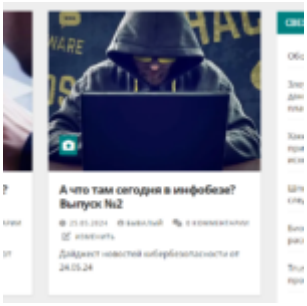
Дайджесты главных новостей кибербезопасности в формате веб-историй на портале InfoSecPortal.ru

написано GlobalTrust.ru | 28.05.2024



На портале кибербезопасности InfoSecPortal.ru началась публикация материалов в популярном формате веб-историй, совмещающем в себе все виды аудио-визуального представления данных.

Уже опубликованы дайджесты главных новостей информационной безопасности за прошедшую неделю. Источником новостей для веб-историй служит агрегатор рунета, который в автоматическом режиме формирует дайджесты новостей со всей значимых русскоязычных источников.

Создание веб-историй доступно всем пользователям портала с ролью Участник и выше. Истории создаются при помощи визуального редактора, разработанного компанией Google.

GlobalTrust рекомендует всем блогерам, авторам статей и новостей информационной безопасности взять на вооружение данный формат публикации. Это позволит оживить сухой статичный контент, порой, довольно сложных и скучных ИБ-повествований.

Рассказывайте читателям увлекательные истории, вместо обычной писанины!

https://infosecportal.ru/web-stories

ISO/IEC 27001:2022 и ISO/IEC 27002:2022: Ключевые обновления и идеи

написано GlobalTrust.ru | 28.05.2024

Международный стандарт на системы менеджмента информационной безопасности ISO 27001 и сопутствующий ему стандарт ISO 27002 были обновлены в 2022 году. В этой статье рассказывается о наиболее заметных изменениях этих стандартов.

Изменения ISO/IEC 27001:2022

ISO 27001:2022 существенно не отличается от ISO 27001:2013, но есть некоторые заметные изменения. Однако большинство из них относятся к Приложению SL, структуре высокого уровня, общей для всех новых стандартов систем менеджмента ISO, а не к информационной безопасности:

- **Контекст и область действия.** Теперь вы должны определить «релевантные» требования заинтересованных сторон и определить, какие требования будут удовлетворяться посредством СМИБ, которая теперь должна явно включать в себя «необходимые процессы и их взаимодействие».
- **Планирование.** Цели информационной безопасности теперь должны контролироваться и «быть доступными в виде документированной информации». Появился новый подраздел, посвященный

планированию изменений в СМИБ. Здесь не указаны какие-либо процессы, которые должны быть включены, поэтому вам следует определить, как вы можете продемонстрировать, что изменения в СМИБ действительно были запланированы.

- **Поддержка.** Требования по определению того, кто будет коммуницировать, и процессы осуществления коммуникации были заменены требованием определить, «каким образом следует коммуницировать».
- **Операции.** Требование планировать способы достижения целей информационной безопасности было заменено требованием установить критерии для процессов реализации действий, определенных в разделе 6, и управлять этими процессами в соответствии с этими критериями. От организаций теперь требуется контролировать «предоставляемые из-вне процессы, продукты или услуги», имеющие отношение к СМИБ.
- **Приложение.** Приложение А было пересмотрено для приведения его в соответствие с ISO 27002:2022. Механизмы контроля согласно Приложению А обсуждаются в разделе ниже.

Каковы изменения контроля в Приложении А?

Некоторые механизмы контроля Приложения А были объединены, а также было добавлено 11 новых:

- Несмотря на то, что никакие контроли не были удалены, в ISO 27001:2022 перечислено только 93 контроля, а не 114 как в ISO 27001:2013. Это связано с большим количеством объединенных контролей (24 вместо 56).
- Эти контроли сгруппированы в 4 «темы», а не в 14 областей контроля, как раньше. Они включают в себя:
    - Кадровые (8 контролей)
    - Организационные (37 контролей)
    - Технологические (34 контроля)
    - Физические (14 контролей)

- Совершенно новые контроли:
    - Разведка угроз
    - Информационная безопасность при использовании Облачных сервисов
    - Готовность ИКТ к обеспечению непрерывности бизнеса
    - Мониторинг физической безопасности
    - Управление конфигурацией
    - Удаление информации
    - Маскирование данных
    - Предотвращение утечки данных
    - Мониторинг активности
    - Веб-фильтрация
    - Безопасное кодирование

