Защита данных и кибербезопасность после вступления в силу общего регламента ЕС по защите данных (GDPR)

#KingstonIsWithYou

Защита данных и кибербезопасность после вступления в силу общего регламента ЕС по защите данных (GDPR)

Предисловие

Великое множество компаний и организаций вели напряженную работу, в том числе с кадрами, готовясь к внедрению GDPR. Возможно, среди них было и ваше предприятие. Однако изменчивый характер киберпреступлений означает, что вы не можете позволить себе остановиться и перевести дыхание. Обеспечение соответствия правилам GDPR не похоже на заполнение анкеты. Скорее, это структура, позволяющая оценивать ваши текущие усилия, направленные на защиту данных и кибербезопасность. Тут нет места беспечности.

В этой небольшой электронной книге мы обобщим знания ряда самых опытных обозревателей из Великобритании в сфере кибербезопасности и рассмотрим, как изменилась защита данных после внедрения GDPR. Мы также расскажем, как компании информируют своих сотрудников о необходимости соблюдения нормативных требований, и обсудим, как ИТ-отделы и поставщики технологий могут улучшить защиту ИТ-инфраструктуры и предоставлять конечным пользователям информацию о новых проблемах безопасности.

Защита данных и кибербезопасность после вступления в силу общего регламента ЕС по защите данных (GDPR)

Авторы

Эта небольшая электронная книга составлена пятью экспертами в области защиты данных и кибербезопасности.

Rob Allen
@Rob_A_kingston

Роб является директором по маркетингу и техническому обслуживанию в Kingston Technology и работает в компании с 1996 года. Роб курирует связи с общественностью, социальные сети, дистрибуторский маркетинг в подразделениях Digital Marketing Media и Creative для всех брендов и продуктов Kingston.

Tara Taubman-Bassirian
@clarinette02

У Тары есть множество титулов: юрист, адвокат, посредник, исследователь, консультант, докладчик, писатель. Обладая обширным опытом в таких областях, как конфиденциальность, интеллектуальная собственность и защита данных, она получила известность в различных регионах мира, особенно в Великобритании, Франции и США.

Rafael Bloom
@rafibloom73

Рафаэль — директор Salvatore ltd. В этой должности он помогает компаниям управлять стратегическими, коммерческими и процедурными проблемами и возможностями, образовавшимися в результате технологических и нормативных изменений.

Miriam Brown
@Kingston_MBrown

Мириам — менеджер по стратегическому маркетингу в корпоративном секторе в Kingston Technology. Она работает в компании с 1996 года. Мириам отвечает за маркетинговую стратегию, материалы и кампании для всех продуктов Kingston для корпоративных клиентов.

Sally Eaves
@sallyeaves

Профессора Салли Ивс называют «светочем движения за этичность технологий». Она обладает богатым опытом работы в качестве главного исполнительного директора и главного директора по технологиям, как профессор в области новых технологий и советник по глобальным стратегиям. Салли удостоена наград как докладчик по ключевым вопросам на международных мероприятиях, автор, исследователь. Она отличается свежестью мышления и новаторскими идеями.

Защита данных и кибербезопасность после вступления в силу общего регламента ЕС по защите данных (GDPR)

Содержание

Раздел 1 – Как изменилась защита данных после внедрения GDPR?

Компании проделали долгий путь. За прошедшие два года были расширены юридические отделы, найм ведущих специалистов по защите данных взлетел до небес[1], и вырос объем консультаций с независимыми советниками по защите данных. Выполнение оценок воздействия на защиту данных (DPIA) теперь хорошо знакомо тысячам организаций.

Но многое еще предстоит сделать.

Когда речь заходит о GDPR, одной из самых больших сложностей является то, что вы не можете ослабить внимание. В большинстве организаций практически любой сотрудник в любой момент может нарушить правила. Проблема усугубляется в секторах, где сотрудники работают на пределе своих возможностей или существует высокая степень самостоятельной работы, таких как здравоохранение, образование и право. В области права, например, многие адвокаты не видят ничего плохого в обмене конфиденциальными подробностями дела, просто вкладывая документы в электронное письмо. Медицинские работники могут обмениваться данными пациентов или результатами МРТ-сканирования, используя незащищенные адреса электронной почты. В организациях, где сотрудники работают в стрессовой обстановке, все, что нужно, чтобы они забыли о соответствии нормативным требованиям, — это еще немного расширить список дел. Казалось бы, ради производительности можно пренебречь протоколами.

