Dropbox

Privasi dan Perlindungan Data

Pengantar

Data pribadi memiliki perang yang penting dalam masyarakat dan perekonomian. Setiap orang semakin menginginkan kendali dan kejelasan yang lebih baik mengenai bagaimana data pribadi mereka digunakan dan dilindungi oleh organisasi yang berhubungan dengan mereka.

Di Dropbox, kepercayaan merupakan dasar hubungan kami dengan jutaan orang dan bisnis di seluruh dunia. Kami menghargai kepercayaan yang Anda berikan dan kami bertanggung jawab untuk melindungi data pribadi Anda dengan serius.

Komitmen Kami Kepada Anda

Kami berkomitmen untuk melindungi data pribadi Anda. Persyaratan Layanan Dropbox menguraikan tanggung jawab Anda ketika menggunakan layanan kami. Kebijakan Privasi kami menjelaskan komitmen privasi kami terhadap pelanggan dan menjelaskan bagaimana kami mengumpulkan, menggunakan, dan menangani data pribadi Anda ketika Anda menggunakan layanan kami. Jika Anda tinggal di Amerika Utara (Amerika Serikat, Kanada, dan Meksiko), Dropbox, Inc. bertindak sebagai penyedia layanan Anda. Bagi semua pengguna lain, Dropbox International Unlimited Company bertindak sebagai pengontrol data pribadi Anda.

Jika Anda adalah pengguna Dropbox Business atau Dropbox Education, organisasi Anda bertindak sebagai pengontrol data untuk setiap data pribadi yang diberikan kepada Dropbox sehubungan dengan penggunaan Dropbox Business atau Dropbox Education oleh Anda. Pengontrol data menentukan tujuan dan cara memproses data pribadi. Dropbox bertindak sebagai pemroses data, yang memproses data atas nama organisasi Anda ketika Anda menggunakan Dropbox Business atau Dropbox Education, dan Perjanjian Bisnis kami mencakup komitmen yang terkait dengan pemrosesan data dan transfer data internasional.

Rekam Jejak Kami: Kepatuhan

Kepatuhan adalah cara efektif untuk memvalidasi ketepercayaan sebuah layanan. Kami mendukung dan senang memberikan verifikasi independen bahwa praktik-praktik keamanan dan privasi kami mematuhi standar dan peraturan yang paling banyak diterima, seperti ISO 27001, ISO 27017, ISO 27018, HIPPA/HITECH, Germany BSI C5, dan SOC 1, 2, dan 3.

Selain itu, kami adalah salah satu penyedia layanan awan pertama yang mendapatkan sertifikasi ISO 27018, standar yang diakui secara internasional untuk praktik-praktik terbaik dalam privasi awan dan perlindungan data. Auditor pihak ketiga independen menguji kontrol kami dan menyampaikan laporan dan opininya. Kami dapat membagikan laporan dan opini tersebut kepada Anda jika memungkinkan.

Mohon diingat, meskipun cakupan sertifikasi dan laporan audit kami umumnya mengacu pada Dropbox Business dan Dropbox Education, sebagian besar kontrol kami juga berlaku untuk pengguna Dropbox Basic, Plus, dan Professional. Informasi selengkapnya mengenai standar yang kami patuhi dan cara kami memverifikasi praktik-praktik kami tersedia di halaman web kepatuhan kami.

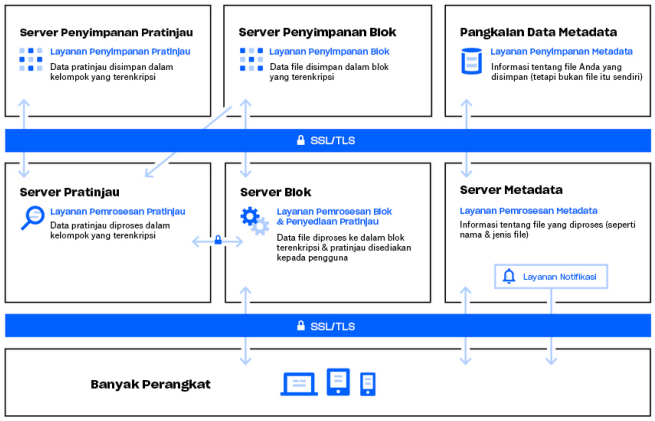
Dropbox

Arsitektur Dropbox: Melindungi Data Pribadi Anda

Di Dropbox, kami percaya bahwa melindungi data pribadi Anda dimulai dengan menjaga keamanan data Anda. Untuk itu, Dropbox dirancang dengan perlindungan berlapis, termasuk transfer data file yang aman, enkripsi, dan kontrol tingkat aplikasi yang didistribusikan di seluruh infrastruktur yang dapat ditingkatkan dan aman.

