Dropbox

Конфиденциальность и защита данных

Введение

Персональные данные играют огромную роль в обществе и экономике. Все чаще люди хотят контролировать и четко понимать, как их персональные данные используются и защищаются организациями, с которыми они взаимодействуют.

В Dropbox доверие — это основа наших взаимоотношений с миллионами пользователей и компаний по всему миру. Мы ценим доверие наших пользователей и ответственно относимся к защите их персональных данных.

Наши обязательства

Наша основная цель — защитить ваши персональные данные. В Условиях обслуживания Dropbox обозначены обязанности, которые вы принимаете на себя, пользуясь нашими услугами. В нашей Политике конфиденциальности описаны наши обязательства по обеспечению конфиденциальности пользователей и объясняется, как мы собираем, используем и обрабатываем ваши персональные данные, когда вы пользуетесь нашими услугами. Если вы проживаете в Северной Америке (США, Канаде и Мексике), компания Dropbox, Inc. выступает в качестве вашего поставщика услуг.

Для всех остальных пользователей Dropbox International Unlimited Company выступает в качестве контролера ваших персональных данных.

Если вы являетесь пользователем Dropbox Business или Dropbox Education, ваша организация выступает в качестве контролера любых персональных данных, предоставляемых Dropbox в связи с использованием вами Dropbox Business или Dropbox Education. Контроллер данных определяет цели и средства обработки персональных данных. Dropbox выступает в качестве обработчика данных, обрабатывая данные от имени вашей организации, когда вы используете Dropbox Business или Dropbox Education, а наше Соглашение по использованию аккаунта Dropbox Business включает обязательства, связанные с обработкой данных и международной передачей данных.

Наше достижение — соответствие стандартам

Соответствие стандартам — это эффективный способ проверить надежность предоставляемых услуг. Мы предлагаем и всегда готовы предоставить независимую проверку того, что наши методы обеспечения безопасности и конфиденциальности соответствуют наиболее широко принятым стандартам и нормам, например ISO 27001, ISO 27017, ISO 27018, HIPPA/HITECH, стандартам Германии BSI C5, а также SOC 1, 2 и 3.

Кроме того, мы были одними из первых поставщиков облачных услуг, которые прошли сертификацию по международно признанному стандарту для передовых практик в области конфиденциальности и защиты данных в облаке ISO 27018. Наши независимые сторонние аудиторы проверяют наши средства управления и предоставляют свои отчеты и заключения. Если это возможно, мы можем поделиться этой информацией с вами.

Обращаем ваше внимание, что хотя сфера охвата наших сертификатов и аудиторских отчетов обычно относится к Dropbox Business и Dropbox Education. Большинство наших средств управления также применимы для пользователей Dropbox Basic, Plus и Professional. Дополнительную информацию о стандартах, которые мы соблюдаем, и о том, как мы проверяем наши практики, можно найти на нашей веб-странице соответствия.

Подробную информацию о функциях и политиках безопасности Dropbox смотрите в технической документации по безопасности Dropbox Business или свяжитесь с нами по электронной почте sales@dropbox.com

Архитектура Dropbox: защита ваших персональных данных

В Dropbox мы считаем, что защита ваших персональных данных начинается с обеспечения безопасности ваших данных. Поэтому в Dropbox разработано несколько уровней защиты: в частности, мы используем безопасную передачу файловых данных, шифрование, а также элементы управления на уровне приложений, распределенные по масштабируемой, безопасной инфраструктуре.

Наша инфраструктура: файлы

Инфраструктура Dropbox для файлов состоит из компонентов, изображенных на диаграмме ниже.

Серверы метаданных

Некоторая основная информация о данных пользователей называется метаданными, которые хранятся в отдельном хранилище и являются своего рода каталогом данных в аккаунтах пользователей. Метаданные включают в себя базовые сведения об аккаунте и пользователе, например адрес электронной почты, имя и названия устройств. Метаданные также включают в себя базовые сведения о файлах, в том числе названия и типы файлов, которые помогают поддерживать такие функции, как журнал версий, восстановление и синхронизация.

Базы метаданных

Метаданные файлов хранятся в службе базы данных на основе MySQL, и их разделение и репликация осуществляются по мере необходимости с целью обеспечения соответствия требованиям в отношении эффективности и высокой доступности.