- В ISO 27002 контроли также имеют пять типов «атрибутов», чтобы их было легче классифицировать:
    - Тип контроля (превентивный, детектирующий, корректирующий)
    - Свойства информационной безопасности (конфиденциальность, целостность, доступность)
    - Концепции кибербезопасности (идентификация, защита, обнаружение, реагирование, восстановление)
    - Операционные возможности (стратегическое управление, управление активами и т. д.)
    - Домены безопасности (стратегическое управление и экосистема, защита, оборона, устойчивость)

Что изменилось в ISO 27002?

Фраза «свод правил» (“code of practice”) была исключена из названия обновленного стандарта ISO 27002. Это лучше отражает его цель как эталонного набора мер по обеспечению информационной безопасности.

Сам стандарт значительно длиннее предыдущей версии, а элементы

управления были переупорядочены и обновлены, как описано в разделе выше.

Как обновление ISO 27001 повлияет на вашу организацию?

Если вы находились на стадии внедрения предыдущей версии стандарта, не паникуйте. Органы по сертификации, скорее всего, предложат сертификацию по стандарту ISO 27001:2022 всего через шесть месяцев после его публикации. Кроме того, стандарт ISO 27001:2013 будет сохранен еще на три года, так что ваша работа по внедрению стандарта 27001:2013 не пропадет. Однако вы можете использовать новые контроли согласно Приложению A из ISO 27001:2022 в качестве альтернативного набора контролей.

Если вы уже сертифицированы по стандарту ISO 27001:2013, помните, что у вас будет время («Переходный период») для полного перехода на новые требования. Однако лучший момент для этого — перед следующим внутренним аудитом , независимо от того, прошли ли вы сертификацию давным давно или только находитесь в процессе сертификации.

Внутренний аудит ISO 27001 включает детальную оценку СМИБ вашей организации, чтобы убедиться в ее соответствии критериям стандарта. Это позволит вам оценить, правильно ли вы отразили в СМИБ изменения, не подвергая риску статус вашей сертификации. Рекомендуется проведение внутреннего аудита как минимум за три месяца до проведения внешней оценки. Это позволит выявить любые потенциальные несоответствия и исправить их до прихода внешнего оценщика.

Политики безопасности

GlobalTrust для приведения финансовых организаций в соответствие с ГОСТ Р 57580 по усиленному уровню защиты информации

написано GlobalTrust.ru | 28.05.2024

Компания GlobalTrust разработала комплект типовых политик информационной безопасности GTS 57580 (У), адаптированный специально для финансовых организаций, которым необходимо обеспечивать усиленный уровень защиты информации. Комплект включает в себя 10 типовых политик защиты информации, охватывающих все предъявляемые к финансовым организациям требования по обеспечению безопасности информации с учетом рекомендаций Банка России в области стандартизации процессов обеспечения ИБ (РС БР ИББС).

В соответствии с Положением Банка России от 17 апреля 2019 г. № 683-П кредитные организации должны обеспечивать реализацию требований национального стандарта РФ ГОСТ Р 57580.1-2017 по защите информации для объектов информационной инфраструктуры, используемых для обработки, передачи, хранения защищаемой информации в целях осуществления банковских операций.

Системно значимые кредитные организации, кредитные организации, выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитные организации, значимые на рынке платежных услуг, должны реализовывать усиленный уровень защиты

информации. Остальным кредитным организациям достаточно реализовать стандартный уровень защиты информации, определяемый ГОСТ Р 57580.1-2017.

Политики безопасности из комплекта GTS 57580 (У) также подойдут некредитным финансовым организациям (репозитарии, депозитарии, клиринговые организации, организаторы торговли, пенсионные фонды, брокеры, страховые компании и т.п.), которым в соответствии с Положением Банка России № 757-П, необходимо обеспечить соответствие ГОСТ Р 57580.1-2017 по усиленному или стандартному уровню защиты информации.

Некредитным финансовым организациям с минимальным уровнем защиты информации, подойдет упрощенная версия комплекта политик информационной безопасности GTS 57580 (М). К таким организациям относятся в частности банковские платежные агенты, небольшие пенсионные фонды, управляющие компании и т.п.