Infrastruktur Kami: File

Infrastruktur Dropbox untuk file terdiri dari komponen yang digambarkan dalam diagram di bawah ini.



Server Metadata

Informasi dasar tertentu tentang data pengguna, yang disebut metadata, disimpan dalam layanan penyimpanan tersendiri dan berfungsi sebagai indeks untuk data dalam akun pengguna. Metadata meliputi informasi dasar mengenai akun dan pengguna, seperti alamat email, nama, dan nama perangkat. Metadata juga meliputi informasi dasar tentang file, termasuk nama dan jenis file, yang membantu mendukung fitur-fitur seperti riwayat versi, pemulihan, dan sinkronisasi.

Pangkalan Data Metadata

Metadata file disimpan di layanan pangkalan data berbasis MySQL, dan dipecahkan serta digandakan sesuai kebutuhan untuk memenuhi persyaratan kinerja dan ketersediaan yang tinggi.

Server Blok

Pada dasarnya, Dropbox menyediakan mekanisme keamanan unik yang melebihi enkripsi tradisional untuk melindungi data pengguna. Server blok memproses file dari aplikasi Dropbox dengan memecah tiap file menjadi blok, mengenkripsi tiap blok dengan cipher kuat, dan menyinkronkan blok yang hanya dimodifikasi antar revisi. Ketika aplikasi Dropbox mendeteksi sebuah file baru atau perubahan pada file yang telah ada, aplikasi akan memberi tahu Server Blok mengenai perubahan tersebut, dan blok file baru atau yang dimodifikasi akan diproses dan ditransfer ke Server Penyimpanan.

Server Penyimpanan Blok

Konten aktual dari file pengguna disimpan dalam blok terenkripsi dengan Server Penyimpanan Blok. Sebelum transmisi, klien Dropbox membagi file menjadi blok file untuk persiapan penyimpanan. Server Penyimpanan Blok berfungsi sebagai sistem Content-Addressable Storage (CAS), dengan masing-masing blok file terenkripsi diambil berdasarkan nilai hash.

Server Pratinjau

Server Pratinjau bertanggung jawab untuk menghasilkan pratinjau file. Pratinjau adalah penggambaran file pengguna dalam format file yang berbeda yang lebih sesuai untuk tampilan cepat di perangkat pengguna akhir. Server Pratinjau mengambil blok file dari Server Penyimpanan Blok untuk menghasilkan pratinjau. Ketika pratinjau file diminta, Server Pratinjau akan mengambil pratinjau yang tersimpan di cache dari Server Penyimpanan Pratinjau dan mentransfernya ke Server Blok. Pratinjau akhirnya diberikan kepada pengguna oleh Server Blok.

Server Penyimpanan Pratinjau

Pratinjau yang tersimpan di cache disimpan dalam format terenkripsi di Server Penyimpanan Pratinjau.

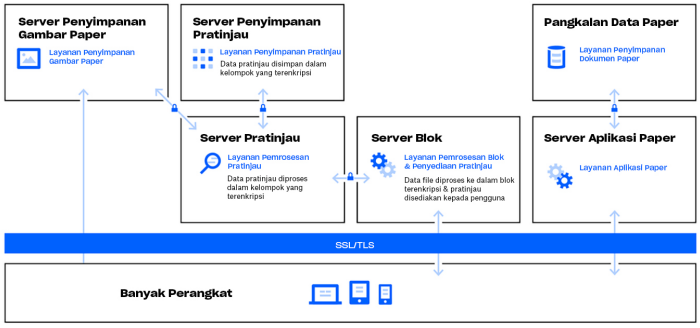
Layanan Pemberitahuan

Layanan terpisah ini disediakan khusus untuk memantau apakah terdapat perubahan pada akun Dropbox atau tidak. Tidak ada file atau metadata yang disimpan di sini atau ditransfer. Setiap klien membuat koneksi long polling ke layanan pemberitahuan dan menunggu. Ketika terjadi perubahan pada suatu file di Dropbox, layanan pemberitahuan mengirimkan tanda perubahan pada klien yang sesuai dengan menutup koneksi long polling . Menutup koneksi menandakan bahwa klien harus terhubung ke Server Metadata dengan aman untuk menyinkronkan setiap perubahan.