Серверы блочной обработки

Благодаря своему дизайну Dropbox предоставляет уникальный механизм безопасности, который выходит за рамки традиционного шифрования для защиты пользовательских данных. Серверы блочной обработки обрабатывают файлы в программах и приложениях Dropbox: файлы делятся на отдельные блоки, каждый из которых шифруется с помощью криптостойкого шифра; синхронизации подлежат только те блоки, которые были изменены после создания очередной версии файла. Когда приложение Dropbox обнаруживает новый файл или изменения в существующем файле, оно уведомляет серверы блочной обработки об этом изменении, и новые или измененные блоки файлов обрабатываются и пересылаются на сервер хранения данных.

Серверы блочного хранения

Серверы блочного хранения позволяют хранить содержимое файлов пользователей в виде зашифрованных блоков. Перед пересылкой программа Dropbox разбивает файлы на блоки файлов при подготовке к хранению. Серверы блочного хранения действуют как система хранения данных с адресацией по содержимому (Content-Addressable Storage — CAS), причем каждый индивидуальный зашифрованный блок файлов вызывается на основе его хеш-значения.

Серверы предварительного просмотра

Серверы предварительного просмотра отвечают за создание предпросмотра файлов. Предварительный просмотр — это рендеринг файла пользователя в другой формат, который больше подходит для быстрого отображения на устройстве конечного пользователя. Серверы предварительного просмотра вызывают блоки файлов с серверов блочного хранения для генерации изображения предварительного просмотра. При запросе предварительного просмотра файла серверы предварительного просмотра вызывают кэшированное изображение предварительного просмотра с серверов хранения изображений предварительного просмотра и передают его на серверы блочной обработки. В конечном итоге предварительный просмотр для пользователей обеспечивают серверы блочной обработки.

Серверы хранения изображений предварительного просмотра

Кэшированные изображения предварительного просмотра хранятся в зашифрованном формате на серверах хранения изображений предварительного просмотра.

Уведомления

Эта отдельная служба предназначена для отслеживания изменений в аккаунтах Dropbox. Данная служба не хранит и не пересылает никаких файлов или метаданных. Каждая программа Dropbox подключается к службе уведомлений методом длинных опросов и переходит в режим ожидания. Когда происходит изменение какого-либо файла в Dropbox, служба уведомлений сообщает об изменении соответствующей(-им) программе(-ам) Dropbox, закрывая соединение методом длинных опросов. Закрытие соединения сигнализирует о том, что программа Dropbox должна безопасно подключиться к серверам метаданных для синхронизации любых изменений.

Подробную информацию о функциях и политиках безопасности Dropbox смотрите в технической документации по безопасности Dropbox Business или свяжитесь с нами по электронной почте sales@dropbox.com

Наша инфраструктура: Paper

Dropbox Paper (Paper) — это функция Dropbox. Тем не менее, Paper использует в основном отдельный комплекс систем в инфраструктурной среде Dropbox. Инфраструктура Paper состоит из компонентов, изображенных на диаграмме ниже.

Серверы приложения Paper

Серверы приложения Paper обрабатывают запросы пользователей, передают документы Paper со внесенными изменениями обратно пользователю и осуществляют работу, связанную с уведомлениями. Серверы приложения Paper записывают внесенные пользователями изменения в базы данных Paper, где они помещаются на постоянное хранение. Сеансы связи между серверами приложения Paper и базами данных Paper шифруются при помощи криптостойкого шифра.

Базы данных Paper

Содержимое документов Paper, принадлежащих пользователям, а также определенные метаданные, относящиеся к этим документам, хранятся в зашифрованном виде в базах данных Paper. Сюда относится информация о документе Paper (например, его название, список участников, имеющих к нему доступ, права доступа, проекты или папки, с которыми связан этот документ, и другие данные), а также содержимое самого документа Paper, включая комментарии и задания. Разделение и репликация баз данных Paper осуществляются по мере необходимости с целью обеспечения соответствия требованиям в отношении эффективности и высокой доступности.