Все предоставляемые компанией GlobalTrust комплекты документов обеспечиваются гарантиями соответствия и актуальности, а также технической и консультационной поддержкой их адаптации и внедрения с учетом специфики конкретных финансовых организаций.

О компании GlobalTrust

Компания GlobalTrust с 2003 года осуществляет полное документальное обеспечение и сопровождение систем защиты информации и систем менеджмента информационной безопасности в организациях различного масштаба и сферы деятельности. С момента основания компании ее клиентами стали более 500 российских организаций. Эксперты GlobalTrust реализовали более 200 комплексных проектов по созданию и совершенствованию систем защиты информации.

Рекомендации НКЦКИ по компенсации ИТ-рисков для организаций РФ в условиях санкционных ограничений

написано GlobalTrust.ru | 28.05.2024

Для компенсации некоторых IT-рисков, формирующихся в условиях санкционных ограничений, Национальный координационный центр по компьютерным инцидентам предлагает воспользоваться следующими рекомендациями:

1. Проверить, что инфраструктура (хостинг), на которых размещаются публичные ресурсы, находится на территории РФ.
2. В случае аренды вычислительных мощностей необходимо компенсировать риск, возникающий в случае отказа хостинга размещать публичный ресурс, имеющий отношение к компании, находящейся под санкциями.
3. Удостовериться, что используемые для корректной работы публичных ресурсов DNS-сервера размещены на территории РФ. Также убедиться в отсутствии в цепочке серверов различных публичных иностранных серверов, например, DNS forwarding 8.8.8.8.
4. Убедиться, что регистратор, который управляет доменными именами публичных ресурсов, находится в РФ. В противном случае передать управление доменными именами любому отечественному регистратору.
5. В случае использования для публичных ресурсов основных доменных зон .com, .org и прочих, следует рассмотреть вариант

преимущественного использования доменной зоны .ru.

6. При наличии собственной автономной системы (AS) проработать вопрос ее связности.
7. Провести ревизию SSL-сертификатов, разработать план по переходу на самоподписанные сертификаты или выпущенные удостоверяющими центрами, находящимися на территории РФ.
8. Организовать инвентаризацию облачных решений и разработать план по переходу на российские аналоги или решения, разворачиваемые локально и неконтролируемые производителем извне. Это касается в том числе и решений, которые используются коммерческими предприятиями: мессенджеры, система управления взаимоотношениями с клиентами (CRM), средства коллективной работы, офисные пакеты, интегрированные среды разработки (IDE) и прочее.
9. Провести инвентаризацию продуктов, требующих проверку лицензии за рубежом. Предпринять меры по поиску альтернатив.
10. Создать локальные хранилища дистрибутивов программных продуктов и используемого в компании ПО с открытым исходным кодом. Не обновлять его до последней версии, а в случае уже произведенного обновления откатиться к версиям продуктов, выпущенных ранее 24 февраля 2022 года. В случае если обновление необходимо, по возможности, устанавливать его только после проверки в тестовой среде.
11. Минимизировать использование или полностью запретить пользователям использовать стороннее ПО с открытым исходным кодом, если в этом отсутствует прямая необходимость.
12. В случае если в IT-инфраструктуре используются комплексные программные решения отечественного производства, в состав которых входит ПО с открытым исходным кодом, проработать мероприятия по его безопасному обновлению, по возможности, совместно с разработчиком такого решения.
13. Оценить финансовые взаимодействия с контрагентами и выявить компании, которые не смогут принимать платежи с территории РФ и потенциально могут отказаться от дальнейшего сотрудничества.

Общий регламент ЕС по защите персональных данных (GDPR): что нужно знать, чтобы соответствовать требованиям

написано GlobalTrust.ru | 28.05.2024

Компании, которые собирают данные о гражданах в странах Европейского Союза (ЕС), должны соблюдать строгие правила защиты данных клиентов. Общий регламент по защите данных (GDPR) устанавливает стандарт прав потребителей в отношении их данных, а компаниям придется обеспечивать соответствие и исполнение данного стандарта.