Untuk rincian selengkapnya tentang fitur dan kebijakan keamanan Dropbox, bacalah Laporan Resmi Keamanan Dropbox Business atau hubungi sales@dropbox.com

Dropbox

Infrastruktur Kami: Paper
Dropbox Paper (Paper) adalah sebuah fitur dari produk Dropbox. Namun, Paper menggunakan sebagian serangkaian sistem yang sangat berbeda dalam infrastruktur Dropbox. Infrastruktur Paper terdiri dari komponen-komponen yang digambarkan dalam diagram di bawah ini.



Server Aplikasi Paper
Server Aplikasi Paper memproses permintaan pengguna, memberikan kembali hasil dokumen Paper yang diedit ke pengguna, dan melakukan layanan notifikasi. Server Aplikasi Paper menulis hasil edit pengguna ke Pangkalan Data Paper, yang kemudian diletakkan ke penyimpanan persisten. Sesi komunikasi antara Server Aplikasi Paper dan Pangkalan Data Paper dienkripsi dengan cipher yang kuat.

Pangkalan Data Paper
Konten sebenarnya dari dokumen Paper pengguna, serta metadata tertentu tentang dokumen Paper tersebut, dienkripsi pada penyimpanan persisten di Pangkalan Data Paper. Konten tersebut mencakup informasi tentang dokumen Paper (misalnya judul, keanggotaan dan izin bersama, proyek dan folder terkait, serta informasi lainnya), termasuk konten dalam dokumen Paper itu sendiri, termasuk komentar dan tugas. Pangkalan Data Paper dipecah dan direplikasi sesuai kebutuhan untuk memenuhi syarat kinerja dan ketersediaan yang tinggi.

Server Penyimpanan Gambar Paper
Gambar yang diunggah ke dokumen Paper disimpan dan dienkripsi dalam Server Gambar Paper. Transmisi data gambar antara Server Aplikasi Paper dan Server Gambar Paper dilakukan melalui sesi yang dienkripsi.

Server Pratinjau
Server Pratinjau menghasilkan pratinjau untuk gambar yang diunggah ke dokumen Paper serta hyperlink yang dilekatkan dalam dokumen Paper. Untuk gambar yang diunggah ke dokumen Paper, Server Pratinjau mengambil data gambar yang disimpan di Server Penyimpanan Gambar Paper melalui saluran yang dienkripsi. Untuk hyperlink yang dilekatkan dalam dokumen Paper, Server Pratinjau mengambil data gambar dan menghasilkan pratinjau gambar tersebut menggunakan enkripsi yang ditentukan oleh tautan sumber. Pratinjau akhirnya diberikan kepada pengguna oleh Server Blok.

Server Penyimpanan Pratinjau
Paper menggunakan Server Penyimpanan Pratinjau yang dijelaskan dalam diagram infrastruktur Dropbox untuk menyimpan pratinjau gambar yang tersimpan di cache. Pratinjau yang tersimpan di cache disimpan dalam format terenkripsi di Server Penyimpanan Pratinjau.

Dropbox

Kontrol Dropbox: Praktik Internal Kami

Kami melakukan langkah-langkah yang menyeluruh untuk melindungi infrastruktur, jaringan, dan aplikasi kami. Beberapa langkah keamanan yang kami miliki meliputi enkripsi dalam penyimpanan, enkripsi dalam pemindahan, dan penghapusan file secara permanen. Kami juga memberikan pelatihan privasi dan keamanan yang kuat untuk semua karyawan kami, untuk membangun budaya di mana ketepercayaan merupakan prioritas. Rincian beberapa kontrol kami dijelaskan di bawah ini:

Pelatihan

Bagian dari melindungi data pribadi pengguna kami meliputi membangun dan menumbuhkan budaya keamanan dan kesadaran privasi. Karyawan Dropbox harus menyetujui kebijakan keamanan, termasuk kebijakan privasi data pengguna, sebelum memperoleh akses sistem. Hanya karyawan dengan kebutuhan spesifik yang memiliki akses ke sistem tersebut. Karyawan juga mengikuti pelatihan keamanan dan privasi wajib setiap tahun.