Серверы хранения изображений Paper

Загружаемые в документы Paper изображения хранятся в зашифрованном виде на серверах изображений Paper. Передача данных, содержащих изображения, между серверами приложения Paper и серверами изображений Paper осуществляется во время зашифрованных сеансов.

Серверы предварительного просмотра

Серверы предварительного просмотра создают изображения предварительного просмотра как для изображений, загруженных в документы Paper, так и для гиперссылок, встроенных в документы Paper. В отношении изображений, загруженных в документы Paper, серверы предварительного просмотра осуществляют доступ к данным изображений, хранящимся на серверах хранения изображений Paper, через зашифрованный канал. Для гиперссылок, встроенных в документы Paper, серверы предварительного просмотра осуществляют доступ к данным изображений и выполняют рендеринг изображения предварительного просмотра с использованием шифрования, как указано в ссылке на источник. В конечном итоге предварительный просмотр для пользователей обеспечивают серверы блочной обработки.

Серверы хранения изображений предварительного просмотра

Paper использует те же серверы хранения изображений предварительного просмотра, которые описаны на диаграмме инфраструктуры Dropbox, для хранения кэшированных изображений предварительного просмотра. Блоки кэшированных изображений предварительного просмотра хранятся в зашифрованном формате на серверах хранения изображений предварительного просмотра.

Dropbox

Элементы управления Dropbox: наши внутренние практики

Мы применяем комплексные меры для защиты нашей инфраструктуры, сети и приложений. Некоторые меры безопасности, которые мы применяем, включают шифрование данных при хранении и при передаче и постоянное удаление файлов. Мы также предлагаем всем нашим сотрудникам пройти тренинги в области конфиденциальности и безопасности, чтобы построить культуру, в которой доверие является основным приоритетом. Ниже представлена подробная информация о некоторых наших элементах управления:

Обучение

Частью защиты персональных данных наших пользователей является создание и развитие культуры безопасности и конфиденциальности. Сотрудники Dropbox обязаны согласиться с политиками безопасности, включая политику конфиденциальности пользовательских данных, прежде чем им будет предоставлен доступ к системам. Доступ к таким системам имеют только те сотрудники, которым он необходим.
Также сотрудники ежегодно принимают участие в обязательных тренингах по безопасности и конфиденциальности.

Шифрование при передаче

Для защиты данных файлов, передаваемых между программой Dropbox (в настоящий момент программой для компьютера, мобильным приложением, API или веб-приложением) и интерфейсными серверами Dropbox, устанавливается зашифрованное соединение, обеспечивающее безопасную доставку. Аналогичное зашифрованное соединение устанавливается для защиты данных документов Paper при их передаче между программой Paper (в настоящий момент мобильным приложением, API или веб-приложением) и размещенной службой. Эти соединения шифруются с использованием протокола Secure Sockets Layer (SSL)/Transport Layer Security (TLS) для создания безопасного туннеля, защищенного 128-битным или более высоким шифрованием по стандарту Advanced Encryption Standard (AES).

Шифрование в Dropbox

Файлы, загруженные пользователями, хранятся на серверах хранения Dropbox в виде отдельных блоков файлов. Каждый блок зашифрован с использованием 256-разрядного алгоритма шифрования AES. Только измененные между редакциями блоки подлежат синхронизации. Аналогично данные документов Paper, которые хранятся в базах данных Paper, также шифруются при хранении с использованием 256-разрядного алгоритма шифрования AES.

Постоянное удаление файлов и документов Paper

Если пользователь Dropbox или администратор рабочей группы Dropbox Business или Dropbox Education помечает файл для окончательного удаления, он запускает процесс окончательного удаления файла. Аналогичным образом, если пользователь или администратор рабочей группы Dropbox Business или Dropbox Education помечает документ Paper для окончательного удаления, происходит аналогичный процесс окончательного удаления данных документов и изображений Paper.

Запросы на доступ к персональным данным

Для доступа к персональным данным, помимо файлов и документов Paper, которые хранятся в Dropbox, пользователи могут войти на веб-сайт и перейти на страницу своего аккаунта. На странице аккаунта будет отображаться такая информация, как имя и адрес электронной почты, связанный с аккаунтом. Пользователи также могут просматривать IP-адреса подключенных сеансов, компьютеров и мобильных устройств, а также приложения, подключенные к их аккаунтам, со страницы безопасности и страницы подключенных приложений.

