Dropbox

Prywatność i ochrona danych

Wstęp

Ochrona danych osobowych jest niezwykle istotna dla społeczeństwa i gospodarki. Użytkownicy coraz częściej oczekują większej kontroli i jasności odnośnie do sposobu, w jaki ich dane są wykorzystywane i chronione przez organizacje, z którymi wchodzą w interakcję.

Zaufanie jest podstawą naszych relacji z milionami osób i firm na całym świecie. Cenimy sobie Twoje zaufanie i poważnie traktujemy odpowiedzialność za ochronę Twoich danych osobowych.

Nasze zobowiązania wobec Ciebie

Ochrona Twoich danych jest dla nas bardzo ważną kwestią. Warunki dotyczące usług Dropbox określają zobowiązania użytkownika podczas korzystania z tych usług. Nasza Polityka prywatności opisuje nasze obowiązki wobec użytkowników w zakresie prywatności i określa sposób, w jaki gromadzimy, wykorzystujemy i przetwarzamy dane osobowe użytkowników naszych usług. Jeśli mieszkasz w Ameryce Północnej (tj. w USA, Kanadzie lub Meksyku), dostawcą usług jest Dropbox Inc.

W przypadku wszystkich innych użytkowników administratorem danych osobowych jest Dropbox International Unlimited Company.

Jeśli jesteś użytkownikiem platformy Dropbox Business lub Dropbox Education, Twoja organizacja jest administratorem wszystkich danych osobowych dostarczanych Dropbox w związku z korzystaniem z Dropbox Business lub Dropbox Education.

Administrator danych określa cele i sposoby przetwarzania danych osobowych. Dropbox jest podmiotem przetwarzającym dane w imieniu Twojej organizacji, gdy korzystasz z platformy Dropbox Business lub Dropbox Education, a nasza Umowa handlowa określa zobowiązania związane z przetwarzaniem danych i międzynarodowym transferem danych.

Nasza historia: Zgodność

Zgodność jest skutecznym sposobem, aby potwierdzić wiarygodność danej usługi. Wspieramy i z przyjemnością zapewniamy niezależną weryfikację zgodności naszych praktyk bezpieczeństwa i prywatności z najbardziej powszechnymi normami i przepisami, np. ISO 27001, ISO 27017, ISO 27018, HIPPA/HITECH, niemieckimi BSI C5 oraz SOC 1, 2 i 3.

Ponadto jesteśmy jednym z pierwszych dostawców usług w chmurze, którzy otrzymali certyfikat zgodności z normą ISO 27018, uznanym na całym świecie standardem praktyk dotyczących prywatności i ochrony danych w chmurze. Nasi niezależni audytorzy zewnętrzni badają nasze procedury kontrolne oraz przedstawiają swoje sprawozdania i opinie. W miarę możliwości dzielimy się tymi informacjami z użytkownikami.

Należy pamiętać, że chociaż zakres naszych certyfikatów i raportów z audytu zwykle odnosi się do platform Dropbox Business i Dropbox Education, większość naszych kontroli dotyczy również użytkowników Dropbox Basic, Plus i Professional. Więcej informacji na temat przestrzeganych przez nas norm oraz sposobu, w jaki weryfikujemy nasze praktyki, można znaleźć na naszej stronie dotyczącej zgodności.

Aby uzyskać więcej informacji na temat funkcji i zasad bezpieczeństwa Dropbox, zapoznaj się z Białą księgą bezpieczeństwa Dropbox Business lub wyślij wiadomość na adres sales@dropbox.com