Enkripsi saat Transit

Untuk melindungi data file saat perpindahan antara klien Dropbox (saat ini desktop, seluler, API, atau web) dan server front-end Dropbox, koneksi terenkripsi dinegosiasikan untuk memastikan pengiriman yang aman. Demikian pula, koneksi terenkripsi dinegosiasikan untuk melindungi data dokumen Paper saat perpindahan antara klien Paper (saat ini seluler, API, atau web) dan layanan yang disediakan. Koneksi ini dienkripsi menggunakan Secure Sockets Layer (SSL)/Transport Layer Security (TLS) untuk membuat saluran aman yang dilindungi oleh enkripsi Advanced Encryption Standard (AES) 128 bit atau lebih tinggi.

Enkripsi saat diam

File yang diunggah oleh pengguna disimpan di Server Penyimpanan Dropbox sebagai blok file tersendiri. Masing-masing blok dienkripsi menggunakan Advanced Encryption Standard (AES) 256 bit. Hanya blok yang telah dimodifikasi antar revisi yang disinkronkan. Demikian pula, data dokumen Paper yang disimpan di Pangkalan Data Paper juga dienkripsi menggunakan Advanced Encryption Standard (AES) 256 bit saat tidak digunakan.

Penghapusan File dan dokumen Paper secara Permanen

Ketika ada pengguna Dropbox atau administrator untuk Dropbox Business atau tim Dropbox Education menandai file untuk dihapus secara permanen, penandaan ini memicu proses untuk menghapus file secara permanen. Demikian juga, ketika pengguna, atau administrator tim Dropbox Business atau Dropbox Education menandai sebuah dokumen Paper untuk dihapus secara permanen, terdapat sebuah proses serupa untuk menghapus data dokumen Paper dan data gambar secara permanen.

Permintaan Akses Data Pribadi

Untuk akses ke data pribadi selain file dan dokumen Paper yang disimpan di Dropbox, pengguna dapat masuk ke situs web dan membuka halaman akun mereka. Halaman akun akan menunjukkan informasi seperti nama dan alamat email yang terkait dengan akun tersebut. Pengguna juga dapat melihat alamat IP dari sesi yang terhubung, komputer, dan perangkat seluler, serta aplikasi yang terhubung dengan akun mereka dari halaman keamanan dan halaman aplikasi yang terhubung.

Pengguna Dropbox juga memiliki opsi untuk meminta akses atau penghapusan data pribadi mereka yang lain yang mungkin dikumpulkan oleh Dropbox. Informasi selengkapnya mengenai proses ini tersedia di Pusat Bantuan Dropbox.

Tata Kelola Privasi di Dropbox

Tim Program Privasi bertanggung jawab untuk menjalankan Program Privasi Dropbox. Ini menerapkan prakarsa privasi utama kami dan memperjuangkan privasi sebagai dasar dalam siklus hidup data kami. Program Privasi Dropbox didukung oleh berbagai sub-tim Hukum lintas fungsi. Sub-tim ini memberikan keahlian tambahan yang diperlukan untuk menjalankan dan mengawasi tugas sehari-hari Program Privasi.

Tim DPO bekerja secara terpisah dari fungsi privasi lainnya dan bertugas dalam kepatuhan dan pengawasan privasi, yang secara langsung mendukung Petugas Perlindungan Data dalam pelaksanaan tugas mereka. Petugas Perlindungan Data (DPO) adalah perwakilan setempat di UE dan dapat dihubungi melalui privacy@dropbox.com.

Dropbox

Prinsip-Prinsip Permintaan Data Pemerintah

Kami memahami bahwa ketika pengguna mempercayakan data pribadi mereka pada kami, mereka berharap kami menjaga kerahasiaan data tersebut. Seperti kebanyakan layanan online, Dropbox kadang-kadang menerima permintaan dari pemerintah yang meminta informasi mengenai penggunanya.