Пользователи Dropbox также имеют возможность запросить доступ к другим персональным данным, которые Dropbox может собрать о них, либо выполнить запрос на их удаление.
Более подробную информацию об этом процессе можно найти в Справочном центре Dropbox.

Управление конфиденциальностью в Dropbox

Рабочая группа Программы конфиденциальности отвечает за работу Программы конфиденциальности Dropbox. Она реализует наши ключевые инициативы в области конфиденциальности и защищает встроенный алгоритм конфиденциальности в жизненном цикле данных. Программа конфиденциальности Dropbox поддерживается несколькими многофункциональными юридическими подгруппами. Эти подгруппы предоставляют дополнительную экспертизу, необходимую для работы и контроля за повседневными задачами Программы конфиденциальности.

Рабочая группа СЗД работает отдельно от других служб обеспечения конфиденциальности и выполняет функции соблюдения конфиденциальности и функции надзора, непосредственно поддерживая специалиста по защите данных в выполнении своих обязанностей. Специалист по защите данных (СЗД) является местным представителем в ЕС, с которым можно связаться по электронной почте privacy@dropbox.com.

Подробную информацию о функциях и политиках безопасности Dropbox смотрите в технической документации по безопасности Dropbox Business или свяжитесь с нами по электронной почте sales@dropbox.com

Принципы обработки государственного запроса о предоставлении данных

Мы понимаем, что если пользователи доверяют нам свои персональные данные, они ожидают, что мы будем хранить эти данные в тайне. Как и большинство онлайн-сервисов, Dropbox иногда получает от государственных органов запросы на раскрытие информации о некоторых пользователях.

Приведенные ниже принципы описывают, как мы обрабатываем получаемые нами государственные запросы на информацию.

За прозрачность

Мы считаем, что онлайн-сервисам нужно разрешать публиковать данные о том, сколько государственных запросов (и какие именно) они получают, а также уведомлять отдельных пользователей, когда запрашивается информация о них. Такого рода прозрачность помогает пользователям лучше разбираться в разных судебных инстанциях и понимать, не превышает ли правительство свои полномочия. Мы планируем и далее публиковать подробные данные о такого рода запросах и защищать свое право на публикацию большего количества сведений.

Борьба с чрезмерно широкими запросами

Запросы, поступающие от государственных органов, должны касаться только определенной информации и конкретных лиц или уголовных дел. Мы будем выступать против слишком общих и широких запросов.

Против недобросовестности

Государственные органы не должны устанавливать в онлайн-сервисах бэкдор-программы или иным образом нарушать их инфраструктуру с целью получения данных о пользователях. Мы планируем и дальше защищать наши системы и бороться с законами, которые допускают такие действия со стороны государства.

Защита всех пользователей

Законы, которые защищают только людей, живущих в определенной стране или имеющих определенное гражданство, являются устаревшими и не соответствуют международному положению онлайн-сервисов. Мы планируем и далее выступать за реформу этих законов.

Эти принципы вместе с нашим ежегодным отчетом о доступе к информации публикуются на веб-сайте Dropbox: https://www. dropbox.com/transparency.

Подробную информацию о наших средствах управления, а также о нашем подходе к защите ваших персональных данных смотрите в технической документации по безопасности Dropbox Business.

Другие лица, работающие на и с Dropbox

Dropbox управляет большинством действий, связанных с предоставлением наших услуг; тем не менее, мы прибегаем к помощи доверенных сторонних лиц при предоставлении наших услуг (например, к поставщикам услуг службы поддержки и ИТ-услуг). Эти сторонние лица получают доступ к вашей информации только для выполнения задач от нашего имени в соответствии с нашей Политикой конфиденциальности. Мы по-прежнему будем нести ответственность за то, как они обращаются с вашей информацией в соответствии с нашими инструкциями.

Все сторонние лица проходят строгий процесс проверки, включая проверки безопасности и регулярные проверки контрактов, необходимые для оценки их способности выполнять наши обязательства по защите данных.