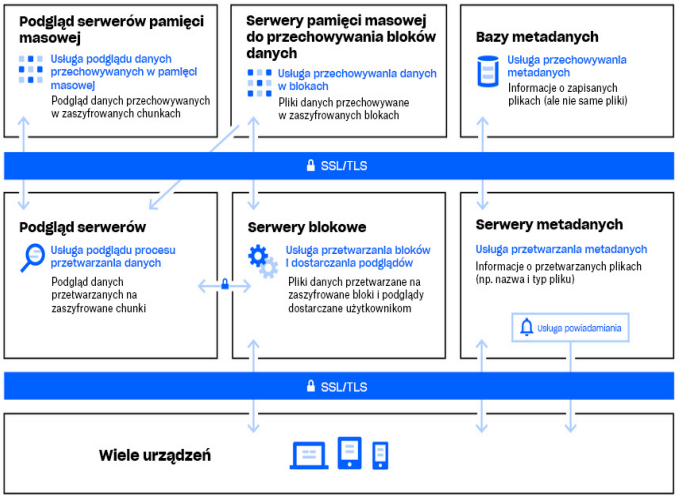
Dropbox

Architektura Dropbox: Ochrona Twoich danych osobowych

W Dropbox uważamy, że ochrona danych osobowych zaczyna się od zapewnienia bezpieczeństwa danych. Dlatego usługa Dropbox została stworzona z wykorzystaniem wielu warstw ochrony, w tym bezpieczne przesyłanie danych, szyfrowanie oraz kontrolę z poziomu aplikacji, zastosowanych na różnych poziomach skalowalnej i bezpiecznej infrastruktury.

Nasza infrastruktura: Pliki

Infrastruktura plików Dropbox obejmuje składniki przedstawione na poniższym schemacie.



Serwery metadanych

Niektóre podstawowe informacje o danych użytkownika, tzw. metadane, są przechowywane we własnej, odrębnej usłudze przechowywania i działają jak indeks danych na kontach użytkowników. Metadane obejmują podstawowe informacje o koncie i użytkowniku, np. adres e-mail, imię i nazwisko oraz nazwy urządzeń. Metadane zawierają również podstawowe informacje o plikach, w tym nazwy i typy plików, które pomagają obsługiwać funkcje takie jak historia wersji, odzyskiwanie i synchronizacja.

Bazy metadanych

Metadane plików są przechowywane w usłudze bazy danych opartej na systemie MySQL i w razie potrzeby są partycjonowane i replikowane, aby spełnić wymagania z zakresu wydajności i wysokiej dostępności.

Serwery bloków

Dropbox z założenia zapewnia unikalny mechanizm bezpieczeństwa, który wykracza poza tradycyjne szyfrowanie w celu ochrony danych użytkownika. Serwery bloków przetwarzają pliki pochodzące z różnych aplikacji Dropbox, dzieląc każdy plik na bloki, szyfrując każdy blok przy użyciu silnego szyfru oraz synchronizując tylko te bloki, które uległy modyfikacji pomiędzy kolejnymi wersjami pliku. Gdy aplikacja Dropbox wykrywa nowy plik lub zmiany w istniejącym pliku, powiadamia serwery bloków o zmianie, a nowe lub zmodyfikowane bloki plików zostają przetworzone i przesłane do serwera przechowywania.

Serwery przechowywania bloków

Właściwa zawartość plików użytkowników jest przechowywana w zaszyfrowanych blokach na serwerach przechowywania bloków. Przed przekazaniem klient Dropbox dzieli pliki na bloki plików w ramach przygotowań do przechowywania. Serwery przechowywania bloków działają jako system Storage-Addressable Storage (CAS), a każdy zaszyfrowany blok pliku jest pobierany na podstawie jego wartości skrótu.

Serwery podglądu

Serwery podglądu odpowiadają za tworzenie podglądów plików. Podglądy to renderowanie pliku użytkownika w innym formacie pliku, który lepiej nadaje się do szybkiego wyświetlania na urządzeniu użytkownika końcowego. W celu wygenerowania podglądów serwery podglądu pobierają bloki plików z serwerów przechowywania bloków. Po otrzymaniu żądania podglądu pliku serwery podglądu pobierają podgląd z pamięci podręcznej serwerów przechowywania podglądów i przesyłają je do serwerów bloków. Podglądy są ostatecznie dostarczane użytkownikom przez serwery bloków.

Serwery przechowywania podglądów

Podglądy z pamięci podręcznej są przechowywane w zaszyfrowanych formatach na serwerach przechowywania podglądów.