Соблюдение GDPR вызывает некоторые опасения и ожидания у служб безопасности. Например, GDPR достаточно широко трактует то, что представляет собой личную информацию (personally identifiable information, PII). Компаниям необходимо обеспечить такой же уровень защиты таких вещей, как IP-адрес человека или данные файлов cookie, как и для имени, адреса и номера социального страхования.

GDPR оставляет много возможностей для интерпретации. Например, в нем говорится, что компании должны обеспечивать «разумный» уровень защиты персональных данных, но не определяется, что считать «разумным». Это дает регулирующему органу GDPR большую свободу действий, когда дело доходит до назначения штрафов за утечку данных и несоблюдение требований.

Что такое GDPR?

GDPR — это постановление, принятое Европейским парламентом в апреле 2016 года , заменившее устаревшую директиву о защите данных от 1995 года. Он содержит положения, которые требуют от предприятий защищать персональные данные и конфиденциальность граждан ЕС при транзакциях, осуществляемых в государствах-членах ЕС. GDPR также регулирует экспорт персональных данных за пределы ЕС.

Положения одинаковы во всех 28 государствах-членах ЕС, а это означает, что у компаний есть только один стандарт, которому нужно соответствовать в ЕС. Однако этот стандарт довольно высок и требует от большинства компаний крупных инвестиций для его соблюдения.

Почему существует GDPR?

Обеспокоенность общественности по поводу конфиденциальности привела к созданию GDPR. В Европе уже давно действуют строгие правила использования компаниями персональных данных своих граждан. GDPR заменяет Директиву ЕС о защите данных , которая вступила в силу в 1995 году. Это было задолго до того, как Интернет стал центром онлайн-бизнеса, которым он является сегодня. Следовательно, директива устарела и не учитывает многих способов хранения, сбора и передачи данных сегодня.

Насколько реальна общественная обеспокоенность по поводу конфиденциальности? Она возрастает с каждой новой громкой утечкой данных. Согласно отчету RSA о конфиденциальности и безопасности данных, для которого RSA опросила 7500 потребителей во Франции, Германии, Италии, Великобритании и США, 80% потребителей заявили, что потеря банковских и финансовых данных является главной проблемой. Утечка данных безопасности (например, паролей) и идентификационной информации (например, паспортов или водительских прав) была названа проблемой 76% респондентов.

Тревожная статистика для компаний, которые имеют дело с данными потребителей, заключается в том, что 62% респондентов отчета RSA заявили, что будут винить компанию, а не хакера, в утечке данных в случае

взлома. Авторы отчета пришли к выводу, что «по мере того, как потребители становятся более информированными, они ожидают большей прозрачности и оперативности от обработчиков их данных».

Отсутствие доверия к тому, как компании обращаются с их личной информацией, заставило некоторых потребителей принять собственные контрмеры. Согласно отчету RSA, 41% респондентов заявили, что намеренно фальсифицируют данные при подписке на услуги онлайн. Проблемы безопасности, желание избежать нежелательного маркетинга или риск перепродажи данных были среди их главных опасений.

Отчет также показывает, что потребителям нелегко простить компании, если произойдет нарушение, раскрывающее их личные данные. Семьдесят два процента респондентов в США заявили, что будут бойкотировать компанию, которая, по всей видимости, игнорирует защиту их данных. Пятьдесят процентов всех респондентов заявили, что они с большей вероятностью будут делать покупки в той компании, которая сможет доказать, что серьезно относится к защите данных.

«Поскольку предприятия продолжают цифровую трансформацию, более широко используя цифровые активы, услуги и большие данные, они также должны нести ответственность за ежедневный мониторинг и защиту этих данных», — делается вывод в докладе.

Какие типы конфиденциальных данных защищает GDPR?

GDPR защищает следующие типы персональных данных:

- Основная идентификационная информация, такая как имя, адрес и идентификационные номера.
- Веб-данные, такие как местоположение, IP-адрес, данные файлов cookie и RFID-метки.
- Здоровье и генетические данные
- Биометрические данные
- Расовые или этнические данные
- Политические взгляды

- Сексуальная ориентация

На какие компании распространяется GDPR?