Эта ситуация должна измениться.

Также существует проблема осведомленности в секторе благотворительности. Слишком часто благотворительные организации полагают, что действие GDPR на них не распространяется. Даже когда они осознают, что GDPR применяется ко всем без исключения частным, государственным и некоммерческим организациям, они (возможно, по вполне понятным причинам) неохотно отвлекают деньги от своей основной задачи, чтобы инвестировать их в защиту данных. Это благородно, но наивно. Потенциальные штрафы за нарушение правил GDPR затмевают вероятные расходы на ИТ.

С 2016 г. потребность в уполномоченных по защите данных (DPO) резко выросла более чем на 700%.

Tara Taubman-Bassirian
@clarinette02

GDPR, защита данных и консультанты по интеллектуальной собственности

«Во многих некоммерческих организациях говорят: “Правила GDPR к нам не относятся, ведь наша организация благотворительная”. Даже когда речь идет о соответствии веб-сайта правилам, я пытаюсь объяснить им, что речь идет не о данных, которые вы хотите собирать, а о третьих сторонах, которым вы предоставляете доступ к данным ваших посетителей».

1. **Varonis: год жизни по правилам GDPR. Важная статистика и выводы** www.varonis.com/blog/gdpr-effect-review/ **[на 26.11.19]**

Как изменилась защита данных после внедрения GDPR?

Минимизация объемов данных является обнадеживающей тенденцией

Мы живем в эпоху неописуемого сбора данных. «Большая четверка» (Google, Apple, Facebook и Amazon) хранит колоссальные объемы данных пользователей. Можно предположить, что другие организации захотят действовать также и собирать как можно больше данных. Тем не менее, чем больше данных вы храните, тем большему риску подвергаетесь. Одной из наиболее позитивных тенденций, наблюдаемых после внедрения GDPR, является отказ от чрезмерного сбора данных. Дальновидные компании руководствуются принципом минимизации: если данные вам не нужны, не собирайте их.

Tara Taubman-Bassirian
@clarinette02

GDPR, защита данных и консультанты по интеллектуальной собственности

«Минимизация данных является, вероятно, одним из лучших требований GDPR. Любое создание базы данных означает создание риска».

Rob Allen
@Rob_A_kingston

Директор по маркетингу и техническому обслуживанию, Kingston Technology

«У нас действуют жесткие правила в отношении удаления данных. Да, важные бизнес-данные должны храниться должным образом. А как насчет прочих данных? Через год они уже неактуальны. Так зачем их хранить?»

Преимущества заключаются не только к ограничении риска. К примеру, возьмите маркетинг. Если вы не следите за чистотой базы маркетинговых данных, то, возможно, храните устаревшую информацию. Если ваша база данных охватывает десятки тысяч людей, и вы часто проводите маркетинговые кампании по электронной почте, затраты растут. Это также искажает статистическую картину эффективности кампании.

Минимизация относится и к физическим данным. Будьте осторожны с тем, что вы распечатываете (например, отсканированные паспорта клиентов); будьте осторожны с тем, что записываете (например, пароли учетных записей) А если вам нужна физическая копия чего-либо, обеспечьте ее надежное хранение. Возможно, гора документов на вашем столе выглядит внушительно. Но она совсем не защищена.

Rafael Bloom
@rafibloom73

Директор, Salvatore Ltd

«Мы наблюдаем совершенно иной подход к взаимодействию между технологиями и реальным ведением бизнеса. Такой уровень цифровой зрелости среди бизнес-руководства был крайне необходим».