Usługa powiadomień

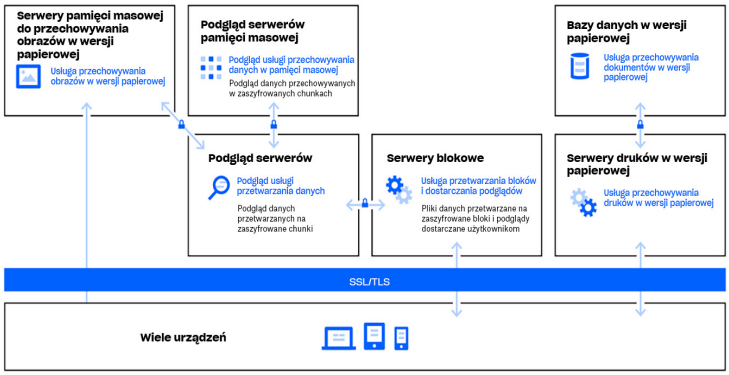
Jest to osobna usługa służąca do monitorowania kont Dropbox pod względem zmian. Żadne pliki ani metadane nie są tutaj przechowywane ani przenoszone. Każdy klient nawiązuje połączenie typu long poll z usługą powiadomień, a następnie oczekuje. W przypadku zmiany jakiegokolwiek pliku w Dropbox usługa powiadomień sygnalizuje zmianę odpowiedniemu klientowi (klientom) poprzez zamknięcie połączenia long poll. Zamknięcie połączenia oznacza, że w celu zsynchronizowania wszelkich zmian klient musi się bezpiecznie połączyć z serwerami metadanych.

Aby uzyskać więcej informacji na temat funkcji i zasad bezpieczeństwa Dropbox, zapoznaj się z Białą księgą bezpieczeństwa Dropbox Business lub wyślij wiadomość na adres sales@dropbox.com

Dropbox

Nasza infrastruktura: Paper

Dropbox Paper (Paper) to funkcja produktu Dropbox, która korzysta z najbardziej unikatowego zestawu systemów w środowisku infrastruktury Dropbox. Infrastruktura Paper składa się z elementów przedstawionych na poniższym schemacie .



Serwery aplikacji Paper

Serwery aplikacji Paper przetwarzają żądania użytkowników, renderują u użytkowników wyjściową postać edytowanych dokumentów Paper i wykonują zadania związane z powiadomieniami. Serwery aplikacji Paper zapisują zmiany użytkowników w bazach danych Paper, gdzie trafiają one do trwałej pamięci masowej. Sesje komunikacji między serwerami aplikacji Paper i bazami danych Paper są szyfrowane silnym szyfrem.

Bazy danych Paper

Właściwa zawartość dokumentów Paper użytkowników, a także pewne metadane na temat tych dokumentów, są szyfrowane w trwałej pamięci masowej w bazach danych Paper. Obejmuje to informacje o każdym dokumencie Paper (takie jak jego tytuł, członkowie i uprawnienia, powiązania z projektem i folderem itd.) oraz zawartość samego dokumentu, łącznie z komentarzami i zadaniami. Bazy danych Paper są partycjonowane i replikowane odpowiednio do potrzeb, aby spełnić wymagania z zakresu wydajności i wysokiej dostępności.

Serwery przechowywania Paper

Obrazy przesłane do dokumentów Paper są przechowywane na serwerach obrazów Paper i w takiej postaci szyfrowane. Transmisja danych obrazów między aplikacją Paper i serwerami obrazów Paper odbywa się w ramach zaszyfrowanej sesji.

Serwery podglądu

Serwery podglądu tworzą podglądy obrazów przesłanych do dokumentów Paper i hiperłączy osadzonych w tych dokumentach. W przypadku obrazów przesyłanych do dokumentów Paper serwery podglądu pobierają dane dotyczące obrazu przechowywane na serwerach przechowywania obrazów Paper za pośrednictwem zaszyfrowanego kanału. W przypadku hiperłączy osadzonych w dokumentach Paper serwery podglądu pobierają dane dotyczące obrazu i tworzą jego podgląd przy użyciu szyfrowania, zgodnie z tym, co określa łącze źródłowe. Podglądy są ostatecznie dostarczane użytkownikom przez serwery bloków.

Serwery przechowywania podglądów

Do przechowywania podglądów obrazów w pamięci podręcznej narzędzie Paper korzysta z serwerów przechowywania podglądów opisanych na schemacie infrastruktury Dropbox. Fragmenty podglądu z pamięci podręcznej są przechowywane w zaszyfrowanych formatach na serwerach przechowywania podglądów.