Любая компания, которая хранит или обрабатывает личную информацию о гражданах ЕС в государствах ЕС, должна соблюдать GDPR, даже если у компании нет делового присутствия в ЕС. Конкретными критериями применимости данного регулирования к компаниям являются:

- Присутствие в стране ЕС.
- Нет присутствия в ЕС, но обрабатывает персональные данные жителей Европы.
- Более 250 сотрудников.
- Менее 250 сотрудников, но обработка данных влияет на права и свободы субъектов данных, не является случайной или включает определенные типы конфиденциальных персональных данных.

Это означает, что почти все компании должны соблюдать GDPR.

В ходе опроса, проведенного Propeller Insights и спонсируемого Netsparker Ltd., руководителям было задано вопрос, какие отрасли больше всего пострадают от GDPR. Большинство (53%) отметили, что больше всего пострадал сектор технологий, за ним следуют интернет-торговля (45%), компании-разработчики программного обеспечения (44%), финансовые услуги (37%), онлайн-услуги/SaaS (34%) и розничная торговля (33%).

Кто в моей компании несет ответственность за соблюдение требований?

GDPR определяет несколько ролей, которые отвечают за обеспечение соответствия: контролер данных, обработчик данных и сотрудник по защите данных (DPO).

Контроллер данных определяет, как обрабатываются персональные данные и цели, для которых они обрабатываются. Контролер также несет ответственность за обеспечение соблюдения требований внешними подрядчиками.

Обработчиками данных могут быть внутренние группы, которые обрабатывают записи персональных данных, или любая аутсорсинговая фирма, которая выполняет всю или часть этой деятельности. GDPR возлагает на обработчиков ответственность за нарушения или несоблюдение требований. Таким образом, возможно, что и ваша компания, и партнер по обработке, например поставщик облачных услуг, будут нести ответственность и получать штрафные санкции, даже если вина полностью лежит на партнере по обработке.

GDPR требует, чтобы контролер и обработчик назначили ответственного за защиту персональных данных (DPO) для надзора за стратегией безопасности персональных данных и соблюдением GDPR. Компании обязаны иметь DPO, если они обрабатывают или хранят большие объемы данных граждан ЕС, обрабатывают или хранят специальные персональные данные, регулярно контролируют субъектов персональных данных или являются государственным органом. Некоторые государственные организации, такие как правоохранительные органы, могут быть освобождены от требования к наличию DPO.

Какое отношение GDPR имеет в кибербезопасности?

Многие требования GDPR не имеют прямого отношения к кибербезопасности, но процессы и системные изменения, необходимые для его соблюдения, могут повлиять на существующие системы и процессы обеспечения безопасности.

GDPR может также изменить отношение представителей бизнеса и групп безопасности к данным. Большинство компаний рассматривают свои данные и процессы, которые они используют для их анализа, как актив, но это восприятие изменится, говорит Льюис. «Учитывая необходимость получения явного согласия на обработку персональных данных, а также более

детального отслеживания состава данных и информационных потоков, у компаний теперь существует целый набор обязательств, связанных с накоплением данных», — говорит Льюис.

Как GDPR влияет на контракты с третьими сторонами и клиентами?

GDPR возлагает равную ответственность на контролеров данных (организацию, владеющую данными) и обработчиков данных (внешние организации, которые помогают управлять этими данными). Если сторонний обработчик не соответствует требованиям, это означает, что и ваша организация не соответствует требованиям. В новом постановлении также предусмотрены строгие правила сообщения о нарушениях, которые должен соблюдать каждый участник цепочки. Организации также должны информировать клиентов об их правах в отношении персональных данных.

Это означает, что во всех существующих контрактах с обработчиками персональных данных (например, поставщиками облачных услуг, поставщиками SaaS или поставщиками услуг по расчету заработной платы) и клиентами необходимо прописывать обязанности сторон в отношении персональных данных. Пересмотренные контракты также должны определить последовательные процессы управления и защиты данных, а также способы сообщения о нарушениях.

«Самая большая работа приходится на закупочную деятельность компании — ваши отношения с поставщиками, которые обрабатывают данные от вашего имени», — говорит Мэтью Льюис, руководитель практики банковского дела и регулирования в поставщике юридических услуг Axiom. «Существует целая группа поставщиков, которые имеют доступ к персональным данным, и GDPR очень четко определяет, что вам необходимо убедиться, что все эти третьи стороны соблюдают GDPR и обрабатывают данные соответствующим образом».

