke verarbeitet und an die Speicherserver übertragen.

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 den Metadatenservern herstellen muss, um alle Änderungen synchronisieren zu können.

Metadatenserver

Grundinformationen, sogenannte Metadaten, werden in einem eigens dafür vorgesehenen Speicherdienst aufbewahrt und dienen als Index für die Daten in den Nutzerkonten. Dropbox-Metadaten werden in einem MySQL-Datenbankdienst gespeichert und nach Bedarf fragmentiert und repliziert, um Leistungs- und Hochverfügbarkeitsanforderungen zu erfüllen. Metadaten umfassen grundlegende Konto- und Nutzer-informationen 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 Funktionen wie Versionsverlauf, Wiederherstellung und Synchronisierung unterstützt werden.

Speicherserver

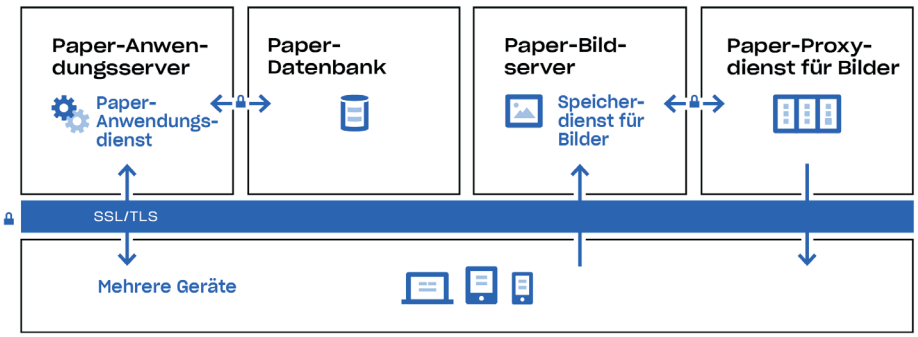
Wenn Dateien von den Blockservern in Blöcke unterteilt und verschlüsselt wurden, werden die Inhalte dieser Dateiblöcke auf den Speicherservern gespeichert. Die Speicherserver nutzen das Content Addressed Storage (CAS)-Speicherverfahren. Dabei wird jeder verschlüsselte Dateiblock anhand seines Hash-Wertes abgerufen.

Wenn Sie weitere Details über die Sicherheitsfunktionen und -richtlinien von Dropbox erfahren möchten, lesen Sie bitte das Dropbox Business-Whitepaper zur Sicherheit oder kontaktieren Sie sales@dropbox.com

Dropbox

Unsere Infrastruktur: Paper

Dropbox Paper (Paper) ist ein Element des Dropbox-Produkts. Paper nutzt jedoch hauptsächlich 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-Proxydienst für Bilder

Der Paper-Proxydienst für Bilder liefert Voransichten von Abbildungen, die in Paper-Dokumente eingefügt werden, sowie von Hyperlinks in Paper-Dokumenten. Wenn Abbildungen in Paper-Dokumente eingefügt werden, holt sich der Paper-Proxydienst für Bilder die auf den Paper-Bildservern gespeicherten Bilddaten über eine verschlüsselte Verbindung. Wenn Hyperlinks in Paper-Dokumente eingebettet werden, holt sich der Paper-Proxydienst für Bilder die Bilddaten vom jeweiligen Quelllink und erstellt unter Verwendung des HTTP- oder HTTPS-Protokolls (Vorgabe des Quelllinks) eine Voransicht der Abbildung.

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 (z. B. der Titel, Freigaben und Berechtigungen, Projekt- und Dateizuordnungen usw.) und Inhalte des Paper-Dokuments wie Kommentare und Aufgaben. Die Paper-Datenbanken werden nach Bedarf fragmentiert und repliziert, um Leistungs- und Hochverfügbarkeits-anforderungen zu erfüllen.

Paper-Bildserver

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.

Wenn Sie weitere Details über die Sicherheitsfunktionen und -richtlinien von Dropbox erfahren möchten, lesen Sie bitte das Dropbox Business-Whitepaper zur Sicherheit oder kontaktieren Sie sales@dropbox.com

Dropbox

Dropbox-Kontrollen: Unsere internen Verfahren

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 eine Priorität ist. 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 Datenschutzrichtlinien, bevor sie Systemzugriff erhalten. Sie nehmen an verpflichtenden Sicherheits- und Datenschutzschulungen für neue Mitarbeiter sowie jährlichen Folgeschulungen teil. Des Weiteren erhalten unsere Mitarbeiter regelmäßige Schulungen zu Sicherheitsbewusstsein per E-Mail, in Gesprächen, Präsentationen und verfügbaren Ressourcen in unserem Intranet.

Verschlüsselung bei der Übertragung

Dateidaten, die zwischen einem Dropbox-Client (Desktop, Mobilgerät, API oder online) und den Front-End-Servern übertragen werden, werden verschlüsselt, um ihre sichere Zustellung zu gewährleisten. Ebenso 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. Ebenso 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 der Administrator eines Dropbox Business- oder Dropbox Education-Teams eine Datei zum endgültigen Löschen auswählt, wird die dauerhafte Entfernung der Datei eingeleitet. Ebenso verhält es sich, wenn ein Dropbox-Nutzer oder der Administrator eines Dropbox Business- oder Dropbox Education-Teams ein Paper-Dokument zum endgültigen Löschen auswählt. Die Dokument- und Bilddaten in Paper werden dauerhaft entfernt.

Private Anfrage nach Datenzugriff

Nutzer können sich auf der Website anmelden und ihre Kontoseiten aufrufen, um Informationen 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 Nutzer Zugriff auf andere von uns gesammelte Informationen zu ihrer Person oder deren Löschung beantragen. Weitere Informationen hierzu finden Sie im Dropbox-Hilfecenter.