Последствия раскрытия данных: от высшего руководства до потребителя

Защита данных как нормативно-правовая концепция существует уже несколько десятилетий. Но крупные штрафы, выплаченные такими компаниями, как Google[1], British Airways и сеть отелей Marriott[2], (а также сопутствующий резонанс в СМИ) привлекли внимание высшего руководства к GDPR. В результате возник эффект просачивания.

1. **Varonis: год жизни по правилам GDPR. Важная статистика и выводы** www.varonis.com/blog/gdpr-effect-review/ **[на 26.11.19]**
2. **The Guardian: Штрафы, связанные с GDPR: на что пойдут 300 млн фунтов стерлингов BA и Marriott?** www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog **[на 26.11.19]**

Как изменилась защита данных после внедрения GDPR?

Продолжение...

Еще одной движущей силой внедрения надежной защиты данных является совместный бизнес. Крупные компании в настоящее время проводят комплексную экспертизу целостности защиты данных, обеспечиваемой потенциальными поставщиками, поскольку они не хотят нести ответственность за утечку данных вместе с ними.

Существует и еще одна сторона повышения осведомленности коммерческих предприятий о GDPR: потребители знают больше о своих правах в отношении данных. И они знают, что если компания потеряет контроль над их данными (обратите внимание: это необязательно должна быть утечка данных), они имеют право на компенсацию. Компании должны сохранять бдительность.

Sally Eaves
@sallyeaves

Генеральный и исполнительный директор, Sally Eaves Consultancy

«Защита данных стала первоочередным требованием бизнеса, проводящей границу между доверием или его потерей».

Раздел 2 – Как организации информируют своих сотрудников?

Обучение персонала: два слова, которые заставят ваших сотрудников закатывать глаза.

Еще одна причина сделать обучение увлекательным. Обученные сотрудники с меньшей вероятностью будут нарушать передовые практики защиты данных. И если произойдет утечка данных, Управление Комиссара по информации (ICO) отнесется к вам более благосклонно, если вы сможете доказать, что предприняли усилия по обучению своих сотрудников вопросам безопасности данных.

Rafael Bloom
@rafibloom73

Директор, Salvatore

«Мне нравится рассматривать данные как элемент цепочки поставок, где необходимо соответствующее управление их происхождением и всем жизненным циклом. Конечно, прекрасно собрать вашу команду в одной комнате на полчаса и рассказать им, что делать (не разбрасывайте бумаги, используйте сильные пароли). Конечно, так вы снизите риск для организации. Однако позже будет ли от этого на самом деле какая-то ощутимая отдача помимо того небольшого первоначального воздействия, как бы навязанного людям? Нет».

Однако в апреле 2019 года министр по цифровым технологиям Марго Джеймс утверждала, что три из десяти британских организаций провели обучение персонала по вопросам борьбы с киберугрозами[1]. Пришло время подойти к обучению серьезно.

Речь идет о формировании культуры, а не об обучении «для галочки»

Обучение должно быть направлено на создание подлинных изменений в поведении и культуре, а не проводиться ради отчетов. Купить онлайн-курс с несколькими простыми вопросами о защите данных, на которые любой может ответить правильно, очень легко. Но действительно ли это поможет защитить вашу организацию?

Хорошие практики защиты данных включают два основополагающих компонента. Первый их них — это продуманное, увлекательное обучение, ориентированное на уникальные задачи вашей организации. Второй — осознание того, что GDPR относится к принципиальным вопросам культуры поведения на рабочем месте, которые ежедневно влияют на всех сотрудников. Речь идет о правильной работе с данными в рамках всей организации. К примеру, рассмотрим отдел кадров. Задумайтесь обо всех личных данных соискателей, которые просто находятся на почтовых серверах.
Защита данных — ответственность каждого.

1. **Intelligent CISO: Год спустя: как внедрение GDPR повлияло на безопасность данных?**
   www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [на 26.11.19]

Как организации информируют своих сотрудников?

За каждым фрагментом данных стоит определенный человек

В первом разделе мы отметили, что потребители становятся более осведомленными о своих правах, связанных с данными. Хороший способ организовать тренинг по защите данных — помочь вашим сотрудникам установить эту связь: за любыми данными всегда стоит какой-то человек. Попросите своих сотрудников подумать о каждой организации, которой они предоставляли свои данные, и они осознают, что защита данных прежде всего ориентирована на неприкосновенность личной жизни.