Dropbox

Kontrole Dropbox: Nasze wewnętrzne praktyki

Podejmujemy kompleksowe działania w celu ochrony naszej infrastruktury, sieci i aplikacji. Stosowane przez nas środki bezpieczeństwa obejmują m.in. szyfrowanie przechowywanych danych, szyfrowanie transferowanych danych i trwałe usuwanie plików.
Aby budować kulturę skupioną na zaufaniu, wszystkim naszym pracownikom oferujemy również gruntowne szkolenia w zakresie prywatności i bezpieczeństwa. Poniżej znajdują się szczegółowe informacje dotyczące niektórych stosowanych przez nas kontroli:

Szkolenia

Ochrona danych osobowych naszych użytkowników obejmuje m.in. budowanie i rozwijanie kultury bezpieczeństwa i świadomości na temat prywatności. Przed uzyskaniem dostępu do systemów pracownicy Dropbox muszą zaakceptować zasady bezpieczeństwa, w tym polityki prywatności danych użytkownika. Dostęp do takich systemów przyznaje się jedynie pracownikom, którym jest on niezbędny. Co roku pracownicy uczestniczą również w obowiązkowych szkoleniach z zakresu bezpieczeństwa i prywatności.

Szyfrowanie transferowanych danych

Aby zapewnić bezpieczną dostawę i chronić dane plików transferowanych między klientem Dropbox (obecnie komputer stacjonarny, telefon komórkowy, API lub Internet) a serwerami front-endowymi Dropbox, negocjowane jest szyfrowane połączenie. Szyfrowane połączenie jest również negocjowane w celu ochrony danych dokumentów Paper przesyłanych między klientem Paper (obecnie telefon komórkowy, API lub Internet) a hostowaną usługą. Połączenia te są szyfrowane przy użyciu protokołu SSL (Secure Sockets Layer)/TLS (Transport Layer Security), tworząc bezpieczny tunel chroniony przez mechanizm szyfrowania AES z kluczem 128-bitowym lub wyższym.

Szyfrowanie przechowywanych danych

Pliki przesłane przez użytkowników są przechowywane na serwerach przechowywania Dropbox jako osobne bloki plików. Każdy blok jest szyfrowany za pomocą 256-bitowego klucza Advanced Encryption Standard (AES).

Synchronizowane są wyłącznie bloki, które zostały zmodyfikowane pomiędzy różnymi wersjami plików. Również dane dokumentów Paper przechowywane w bazach danych Paper są szyfrowane za pomocą 256-bitowego klucza Advanced Encryption Standard (AES).

Trwałe usuwanie plików i dokumentów Paper

Oznaczenie pliku do trwałego usunięcia przez jakiegokolwiek użytkownika Dropbox albo administratora Dropbox Business lub zespołu Dropbox Education uruchomia proces trwałego usuwania pliku. Gdy użytkownik lub administrator zespołu Dropbox Business lub Dropbox Education oznaczy dokument Paper do trwałego usunięcia, uruchamia się podobny proces trwałego usuwania danych dokumentu Paper i danych obrazu.

Żądania dostępu do danych osobowych

Aby uzyskać dostęp do danych osobowych wykraczających poza pliki i dokumenty Paper przechowywane w Dropbox, użytkownik może zalogować się w witrynie i przejść na stronę swojego konta. Strona konta zawiera m.in. informacje dotyczące imienia i nazwiska oraz adresu e-mail powiązanego z kontem. Adresy IP połączonych sesji, komputerów i urządzeń mobilnych, a także aplikacji połączonych z ich kontami można również wyświetlać na stronach bezpieczeństwa i stronach połączonych aplikacji.

Użytkownicy Dropbox mają również możliwość zażądania dostępu lub usunięcia innych danych osobowych, które Dropbox mógł zgromadzić na ich temat.
Więcej informacji na temat tego procesu można znaleźć w Centrum Pomocy Dropbox.

Zarządzanie prywatnością w Dropbox

Zespół Programu prywatności odpowiada za obsługę Programu prywatności Dropbox. Realizuje on nasze kluczowe inicjatywy dotyczące prywatności i wspiera ochronę prywatności od samego początku naszego cyklu życia danych. Program prywatności Dropbox jest dodatkowo wspierany przez kilka międzyfunkcyjnych podzespołów prawnych. Podzespoły zapewniają dodatkową wiedzę specjalistyczną niezbędną do obsługi i nadzorowania codziennych zadań realizowanych w zakresie Programu prywatności.

Zespół inspektora ochrony danych (IOD) działa niezależnie od innych funkcji związanych z prywatnością, a jego zadaniem jest zapewnienie zgodności i nadzoru nad prywatnością oraz bezpośrednie wsparcie inspektora ochrony danych w wykonywaniu obowiązków. Inspektor ochrony danych (IOD) to lokalny przedstawiciel UE, z którym można się skontaktować pod adresem privacy@dropbox.com.