Контракты с клиентами также должны отражать нормативные изменения, говорит Льюис. «Клиентские контракты принимают различные формы, будь то онлайн-переходы по ссылкам или официальные соглашения, в которых вы берете на себя обязательства относительно того, как вы будете

просматривать, получать доступ и обрабатывать данные».

Прежде чем эти контракты будут пересмотрены, бизнес-руководители, ИТ-специалисты и специалисты по безопасности должны разобраться, как данные хранятся и обрабатываются, и согласовать соответствующий процесс отчетности. «Технологическим группам, директору по информационной безопасности и команде по управлению данными требуется довольно серьезная работа, чтобы понять, какие данные обрабатываются в компании, где они хранятся и как они передаются за пределы компании. Как только вы разберетесь с этими потоками данных и их влиянием на бизнес, вы сможете начать определять поставщиков, на которых вам следует сосредоточиться как с точки зрения информационной безопасности, так и с точки зрения управления этими отношениями в будущем и того, как вы зафиксируете это в контракте», — говорит Льюис.

«Данные покидают фирму разными способами», — говорит Льюис. «Директор по информационной безопасности и технологические группы должны иметь возможность отслеживать все это, а также вам необходимо обеспечить защиту». Эти меры защиты должны быть прописаны в контракте, чтобы сторонние фирмы понимали, что они могут и чего не могут делать с данными.

Льюис отмечает, что, пройдя процесс определения обязательств и ответственности, он подготавливает компанию к принятию оперативных мер по соблюдению требований GDPR. «Если один из ваших поставщиков говорит: «Вас взломали прошлой ночью», знают ли они, кому звонить и как реагировать в рамках соблюдения нормативных требований», — говорит он.

72-часовой период отчетности об инцидентах, требуемый GDPR, делает особенно важным, чтобы поставщики знали, как правильно сообщать о нарушениях. «Если поставщика взломали, а вы один из тысяч клиентов, уведомят ли они ваш отдел закупок, лицо, ответственное за работу с клиентами, или кого-то, кто занимается дебиторской задолженностью? Это может произойти по-разному», — говорит Льюис.

В контракте должно быть четко определено, каким образом информация попадет к лицу в вашей организации, ответственному за сообщение о нарушении. «Регулирующий орган не скажет, что у вас не должно было быть

нарушения. Они скажут, что у вас должны были быть политики, процедуры и структура реагирования, чтобы быстро решить эту проблему», — говорит Льюис.

Что произойдет, если моя компания не соблюдает GDPR?

GDPR предусматривает суровые штрафы за несоблюдение требований в размере до 20 миллионов евро или 4% годового оборота, в зависимости от того, что больше.

По данным GDPR Enforcement Tracker, по состоянию на март 2024 года ЕС наложил 2022 штрафа. Подавляющее большинство этих штрафов составляют от нескольких тысяч до десятков тысяч евро. Самый крупный штраф был наложен в мае 2023 года на Meta Platforms Ireland Limited на сумму 1,2 миллиарда евро. Этот штраф был наложен из-за недостаточных правовых оснований для обработки персональных данных.

Регуляторы признали, что у них нет ресурсов, чтобы справиться с объемом сообщений о нарушениях, которые они получили, поэтому потребуется время для установления идентифицируемых прецедентов.

На данный момент способность демонстрировать добросовестное стремление соблюдать требования должна защитить компании от суровых наказаний. В своей речи в 2018 году Лиз Денхэм, информационный комиссар Великобритании, сказала организациям, обеспокоенным штрафами GDPR:

«...Надеюсь, теперь вы знаете, что принуждение — это крайняя мера.... Крупные штрафы будут наложены на те организации, которые систематически, умышленно или по неосторожности нарушают закон. Те организации, которые отчитываются самостоятельно, сотрудничают с нами для решения проблем и демонстрируют эффективные механизмы подотчетности, могут ожидать, что это станет важным фактором при рассмотрении любых нормативный мер».

Какие требования GDPR повлияют на мою компанию?

Требования GDPR вынуждают компании изменить способы обработки, хранения и защиты персональных данных клиентов. Например, компаниям разрешается хранить и обрабатывать персональные данные только с согласия человека и «не дольше, чем это необходимо для целей обработки». Должна быть возможность передачи персональных данных от одной компании к другой, и компании должны удалять персональные данные по запросу.