Разработайте план действий в чрезвычайных ситуациях

Sally Eaves
@sallyeaves

«Постоянное обучение сотрудников по вопросам, связанным с безопасностью и конфиденциальностью данных, является первоочередным требованием бизнеса. Это должно быть не единичное мероприятие, не семинар раз в год, а проактивный, интерактивный и увлекательный опыт, ставший частью повседневной работы. Сотрудники должны быть вовлечены в диалог о том, какие риски мы хотим смягчить, чем хотим управлять и что защищать».

Miriam Brown
@Kingston_MBrown

«Мне кажется любопытным, когда во время тренинга вы говорите людям: “что если бы это были ваши данные?” Если бы менеджер моего банка работал из дома со своего ноутбука, на котором находится конфиденциальная информация, я бы хотел, чтобы эта информация хранилась на зашифрованном диске».

Rob Allen
@Rob_A_kingston

«Относитесь к данным так, как если бы они были вашими».

Раздел 3 – Как ИТ-отделы могут улучшить защиту устройств?

Удаленная работа стала новой нормой

Ваши сотрудники, вероятно, получают доступ к своей рабочей среде с нескольких различных устройств, включая личные устройства, которые можно легко оставить в поезде или забыть в такси. Ваша задача состоит в том, чтобы найти способ помочь вашим сотрудникам работать эффективно, в то же время не подвергая себя риску нарушения безопасности и утечки данных. Даже один человек может свести на нет все ваши усилия по защите данных.

Sally Eaves
@sallyeaves

Генеральный и исполнительный директор, Sally Eaves Consultancy

«Данные должны быть защищены во время передачи, хранения и использования. Очень важно иметь всеобъемлющий план обеспечения безопасности, восстановления и удаления данных, охватывающий все эти контексты. Особенно важно привлекать внимание к областям риска, которые часто недооцениваются. К ним относятся, например, незашифрованные USB-накопители, использование электронной почты для отправки незашифрованных вложений и функции веб-браузера, раскрывающие конфиденциальные данные пользователя. С учетом подключения большого количества устройств и изменения режимов работы очень важно обеспечить для данных, хранящихся на мобильном телефоне, такую же защиту, как и для данных на сервере компании».

Двухфакторная аутентификация

Для типичной организации, безусловно, самое лучшее и самое простое, что можно сделать, — это защитить периметр сети. И это действительно очень просто. Нужны всего лишь диспетчеры паролей и двухфакторная аутентификация. Хороший пример двухфакторной аутентификации: пользователю предлагается ввести пароль на ноутбуке, а также код, отправленный на его мобильный телефон после успешного ввода пароля.

Сети VPN и зашифрованные твердотельные диски и USB-накопители

На малых и средних предприятиях всё большую популярность приобретают виртуальные частные сети (VPN). Они особенно важны для сотрудников, которые получают доступ к бизнес-данным через общедоступные сети WIFI. Но предприятиям не следует переоценивать возможности сетей VPN. Это всего лишь часть решения. Слишком часто предприятия развертывают сети VPN лишь для того, чтобы работающие удаленно сотрудники могли использовать ноутбуки без какого-либо аппаратного шифрования. Практически все хранят файлы на своих ноутбуках. Но что происходит в случае взлома, утери или кражи устройства? Зашифрованные твердотельные и USB-накопители лишь немного дороже стандартных версий. Внедрение зашифрованных USB-накопителей и оснащение ваших ноутбуков твердотельными накопителями с аппаратным шифрованием — это долгий путь к решению проблем, связанных с удаленной работой. А в случае утери или кражи устройства вы можете быть уверены, что никто не получит доступ к зашифрованным файлам. Вы даже можете дистанционно уничтожать данные на утерянных USB-накопителях.