Dropbox

Zasady dotyczące rządowych zapytań o dane

Zdajemy sobie sprawę, że powierzając nam swoje dane osobowe, oczekujesz zachowania przez nas poufności. Podobnie jak większość usług internetowych, Dropbox czasami otrzymuje zapytania od organów rządowych poszukujących informacji o naszych użytkownikach.

Poniższe zasady opisują sposób, w jaki traktujemy rządowe zapytania o dane.

Być transparentnym

Uważamy, że usługi internetowe powinny mieć prawo do publikowania danych na temat liczby i typów otrzymanych zapytań rządowych oraz do powiadamiania osób, których dotyczyły zapytania. Ten rodzaj przejrzystości wzmacnia pozycję użytkowników, ponieważ pozwala im lepiej poznać przypadki i wzorce zbyt daleko sięgających ingerencji władz. Będziemy nadal publikować szczegółowe informacje na temat tych zapytań i walczyć o prawo do przekazywania większej ilości ważnych informacji.

Walka z zapytaniami o zbyt szerokim zakresie

Rządowe zapytania o dane powinny być ograniczone co do zakresu przedmiotowych informacji i osób oraz powinny być powiązane z legalnymi dochodzeniami. Przeciwstawiamy się zapytaniom zbyt ogólnym i o zbyt szerokim zakresie.

Oferować usługi godne zaufania

Rządy nigdy nie powinny instalować technologii „backdoor” w usługach online lub naruszać ich infrastruktury w celu uzyskania danych o użytkownikach. Będziemy nadal działać w kierunku ochrony naszych systemów i zmiany prawa, aby było jasne, że ten rodzaj działalności jest nielegalny.

Ochrona wszystkich użytkowników

Przepisy przyznające ludziom różne stopnie ochrony w zależności od miejsca zamieszkania lub obywatelstwa są przestarzałe i nie odzwierciedlają globalnego charakteru usług internetowych. Nadal będziemy opowiadać się za reformą tych przepisów.

Zasady te, wraz z naszym rocznym sprawozdaniem w sprawie przejrzystości, są publicznie dostępne na stronie internetowej Dropbox pod adresem: https://www.dropbox.com/transparency.

Dodatkowe informacje na temat naszych kontroli i podejścia do ochrony danych osobowych można znaleźć w Białej księdze bezpieczeństwa Dropbox Business.

Inne podmioty pracujące dla Dropbox

Dropbox zarządza większością działań związanych ze świadczonymi przez nas usługami.Jednocześnie korzystamy z usług pewnych zaufanych stron trzecich w (np. dostawcy pomocy technicznej i usług informatycznych). Wspomniane strony trzecie mają dostęp do Twoich danych po to, by wykonać w naszym imieniu zadania zgodnie z Polityką prywatności, a my pozostajemy odpowiedzialni za to, by korzystały one z tych informacji zgodnie z naszymi instrukcjami.

Każda strona trzecia przechodzi rygorystyczny proces weryfikacji, w tym przeglądy bezpieczeństwa i regularne przeglądy umowne, w celu oceny ich zdolności do spełnienia naszych wymagań w zakresie ochrony danych.

Międzynarodowe transfery danych

Pod względem międzynarodowego transferu danych osobowych z UE do Stanów Zjednoczonych Dropbox opiera się na różnych mechanizmach prawnych. Posiadamy certyfikat w ramach programów Tarcza Prywatności UE-USA i Szwajcaria-USA w zakresie przechowywania, korzystania i zapisywania danych osobowych oraz ich przekazywania z Unii Europejskiej do Stanów Zjednoczonych. Oprócz Tarczy Prywatności, Dropbox zapewnia również silne gwarancje umowne dotyczące prywatności swoich usług i stosuje unijne wzory klauzul umownych w zakresie międzynarodowych transferów danych.

Dropbox

RODO: Ogólne rozporządzenie o ochronie danych

Ogólne rozporządzenie o ochronie danych osobowych, RODO, to rozporządzenie UE ustanawiające nowe przepisy dotyczące przetwarzania i ochrony danych osobowych osób, których dane dotyczą.

RODO to najważniejszy akt prawny UE dotyczący ochrony danych od czasu unijnej dyrektywy o ochronie danych z 1995 r. Wiele firm prowadzących działalność w Europie, w tym Dropbox, zainwestowało znaczne środki w przestrzeganie RODO.