Wenn Sie weitere Details über die Sicherheitsfunktionen und -richtlinien von Dropbox erfahren möchten, lesen Sie bitte das Dropbox Business-Whitepaper zur Sicherheit oder kontaktieren Sie sales@dropbox.com

Dropbox

Grundsätze zu Auskunftsersuchen durch Regierungsstellen

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 Auskunftsersuchen 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

Auskunftsersuchen durch Regierungen sollten begrenzt sein bzgl. der nachgefragten Informationen und sich auf spezifische Personen und rechtmäßige Untersuchungen beschränken. Wir werden uns 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 Dropbox Business-Whitepaper zur Sicherheit.

Andere, die für 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 (z. B. für Kundendienst und IT). Diese Dritten greifen nur unter Einhaltung unserer Datenschutzrichtlinien 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. Jeder externe Mitarbeiter wird gründlich geprüft, wir führen Sicherheitsprüfungen durch und untersuchen regelmäßig die Verträge, um sicherzugehen, dass jeder Beteiligte in der Lage ist, unser Datenschutzversprechen zu erfüllen.

Internationale Datenübertragungen

Dropbox vertraut für internationale Übertragungen personenbezogener Daten von der EU in die USA auf eine Reihe von Rechtsinstrumenten. Wir sind nach dem EU-US-Datenschutzschild-Übereinkommen und dem Swiss-US-Datenschutzschild-Übereinkommen berechtigt, personenbezogene Daten zu sammeln, zu verarbeiten, zu speichern und aus der EU und der Schweiz in die USA zu übertragen. Neben dem Datenschutzschild bietet Dropbox starke vertragliche Garantien für Datenschutz in seinen Diensten und verwendet Muster-Vertragsklauseln der EU zur Sicherung internationaler Datenübertragungen.

Wenn Sie weitere Details über die Sicherheitsfunktionen und -richtlinien von Dropbox erfahren möchten, lesen Sie bitte das Dropbox Business-Whitepaper zur Sicherheit oder kontaktieren Sie sales@dropbox.com

Dropbox

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. In der EU niedergelassene Organisationen und solche, die personenbezogene Daten von in der EU ansässigen Personen verarbeiten, müssen die Bestimmungen der DSGVO einhalten.

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 Clouddiensten, 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.

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. Das ist besonders wichtig, da laut DSGVO verstärkt Wert darauf gelegt wird, dass Entscheidungen und Verfahrensweisen in Zusammenhang mit personenbezogenen Daten dokumentiert werden.

Wenn Sie weitere Details über die Sicherheitsfunktionen und -richtlinien von Dropbox erfahren möchten, lesen Sie bitte das Dropbox Business-Whitepaper zur Sicherheit oder kontaktieren Sie sales@dropbox.com

Dropbox

Nutzer auf dem Weg zur DSGVO unterstützen

Dropbox beinhaltet 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 dabei hilft, Team-Aktivitäten zu überwachen, verknüpfte Geräte einzusehen und Freigabeaktivitäten zu protokollieren.

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 können Sie den Zugriff von Teammitgliedern auf Dateien, Ordner und Paper-Dokumente bequem verwalten. Mit unseren Berechtigungsoptionen für freigegebene Links können Sie diese durch Kennwörter 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 Kontoübertragung verwenden, um Dateien und das Eigentumsrecht an Paper-Dokumenten von einem Nutzer auf einen anderen zu übertragen.

Administratoren können auch den Zugriff von Nutzern auf ihr Konto sperren, dabei jedoch deren Daten und Freigabebeziehungen sichern, um die Informationen Ihrer Organisation zu schützen. Mit der Funktion Remote-Löschen können Sie schließlich alle Dateien und Paper-Dokumente von Geräten entfernen, die abhanden gekommen 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 Dropbox Business- und Dropbox Education-Kunden 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.

Wenn Sie weitere Details über die Sicherheitsfunktionen und -richtlinien von Dropbox erfahren möchten, lesen Sie bitte das Dropbox Business-Whitepaper zur Sicherheit oder kontaktieren Sie sales@dropbox.com

Dropbox

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, wir bauen eine Sicherheitskultur dort auf, wo Zuverlässigkeit oberste Priorität hat, und lassen gründliche Tests und Überprüfungen von unabhängigen Dritten an unseren Systemen vornehmen.

Doch auch die Nutzer tragen maßgeblich zum Schutz ihrer personenbezogenen Daten bei. Dropbox ermöglicht es Ihnen, Ihr Konto individuell einzurichten, zu nutzen und zu überwachen – genau so, wie es den Bedürfnissen Ihrer Organisation hinsichtlich Datenschutz, Sicherheit und Compliance entspricht. Unser Leitfaden zur gemeinsamen Verantwortung hält weitere Informationen für Sie bereit, wenn Sie erfahren möchten, wie Sie Ihr Konto schützen und die Kontrolle über Ihre personenbezogenen Daten behalten können.

Zusammenfassung

Täglich setzen Millionen von Nutzern ihr Vertrauen in Dropbox. Das bedeutet uns sehr viel, und daher haben Sicherheit und Datenschutz bei der Entwicklung 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. Weitere Informationen zur DSGVO finden Sie in unserem DSGVO-Guidance-Center.

Wenn Sie weitere Details über die Sicherheitsfunktionen und -richtlinien von Dropbox erfahren möchten, lesen Sie bitte das Dropbox Business-Whitepaper zur Sicherheit oder kontaktieren Sie sales@dropbox.com