«Однажды я познакомился с экспертом по кибербезопасности, который пытался убедить генерального директора компании внедрить двухфакторную аутентификацию, но встретил сопротивление: "Нет, мы не будем это делать, это лишние хлопоты, дополнительные усилия, и мне это не нужно". Вскоре после этого компания стала жертвой мошенничества на 40 000 фунтов стерлингов».

Rafael Bloom
@rafibloom73

Директор, Salvatore Ltd

«В конечном счете, лучший способ повысить осведомленность о безопасности — это вести откровенные диалоги с сотрудниками, чтобы выработать безопасные и продуктивные стратегии».

Rob Allen
@Rob_A_kingston

Директор по маркетингу и техническому обслуживанию, Kingston Technology

Как ИТ-отделы могут улучшить защиту устройств?

Частные серверы и поставщики управляемых услуг

Все больше крупных организаций склоняются к тому, чтобы снова развертывать собственные локальные серверы. Это означает, что они имеют полный контроль над площадкой, на которой находится сервер, и никакие данные не хранятся в общедоступном облаке. Также существуют гибридные серверные решения, в которых неконфиденциальные данные находятся в облаке, а личные данные хранятся на месте. Для малых и средних предприятий и организаций в некоммерческом секторе владение собственным сервером может обходиться слишком дорого. И тут в дело вступают поставщики управляемых услуг и виртуальные частные серверы. Они больше внимания уделяют безопасности, не слишком увеличивая ваши эксплуатационные расходы.

Автоматическая пометка данных с истекающим сроком хранения

Одним из положений GDPR является необходимость удаления старых данных. Например, некоторые типы персональных данных не должны храниться дольше семи лет. Что если бы вы автоматически получали уведомление, когда истекает срок хранения данных? При наличии соответствующей базы данных ваша ИТ-команда могла бы легко создать действие для отправки уполномоченному по защите данных (DPO) автоматически сгенерированного электронного письма, когда истекает срок хранения данных.

Работа с надежными поставщиками

Когда речь идет об информационной безопасности, есть бесчисленное множество производителей и поставщиков. Проведите собственное исследование. Речь идет о наличии системы, созданной надежным поставщиком, обладающим конкретным опытом поддержки организаций в вашей отрасли или секторе. Убедитесь, что выбранные вами поставщики не только обладают нужными технологиями, но и понимают проблемы внедрения, когда речь заходит о безопасности данных.

Раздел 4 – Как поставщики технологий могут улучшить процессы и их анализ?

Внимание к уполномоченным по защите данных

С 2016 г. потребность в уполномоченных по защите данных резко выросла более чем на 700%.[1] На данный момент в Европе работают более 500 000 уполномоченных по защите данных. Это в шесть раз больше, чем прогнозировалось в 2017 году.[2] И все же важность роли этих специалистов часто недооценивается и упрощается.

Уполномоченному по защите данных требуется полное представление о состоянии конфиденциальности данных и безопасности в вашей компании. Это работа, требующая полной занятости. Однако в ряде организаций «уполномоченный по защите данных» — всего лишь значок, отмечающий одного из сотрудников, который лучше всех разбирается в технологии. Такие сотрудники несут ответственность за конфиденциальность данных в рамках всей компании, в то же время продолжая выполнять свои обычные обязанности.

Реальность такова, что для поддержки нового типа уполномоченных по защите данных необходим целый ряд профессиональных услуг и инструментов. Даже если у вас есть уполномоченный по защите данных, работающий на полную ставку, сфера безопасности данных быстро развивается, и постоянно возникают проблемы, требующие мнения другого специалиста. Работа со сторонними консультантами по безопасности данных может существенно помочь, но сначала вы должны как можно лучше организовать всё в своей компании.

Ясность, нештатные ситуации и слаженные действия

Сила всей вашей ИТ-инфраструктуры определяется по ее самому слабому элементу. Вот почему поставщик технологий для любого нового дополнения в вашей ИТ-экосистеме должен предоставить полную информацию в отношении потенциальных угроз безопасности и четкие советы о том, как безопасно использовать новый продукт.