RODO harmonizuje przepisy dotyczące ochrony danych w całej Europie i dostosowuje je do szybkich zmian technologicznych, które obserwujemy w ciągu ostatnich dwóch dekad.

Opiera się on na przeszłych ramach prawnych UE, w tym unijnej dyrektywie o ochronie danych, oraz nakłada nowe obowiązki i zobowiązania na organizacje przetwarzające dane osobowe. Wprowadza również nowe prawa osób fizycznych w odniesieniu do ich danych osobowych.

Organizacje z siedzibą w UE, a także organizacje przetwarzające dane osobowe podmiotów danych w UE, są zobowiązane do przestrzegania RODO.

Droga Dropbox do wdrożenia zasad RODO

Dropbox poważnie podchodzi do przestrzegania przepisów RODO. Poszanowanie prywatności i zasad bezpieczeństwa jest nieodłącznym elementem prowadzenia naszej działalności od momentu założenia firmy. Mimo że firma się rozwija, nacisk na ochronę danych i odpowiednie ich przetwarzanie nieustannie pozostaje jednym z naszych priorytetów. Dropbox od dawna wyprzedza zmiany w zakresie zgodności – jak już wspomnieliśmy, jesteśmy jednym z pierwszych dostawców usług w chmurze, którzy uzyskali certyfikat ISO 27018 dla naszych użytkowników biznesowych. Opierając się na tak solidnych fundamentach, Dropbox traktuje wymagania RODO jako okazję do udoskonalenia obecnych praktyk oraz podejmuje i stale rozwija bieżące inicjatywy, aby zapewnić stałą ochronę danych osobowych naszych użytkowników.

Dropbox rozpoczął wdrażanie postanowień RODO od razu po przyjęciu rozporządzenia w 2016 roku. Naszym pierwszym zadaniem było stworzenie wielofunkcyjnego zespołu składającego się z radców prawnych, specjalistów ds. bezpieczeństwa i zgodności oraz inżynierów produktu i infrastruktury. Nasz zespół przeprowadził pełną ocenę naszych obecnych praktyk w zakresie bezpieczeństwa i ochrony danych pod względem wymogów RODO.

Kolejnym krokiem była ocena działań związanych z przetwarzaniem danych osobowych i śledzenie cyklu życia danych osobowych za pośrednictwem naszych systemów. Zadania te czasami określa się jako realizujące Mapowanie danych i ocena wpływu na ochronę danych.

Aby zapewnić zgodność z wymogami RODO dotyczącymi odpowiedzialności za ochronę danych osobowych, od tego czasu nieustannie doskonalimy nasze wewnętrzne procesy i procedury. Jest to istotne, ponieważ RODO kładzie nacisk na dokumentowanie wszystkich decyzji i działań związanych z danymi osobowymi.

Aby uzyskać więcej informacji na temat funkcji i zasad bezpieczeństwa Dropbox, zapoznaj się z Białą księgą bezpieczeństwa Dropbox Business lub wyślij wiadomość na adres sales@dropbox.com

Dropbox

Wspieranie działań użytkowników w zakresie RODO

Dropbox zapewnia funkcje kontroli i widoczności, które ułatwiają zarządzanie zobowiązaniami dotyczącymi ochrony danych, w tym zgodności z RODO. Oczywiście zgodność z RODO w całej organizacji nie zaczyna się ani nie kończy na relacjach z dostawcami, takimi jak Dropbox. Nasze funkcje pomagają w zarządzaniu obowiązkami, nie stanowią jednak wystarczających środków, by zapewnić zgodność. Zgodność z RODO wymaga szerszego podejścia do przemieszczania i ochrony danych w organizacji. Każda organizacja powinna na własną rękę podejmować kroki, aby osiągnąć zgodność z dostawcami, ponieważ są oni ważnymi partnerami na tej drodze.

Minimalizacja danych
Zgodnie z RODO ważnym elementem wymogu zachowania prywatności na etapie projektowania jest projektowanie usług w sposób minimalizujący dane. Oznacza to należytą widoczność i kontrolę danych w organizacji w celu ułatwienia zarządzania nimi. Panel administratora Dropbox Business to przydatne narzędzie, które pomaga to osiągnąć, ponieważ umożliwia monitorowanie aktywności zespołu, przeglądanie podłączonych urządzeń i audyt udostępniania. Pracujemy nad wprowadzeniem zasad prywatności do nowych produktów i funkcji.