Prinsip-prinsip di bawah ini menjelaskan bagaimana kami menangani permintaan data dari pemerintah yang kami terima.

Bersikap Transparan

Kami percaya bahwa layanan online harus diizinkan untuk memublikasikan jumlah dan jenis permintaan dari pemerintah yang mereka terima, dan untuk memberitahukan kepada seseorang ketika informasi tentang mereka telah diminta. Jenis transparansi ini memberdayakan pengguna dengan membantu mereka memahami lebih baik situasi dan pola penjangkauan pemerintah yang berlebihan. Kami akan terus memublikasikan informasi terperinci tentang permintaan ini dan mendukung hak untuk menyediakan lebih banyak informasi penting ini.

Menentang permintaan yang terlalu luas

Permintaan data dari pemerintah harus dibatasi pada informasi yang mereka minta dan disesuaikan khusus untuk orang-orang tertentu dan penyelidikan yang sah. Kami akan menolak permintaan yang terlalu luas.

Memberikan layanan tepercaya

Pemerintah seharusnya tidak memasang akses rahasia di layanan online atau menembus infrastruktur untuk mendapatkan data pengguna. Kami akan terus berupaya melindungi sistem kami dan mengubah peraturan sehingga jelas bahwa aktivitas jenis ini ilegal.

Melindungi semua pengguna

Hukum yang memberikan perlindungan berbeda kepada para pengguna berdasarkan pada tempat tinggal dan kewarganegaraan mereka sudah ketinggalan zaman dan tidak mencerminkan sifat global layanan online. Kami akan terus mendukung reformasi terhadap hukum tersebut.

Prinsip-prinsip ini, beserta laporan transparansi tahunan kami, tersedia untuk umum di situs web Dropbox di: https://www.dropbox.com/transparency.

Untuk rincian tambahan mengenai kontrol dan pendekatan kami untuk melindungi data pribadi Anda, bacalah Laporan Resmi Keamanan Dropbox Business.

Orang Lain yang Bekerja untuk dan dengan Dropbox

Dropbox mengelola sebagian besar kegiatan yang terkait dengan penyediaan layanan kami; namun, kami memanfaatkan beberapa pihak ketiga yang tepercaya terkait dengan layanan kami (misalnya, penyedia layanan dukungan pelanggan dan layanan TI). Pihak ketiga tersebut hanya akan mengakses informasi Anda untuk melaksanakan tugas atas nama kami, sesuai dengan Kebijakan Privasi, dan kami akan tetap bertanggung jawab atas penanganan informasi Anda sesuai dengan instruksi kami.

Setiap pihak ketiga menjalani proses pemeriksaan yang ketat, termasuk tinjauan keamanan dan tinjauan kontrak berkala, untuk mengevaluasi kemampuan mereka memenuhi komitmen perlindungan data kami.

Transfer Data Internasional

Dropbox mengandalkan berbagai mekanisme legal untuk transfer data pribadi secara internasional dari UE ke Amerika Serikat. Kami tersertifikasi sesuai Undang-Undang Privasi UE-AS dan Swiss-AS Program Shield berkaitan dengan pengumpulan, penggunaan, dan penyimpanan data pribadi dan transfer dari UE dan Swiss ke Amerika Serikat. Selain Privacy Shield, Dropbox juga memberikan jaminan kontraktual yang kuat mengenai privasi layanannya dan telah menerapkan Klausul Kontrak Model UE untuk mencakup transfer data internasional.

Dropbox

GDPR: Peraturan Perlindungan Data Umum

Peraturan Perlindungan Data Umum, atau GDPR, adalah sebuah peraturan UE yang menetapkan kerangka hukum untuk melindungi data pribadi milik subjek data UE.

GDPR adalah sebuah undang-undang perlindungan data Eropa yang paling penting sejak Petunjuk Perlindungan Data UE tahun 1995, dan banyak perusahaan—termasuk Dropbox—yang menjalankan bisnis di Eropa telah banyak mencurahkan perhatian demi kepatuhan terhadap GDPR.

GDPR menyelaraskan hukum perlindungan data di seluruh Eropa, dan menyatukannya agar sesuai dengan perubahan teknologi yang cepat yang telah terjadi dalam dua dekade terakhir.