Международная передача данных

Dropbox использует различные правовые механизмы для международной передачи персональных данных из ЕС в США. У нас имеется сертификат программы Privacy Shield по защите конфиденциальности, соглашения между ЕС и США и между Швейцарией и США в отношении сбора, использования и хранения персональных данных, передаваемых из Европейского Союза и Швейцарии в Соединенные Штаты. В дополнение к программе Privacy Shield компания Dropbox также предоставляет надежные договорные гарантии в отношении конфиденциальности своих услуг и внедрила типовые контрактные положения ЕС для регулирования своих международных передач данных.

Dropbox

GDPR: Генеральный регламент о защите данных

Генеральный регламент о защите данных или GDPR — это регламент ЕС, который закладывает правовую основу для защиты персональных данных лиц, проживающих в ЕС.

GDPR является наиболее важным элементом европейского законодательства о защите данных с момента принятия Директивы ЕС о защите данных 1995 года, и многие компании, включая Dropbox, которые ведут бизнес в Европе, вложили значительные средства для соблюдения требований GDPR.

GDPR гармонизирует законы о защите данных в Европе и приводит их в соответствие с быстрыми технологическими изменениями, произошедшими за последние два десятилетия.

Он основан на прошлых правовых принципах ЕС, включая Директиву ЕС о защите данных, и вводит новые обязательства и ответственность для организаций, которые обрабатывают персональные данные, а также новые права для физических лиц в отношении их персональных данных. Организации, созданные в ЕС, а также организации, которые обрабатывают персональные данные лиц, проживающих в ЕС, обязаны соблюдать GDPR.

Процесс обеспечения соответствия требованиям GDPR в Dropbox

Dropbox стремится к соблюдению GDPR. Уважение конфиденциальности и надлежащая защита данных были интегрированы в наши принципы ведения бизнеса с самого начала. В процессе нашего роста соответствующая обработка и защита информации, которую наши пользователи доверяют нам, всегда оставались приоритетным направлением нашей деятельности. Опыт Dropbox показывает наше умение быть впереди других в вопросах, касающихся обеспечения соответствия. Как было описано выше, мы стали одними из первых поставщиков облачных услуг, которые прошли сертификацию на соответствие требованиям ISO 27018 для наших бизнес-пользователей. Учитывая прочность заложенных основ, Dropbox рассматривает соблюдение GDPR как эволюцию наших существующих практик и средств управления и предлагает постоянно совершенствуемый комплекс инициатив, обеспечивающих защиту персональных данных наших пользователей.

Для Dropbox переход к обеспечению соблюдения GDPR начался сразу после принятия регламента в 2016 году. Нашим первым шагом было формирование многофункциональной команды специалистов по защите данных, состоящей из юристов, специалистов по обеспечению безопасности и соответствию требованиям, инженеров по продуктам и инфраструктуре. Затем наша команда выполнила полную оценку нашей нынешней практики обеспечения безопасности и защиты данных в соответствии с требованиями GDPR.

Нашим следующим шагом была оценка нашей деятельности по обработке персональных данных и отслеживание жизненного цикла персональных данных через наши системы. Иногда это еще называют структурирование данных и оценка последствий, связанных с защитой данных.

С тех пор мы продолжали опираться на наши существующие внутренние процессы и процедуры, чтобы обеспечить соблюдение принципов подотчетности в соответствии с требованиями GDPR. Это важно, поскольку GDPR уделяет повышенное внимание документированию решений и методов работы с персональными данными.

Dropbox

Расширение прав и возможностей наших пользователей в процессе обеспечения соответствия требованиям GDPR

Dropbox предоставляет функции контроля и прозрачности, которые помогут вам легче управлять своими обязательствами по защите данных, включая обязательства по соблюдению GDPR. Конечно, соблюдение GDPR в вашей организации не начинается и не заканчивается отношениями с вашими поставщиками, например с Dropbox. Несмотря на то, что наши функции могут помочь вам в управлении своими обязательствами, они не могут гарантировать их соблюдение. Соответствие требованиям GDPR требует более глубокого понимания того, как перемещаются данные и как они защищены в вашей организации. Каждая организация должна предпринять свои собственные шаги для достижения соответствия требованиям вместе с поставщиками, которые выступают в качестве важных партнеров на этом пути.