Ochrona i przywracanie danych
Ochrona utraconych urządzeń, historia wersji i odzyskiwanie plików pomagają chronić się przed przypadkową utratą, uszkodzeniem lub zniszczeniem danych osobowych. W przypadku wystąpienia zdarzenia losowego pozwalają również przywracać dostępność i dostęp do danych osobowych. Uwierzytelnianie dwustopniowe jest kolejnym ważnym środkiem ochrony danych, który warto stosować.

Ewidencjonowanie
RODO rozszerza również obowiązki organizacji w zakresie prowadzenia szczegółowej dokumentacji działań związanych z przetwarzaniem. Nasze dzienniki inspekcji i dzienniki aktywności pozwalają lepiej zrozumieć czynności przetwarzania w celu wsparcia prowadzenia dokumentacji.

Administracja dostępem

Panel administratora Dropbox Business umożliwia łatwe zarządzanie dostępem członków zespołu do plików, folderów i dokumentów Paper. W przypadku udostępnionych łącz do plików nasza funkcja zgody na łącze zapewnia możliwość zabezpieczenia hasłem udostępnionych łączy, ustawienia daty wygaśnięcia, aby udzielić tymczasowego dostępu, jak również ograniczenia dostępu do łącz przekazywanych w Twojej organizacji. W przypadku zmiany obowiązków wśród użytkowników nasze narzędzie do transferu kont umożliwia łatwe przenoszenie plików i własności dokumentów Paper od jednego użytkownika do drugiego.

Administratorzy mają również możliwość wyłączenia dostępu użytkownika do jego konta przy jednoczesnym zachowaniu jego danych i udostępnieniu relacji w celu zapewnienia bezpieczeństwa informacji w organizacji. Na koniec: funkcja zdalnego czyszczenia pozwala na usuwanie plików i dokumentów Paper z zagubionych lub skradzionych urządzeń.

Infrastruktura UE
Mimo że RODO nie wymaga przechowywania danych osobowych w UE, Dropbox oferuje upoważnionym klientom Dropbox Business i Dropbox Education możliwość przechowywania plików (bloków) w UE. Przechowywanie plików w UE i opiera się na infrastrukturze Amazon Web Services (AWS). Aby dowiedzieć się więcej o naszej infrastrukturze UE, skontaktuj się z naszym zespołem sprzedaży.

Aby uzyskać więcej informacji na temat funkcji i zasad bezpieczeństwa Dropbox, zapoznaj się z Białą księgą bezpieczeństwa Dropbox Business lub wyślij wiadomość na adres sales@dropbox.com

Dropbox

Wspólne działania w celu ochrony Twoich danych

Dropbox współpracuje z użytkownikami, aby zapewnić ochronę ich danych osobowych. Podejmujemy kompleksowe działania w celu ochrony naszej infrastruktury, sieci i aplikacji, szkolimy pracowników w zakresie praktyk bezpieczeństwa i prywatności, budujemy kulturę, w której godność zaufania jest najwyższym priorytetem, oraz poddajemy nasze systemy i praktyki rygorystycznym testom i audytom stron trzecich.

Należy jednak pamiętać, że użytkownicy również odgrywają kluczową rolę w ochronie swoich danych osobowych. Dropbox umożliwia konfigurowanie, używanie i monitorowanie konta w sposób, który spełnia potrzeby organizacji związane z prywatnością, bezpieczeństwem i zgodnością. Nasz przewodnik po wspólnej odpowiedzialności pozwala lepiej zrozumieć, co robimy, aby zapewnić bezpieczeństwo Twojego konta oraz co Ty możesz zrobić, aby zachować widoczność i kontrolę nad swoimi danymi osobowymi.

Podsumowanie

Każdego dnia miliony użytkowników pokładają zaufanie w Dropbox. Aby na nie zasłużyć, rozwijamy i będziemy nadal rozwijać Dropbox, kładąc nacisk na bezpieczeństwo i prywatność. Nacisk na ochronę danych osobowych naszych użytkowników leży u podstaw każdej podejmowanej przez nas decyzji. Więcej informacji można uzyskać, wysyłając wiadomość e-mail na adres privacy@dropbox.com. Aby dowiedzieć się więcej na temat RODO, można również odwiedzić nasze centrum doradztwa RODO.