Undang-undang ini didasarkan pada kerangka hukum masa lalu di UE, termasuk Petunjuk Perlindungan Data UE, dan memperkenalkan kewajiban dan tanggung jawab baru untuk organisasi yang menangani data pribadi, serta hak-hak baru untuk setiap orang sehubungan dengan data pribadi mereka. data pribadi mereka. Organisasi yang didirikan di UE, serta organisasi yang memproses data pribadi subjek data UE, wajib mematuhi GDPR.

Perjalanan Dropbox menuju Kepatuhan Terhadap GDPR

Dropbox berkomitmen untuk mematuhi GDPR. Penghormatan terhadap privasi dan keamanan disertakan dalam bisnis kami sejak awal, dan seiring dengan perkembangan kami, fokus kami pada penanganan dan perlindungan data yang dipercayakan oleh pengguna kami kepada kami tetap menjadi prioritas. Dropbox memiliki rekam jejak yang unggul dalam kurva kepatuhan —seperti yang dijelaskan di atas, kami adalah salah satu penyedia layanan awan pertama yang memperoleh sertifikasi ISO 27018 untuk pengguna bisnis kami. Dengan fondasi yang kuat ini, Dropbox memandang kepatuhan terhadap GDPR sebagai evolusi dari praktik dan kontrol kami yang telah ada, dan mewakili serangkaian inisiatif yang berkelanjutan dan terus berkembang untuk memastikan bahwa data pribadi pengguna kami selalu dilindungi.

Perjalanan Dropbox menuju kepatuhan terhadap GDPR dimulai sejak peraturan tersebut diterapkan pada tahun 2016. Langkah pertama kami adalah membentuk tim lintas fungsi spesialis perlindungan data yang terdiri dari penasihat hukum, profesional di bidang keamanan dan kepatuhan, serta teknisi produk dan infrastruktur. Tim kami kemudian menyelesaikan penilaian menyeluruh atas praktik keamanan dan perlindungan data kami saat ini sehubungan dengan persyaratan GDPR.

Langkah kami selanjutnya adalah melakukan evaluasi terhadap aktivitas pemrosesan data pribadi kami dan melacak siklus hidup data pribadi dalam sistem kami. Langkah-langkah ini kadang-kadang disebut melaksanakan Pemetaan Data dan menyelesaikan Penilaian Dampak Perlindungan Data. Pemetaan Data dan menyelesaikan Penilaian Dampak Perlindungan Data.

Sejak itu, kami terus membangun proses dan prosedur internal yang telah ada untuk memastikan bahwa kami memenuhi prinsip-prinsip akuntabilitas sesuai dengan persyaratan GDPR. Ini adalah hal yang penting karena GDPR lebih berfokus untuk mendokumentasikan keputusan dan praktik yang memengaruhi data pribadi.

Dropbox

Memberdayakan Pengguna Kami dalam Perjalanan GDPR mereka

Dropbox menyediakan fitur kontrol dan visibilitas yang dapat membantu Anda mengelola kewajiban perlindungan data Anda, termasuk kewajiban kepatuhan terhadap GDPR, dengan lebih mudah. Tentu saja, kepatuhan terhadap GDPR di seluruh organisasi Anda tidak dimulai atau diakhiri dengan hubungan dengan pemasok Anda, misalnya Dropbox. Meskipun fitur kami dapat membantu Anda mengelola kewajiban Anda, fitur tersebut tidak dapat memastikan kepatuhan dengan sendirinya. Kepatuhan terhadap GDPR memerlukan pemikiran yang lebih luas tentang bagaimana data berpindah dan dilindungi di organisasi Anda. Setiap organisasi harus melakukan langkahnya sendiri untuk mencapai kepatuhan, dengan pemasok sebagai mitra penting dalam perjalanan itu.

Minimalisasi Data
Salah satu unsur penting dari persyaratan Privasi Sebagai Dasar menurut GDPR adalah bahwa organisasi harus merancang layanan mereka agar meminimalkan data. Ini berarti menyediakan visibilitas dan kontrol data yang baik dalam organisasi Anda untuk membantu Anda mengelolanya. Dasbor admin Dropbox Business adalah alat yang berguna untuk membantu dalam hal ini, karena alat ini memungkinkan Anda untuk memantau aktivitas tim, melihat perangkat yang terhubung, dan melakukan audit terhadap aktivitas berbagi. Kami berupaya menanamkan prinsip Privasi Sebagai Dasar ke dalam produk dan fitur baru.