Этот последний пункт также известен как право на забвение. Есть некоторые исключения. Например, GDPR не отменяет каких-либо юридических требований о хранении в организации определенных данных. Это будет включать требования к медицинским записям HIPAA.

Некоторые требования напрямую влияют на команды безопасности. Во-первых, компании должны быть в состоянии обеспечить «разумный» уровень защиты данных и конфиденциальности гражданам ЕС. Что в GDPR подразумевается под «разумным», не очень четко определено.

Сложным требованием является то, что компании должны сообщать об утечках данных надзорным органам и лицам, пострадавшим от утечки, в течение 72 часов с момента обнаружения утечки. Еще одно требование — проведение оценки воздействия — призвано помочь снизить риск нарушений путем выявления уязвимостей и способов их устранения.

Как выглядит успешный проект GDPR?

Трудно представить компанию, более пострадавшую от GDPR, чем ADP. Компания предоставляет облачные услуги по управлению человеческим капиталом (HCM) и бизнес-аутсорсингу для более чем 650 000 компаний по всему миру. ADP хранит персональные данные миллионов людей по всему миру, и ее клиенты ожидают, что компания будет соответствовать требованиям GDPR и поможет им сделать то же самое. Если будет установлено, что ADP не соответствует GDPR, она рискует не только штрафами, но и потерей бизнеса для клиентов, ожидающих, что ADP их

защитит.

Глобальная направленность и масштаб ADP в некотором смысле являются преимуществом, когда речь идет о соблюдении GDPR. Они уже придерживались существующих правил конфиденциальности и безопасности, поэтому переход к соблюдению требований GDPR был не таким высоким, как мог бы быть. «Мы уже знакомы с законами о конфиденциальности в Европе. Мы не начинаем с нуля с GDPR», — говорит Сесиль Жорж, директор по конфиденциальности ADP. «GDPR требует от нас соблюдения требований не только как компании, но и как поставщика услуг. Мы помогаем нашим клиентам соблюдать GDPR».

Несмотря на то, что ADP подготовлена лучше, чем многие другие компании, Жорж говорит, что ее проект GDPR был масштабным и глобальным. «Мы начали еще до того, как обсуждался GDPR», — говорит она. Компания начала картирование потоков данных и оценку конфиденциальности новых продуктов несколькими годами ранее.

Проект GDPR ADP привлек людей из многих подразделений компании, и Жорж считает, что это было необходимо для успеха. «Мы участвуем во всех операциях и функциональных группах. Это не просто проект обеспечения конфиденциальности или соблюдения требований. На самом деле это касается всей организации, и мы координируем свои действия с менеджерами проектов по всей компании, чтобы убедиться, что мы внедряем правильные процессы», — говорит она.

Механизмы защиты персональных данных, такие как шифрование, уже существовали в ADP. «С точки зрения безопасности мы пришли к выводу, что речь идет больше об общении с нашими клиентами, чтобы убедиться, что они имеют правильную информацию о том, что мы делаем», — говорит Жорж. «Им, возможно, придется транслировать это сообщение своим сотрудникам или своим клиентам».

Поскольку ADP является обработчиком данных для других компаний, ADP предприняла дополнительный шаг по определению обязательных корпоративных правил, касающихся защиты персональных данных. «Внедряя обязательные корпоративные правила в качестве обработчика данных, мы надеемся, что наши клиенты поймут, что мы хотим облегчить их жизнь, и

обязуемся защищать их персональные данные в соответствии со стандартами, требуемыми в ЕС, независимо от того, где находятся и как обрабатываются данные граждан ЕС», — говорит Жорж.

«Существуют разные сценарии применения GDPR в зависимости от особенностей бизнеса и имеющихся в наличии инструментов защиты данных», — говорит Жорж. «После того, как проведена оценка и разработан план обеспечения соответствия, в соответствии с GDPR необходимо документировать процедуры обработки и защиты данных».

Что должна делать моя компания, чтобы соответствовать требованиям GDPR?

Если ваша организация не уверена в своем соответствии нормативным требованиям и вы определили значительный риск несоблюдения требований, выполнение этих шагов поможет вам встать на правильный путь.