Tara Taubman-Bassirian
@clarinette02

GDPR, защита данных и консультанты по интеллектуальной собственности

«Я пытаюсь объяснить людям, которые везде устанавливают камеры видеонаблюдения, что это не обязательно обеспечивает безопасность, потому что часто камеры устанавливаются без пароля. Таким образом, вы можете просто войти на веб-сайт, сидеть и наблюдать. Фактически это говорит грабителю: «приди и проверь, когда меня там нет!»

1. **Varonis: год жизни по правилам GDPR. Важная статистика и выводы** www.varonis.com/blog/gdpr-effect-review/ **[на 26.11.19]**
2. **The Guardian: Штрафы, связанные с GDPR: на что пойдут 300 млн фунтов стерлингов BA и Marriott?** www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog **[на 26.11.19]**

Как поставщики технологий могут улучшить процессы и их анализ?

Существует проблема нештатных ситуаций. Что происходит, когда срок службы продукта истекает или его необходимо обновить? Поставщики технологий должны предоставлять по своим продуктам рекомендации на случай нештатных ситуаций, которые непреднамеренно ставят под угрозу хранящиеся данные или подвергают риску безопасность вашей более обширной ИТ-экосистемы. Например, МРТ-сканер. Он может поставляться с зашифрованным SSD-накопителем емкостью четыре терабайта для хранения снимков пациентов. Но что будет, когда место на нем закончится?

Поставщики технологий и сами организации также должны способствовать созданию среды цифрового единства и согласованности данных, как внутри организации, так и при работе с внешними поставщиками и партнерами. Это особенно важно для многопрофильных организаций, включающих множество подразделений и объектов, таких как Национальная служба здравоохранения (NHS).

Miriam Brown
@Kingston_MBrown

Менеджер по стратегическому маркетингу в корпоративном секторе в Kingston Technology

«Мы продали в NHS большое количество продуктов. Но между трастовыми фондами есть определенные отличия, когда речь заходит о внедренных у них политиках и протоколах защиты».

Поиск информации из различных источников

Технологии быстро развиваются, иногда опережая безопасность. С появлением новых технологий (таких как оплата через распознавание лиц в Китае) иногда случается так, что организации стремятся заполучить новинку прежде, чем оценят ее потенциальные последствия для безопасности и защиты данных. Всего через год–два сети 5G получат широкое распространение, и периферийные вычисления и распределенные хранилища данных станут реальностью. Поставщики технологий должны быть в состоянии помочь организациям безопасно извлечь выгоду из новых технологий, не ставя под угрозу целостность собственных данных или безопасность ИТ-среды.

Sally Eaves
@sallyeaves

Генеральный и исполнительный директор, Sally Eaves Consultancy

«Я полагаю, что будут наблюдаться изменения в отношении к GDPR: от сокращения проблем с внедрением к сосредоточению внимания на оптимизации преимуществ, таких как улучшенные ИТ-процессы, резервное копирование и восстановление данных, повышение безопасности, а также использование всех этих достижений в качестве точки дифференциации по отношению к другим компаниям в отрасли».

Выводы

Внедрение Общего регламента ЕС по защите данных (GDPR) изменило ведение бизнеса в лучшую сторону, привлекая внимание высшего руководства компаний и потребителей к вопросам конфиденциальности данных и безопасности сети. Однако, чтобы обеспечить соответствие его правилам, необходимо постоянное, изо дня в день, внимание к безопасности данных со стороны каждого из ваших сотрудников. Постоянное развитие технологий и киберугроз означает, что для компаний важнейшее значение имеет надлежащая инфраструктура безопасности и правильное обучение, подкрепленное хорошей консультативной поддержкой по технологиям и конфиденциальности данных. Напоминание сотрудникам о том, что за данными всегда стоит человек, может в значительной степени способствовать формированию культуры защиты данных в вашей компании. А изменение культуры гораздо эффективнее эпизодических тренингов.

О компании Kingston

За 32 года работы компания Kingston накопила знания, позволяющие выявлять и решать проблемы заказчиков, связанные с удаленной работой. Благодаря этому ваши сотрудники смогут легко и безопасно работать из любой точки мира, не ставя под угрозу свою организацию.

#KingstonIsWithYou