Минимизация данных

Важной составляющей встроенного алгоритма конфиденциальности GDPR является то, что организации должны оказывать свои услуги таким образом, чтобы работать с минимальным объемом данных. Это означает наличие высокой прозрачности и эффективного контроля над данными в вашей организации, которые помогают вам управлять ими. Панель управления Dropbox Business — полезный инструмент, помогающий справиться с этим, поскольку он позволяет вам контролировать действия рабочей группы, просматривать подключенные устройства и проверять действия по предоставлению общего доступа. Мы работаем над тем, чтобы внедрить принципы встроенного алгоритма конфиденциальности в новые продукты и функции.

Защита и восстановление данных

Защита данных на потерянных устройствах, журнал версий и восстановление файлов могут помочь защитить от случайной потери, повреждения или уничтожения персональных данных, а также могут помочь своевременно восстановить доступность и доступ к персональным данным в случае инцидента. Двухфакторная проверка подлинности — это еще одна важная мера для защиты ваших данных, использование которой мы поощряем.

Ведение документации

GDPR также расширяет обязательства организаций в отношении детального документирования своей деятельности по обработке данных. Наши журналы аудита и журналы событий могут помочь вам лучше понять ваши действия по обработке данных и содействовать работе по ведению документации.

Администрирование доступа

На панели управления Dropbox Business вы легко можете управлять доступом участников рабочей группы к файлам, папкам и документам Paper. Для ссылок на файлы, к которым был предоставлен общий доступ, наша функция разрешений для ссылок позволит защитить паролем общие ссылки, установить срок действия для предоставления временного доступа и ограничить доступ для тех, кто находится в вашей организации. В случае, если обязанности пользователей меняются, наш инструмент переноса данных из аккаунта в аккаунт позволит вам легко пересылать файлы и передавать права владения документом Paper от одного пользователя другому.

Администраторы также могут отключить доступ пользователей к их аккаунтам, сохраняя при этом их данные и предоставляя общий доступ к файлам, чтобы обеспечить безопасность информации вашей организации. И наконец, функция удаленного стирания данных позволяет удалять файлы и документы Paper с потерянных или украденных устройств.

Инфраструктура ЕС

Хотя GDPR не требует размещения персональных данных на территории ЕС, Dropbox предлагает квалифицированным клиентам Dropbox Business и Dropbox Education возможность хранения файлов (блоков) в ЕС. Хранение файлов в ЕС обеспечивается инфраструктурой Amazon Web Services (AWS). Чтобы узнать больше о нашей инфраструктуре в ЕС, свяжитесь с нашим отделомпродаж.

Подробную информацию о функциях и политиках безопасности Dropbox смотрите в технической документации по безопасности Dropbox Business или свяжитесь с нами по электронной почте sales@dropbox.com

Dropbox

Совместная работа для защиты ваших персональных данных

Dropbox работает со своими пользователями для защиты их персональных данных. Мы предпринимаем комплексные меры для защиты нашей инфраструктуры, сети и приложений, обучаем сотрудников методам обеспечения безопасности и конфиденциальности, создаем культуру, в которой доверие является наивысшим приоритетом, и подвергаем наши системы и методы строгому стороннему тестированию и аудиту.

Тем не менее, пользователи также играют ключевую роль в защите своих персональных данных. Dropbox позволяет вам настраивать, использовать и контролировать свой аккаунт таким образом, который соответствует потребностям вашей организации в области конфиденциальности, безопасности и обеспечения соблюдения требований. Наше Руководство по общей ответственности может помочь вам лучше понять, что мы делаем для обеспечения безопасности вашего аккаунта и что вы можете сделать для обеспечения прозрачности и контроля ваших персональных данных.

Краткое описание

Каждый день миллионы пользователей доверяют Dropbox. Чтобы быть достойными этого доверия, мы создали и будем развивать Dropbox, уделяя особое внимание безопасности и конфиденциальности. Наша приверженность защите персональных данных наших пользователей лежит в основе каждого решения, которое мы принимаем. Для получения дополнительной информации напишите на адрес электронной почты privacy@dropbox.com. Для получения дополнительной информации о GDPR вы также можете посетить наш Центр методических рекомендаций по GDPR.