Perlindungan dan Pemulihan Data
Perlindungan perangkat yang hilang, riwayat versi, dan pemulihan file dapat membantu melindungi terhadap kehilangan, kerusakan, atau penghancuran data pribadi yang tidak disengaja, dan dapat membantu dengan kemampuan untuk memulihkan ketersediaan dan akses ke data pribadi secara tepat waktu ketika terjadi insiden. Otentikasi dua faktor adalah tindakan penting lainnya yang kami anjurkan untuk membantu melindungi data Anda.

Pencatatan Arsip
GDPR juga meningkatkan kewajiban organisasi untuk menyimpan catatan terperinci mengenai aktivitas pemrosesan mereka. Catatan audit dan catatan aktivitas kami dapat membantu Anda lebih memahami aktivitas pemrosesan Anda untuk mendukung pencatatan arsip.

Administrasi Akses

Pada dasbor admin Dropbox Business, Anda dapat dengan mudah mengelola akses anggota tim ke file, folder, dan dokumen Paper. Untuk tautan file bersama, fitur izin tautan kami memungkinkan Anda untuk melindungi tautan bersama menggunakan kata sandi, menetapkan tanggal kedaluwarsa untuk memberikan akses sementara, dan membatasi akses ke file dalam organisasi Anda. Jika tanggung jawab berubah di antara pengguna, alat transfer akun kami memungkinkan Anda untuk dengan mudah mentransfer file dan kepemilikan dokumen Paper dari satu pengguna ke pengguna lainnya.

Administrator juga memiliki kemampuan untuk menonaktifkan akses pengguna ke akun mereka sekaligus menjaga data mereka dan berbagi hubungan untuk menjaga keamanan informasi organisasi Anda. Terakhir, fitur penghapusan jarak jauh memungkinkan Anda menghapus file dan dokumen kertas dari perangkat yang hilang atau dicuri.

Infrastruktur UE
Meskipun GDPR tidak mewajibkan data pribadi disimpan di UE, Dropbox menawarkan penyimpanan file (blok) di UE kepada pelanggan Dropbox Business dan Dropbox Education yang memenuhi syarat. Penyimpanan file di UE disediakan menggunakan infrastruktur Amazon Web Service (AWS). Untuk mempelajari selengkapnya tentang infrastruktur UE kami, hubungi tim penjualan kami.

Dropbox

Bekerja Bersama untuk Melindungi Data Pribadi Anda

Dropbox bekerja sama dengan para penggunanya untuk melindungi data pribadi mereka. Kami menempuh langkah-langkah komprehensif untuk melindungi infrastruktur, jaringan, dan aplikasi kami, melatih karyawan dalam praktik keamanan dan privasi, membangun budaya di mana ketepercayaan menjadi prioritas tertinggi, dan menjalankan pengujian dan audit ketat oleh pihak ketiga terhadap sistem dan praktik-praktik kami.

Namun, pengguna juga berperan penting dalam melindungi data pribadi mereka. Dropbox memungkinkan Anda untuk mengonfigurasi, menggunakan, dan memantau akun Anda untuk memenuhi kebutuhan privasi, keamanan, dan kepatuhan dalam organisasi Anda. Panduan tanggung jawab bersama kami dapat membantu Anda lebih memahami apa yang kami lakukan untuk menjaga keamanan akun Anda dan apa yang dapat Anda lakukan untuk menjaga visibilitas dan kontrol terhadap data pribadi Anda.

Ringkasan

Setiap hari, jutaan pengguna mempercayai Dropbox. Agar layak mendapatkan kepercayaan itu, kami membangun dan akan terus menumbuhkan Dropbox dengan penekanan pada keamanan dan privasi. Komitmen kami untuk melindungi data pribadi pengguna adalah inti dari setiap keputusan yang kami buat. Untuk informasi lebih lanjut, silakan kirim email ke privacy@dropbox.com. Untuk informasi selengkapnya tentang GDPR, Anda juga dapat mengunjungi pusat pedoman GDPR kami.