Инициатива должна исходить от высшего руководства. Компания по управлению рисками Marsh подчеркивает важность руководства организации в определении приоритетов в реализации мер по обеспечению кибербезопасности. Соблюдение глобальных стандартов гигиены данных является частью этой инициативы.

Вовлеките все заинтересованные стороны. Одни лишь ИТ-отделы плохо подготовлены к выполнению требований GDPR. Создайте рабочую группу, в которую войдут специалисты по маркетингу, финансам, продажам, операциям — любая группа внутри организации, которая собирает, анализирует или иным образом использует персональные данные клиентов. Имея представительство в целевой группе GDPR, они смогут лучше обмениваться информацией, которая будет полезна тем, кто внедряет необходимые технические и процедурные изменения.

Периодически проводите оценку рисков. Вы хотите знать, какие данные о гражданах ЕС вы храните и обрабатываете, и понимать связанные с ними риски. Помните, что оценка риска должна также определять меры, принятые для снижения этого риска. Ключевым элементом этой оценки будет

выявление всех теневых ИТ, которые могут собирать и хранить персональные данные. Теневые ИТ и более мелкие точечные решения представляют наибольший риск несоблюдения требований; вы можете игнорировать их на свой страх и риск.

И их очень много. По словам Мэтта Фишера, ведущего эксперта в области ИТ и старшего вице-президента Snow Software, известно, что более 39 000 приложений содержат персональные данные. «Эффект айсберга представляет серьезный риск для соблюдения организациями GDPR, поскольку многие из них сосредоточены на 10% приложений, содержащих персональные данные, которые видны над поверхностью», — говорит он.

Фишер ссылается на то, как организации распределяют свои расходы на ИТ и технологии: около половины этих расходов принадлежит бизнес-подразделениям, что может поставить под угрозу соблюдение GDPR», — говорит он.

«Начать оценку рисков — самое сложное», — говорит Фишер. «В первую очередь организации должны получить полную картину всей своей ИТ-инфраструктуры и провести инвентаризацию всех приложений в своих подразделениях. Это, в сочетании с конкретным пониманием того, какие приложения могут обрабатывать персональные данные, значительно сводит к минимуму масштабы проекта, а также затрачиваемое на него время».

Наймите или назначьте DPO, если вы еще этого не сделали. GDPR не говорит, должен ли DPO быть отдельной должностью, поэтому предположительно компания может назначить кого-то, кто уже выполняет эту роль, при условии, что этот человек может обеспечить защиту персональных данных без конфликта интересов. В противном случае вам придется нанять DPO. В зависимости от организации этот DPO не обязательно должен работать полный рабочий день. В этом случае возможен вариант виртуального DPO. Правила GDPR позволяют DPO работать с несколькими организациями, поэтому виртуальный DPO будет похож на консультанта, который привлекается по мере необходимости.

Создайте и поддерживайте план защиты данных. У большинства компаний уже есть план, но им необходимо будет пересмотреть и обновить его, чтобы убедиться, что он соответствует требованиям GDPR.

Периодически пересматривайте и обновляйте его.

Не забывайте о мобильных устройствах: согласно опросу руководителей ИТ и служб безопасности, проведенному Lookout, Inc., 64% сотрудников получают доступ к личным данным клиентов, партнеров и сотрудников с помощью мобильных устройств. Это создает уникальный набор рисков несоблюдения GDPR. Например, 81% респондентов опроса заявили, что большинству сотрудников разрешено устанавливать личные приложения на устройства, используемые в рабочих целях, даже если это их собственные устройства. Если какое-либо из этих приложений получает доступ к персональным данным и сохраняет их, они должны делать это в соответствии с требованиями GDPR. Это сложно контролировать, особенно если учесть все несанкционированные приложения, которые используют сотрудники.

Документируйте свой прогресс соблюдения GDPR: «Пока часы тикают, организации должны демонстрировать, что они добиваются прогресса в заполнении Отчета об обработке данных (RoPA) — статьи 30 регламента GDPR, которая сосредоточена на инвентаризации рискованных приложений — легкая цель для регулирующих органов», — говорит Фишер. «Создание RoPA — это важная часть, на которой следует сосредоточиться на этом этапе, поскольку он позволяет организациям определять, где обрабатываются персональные данные, кто их обрабатывает и как».

Внедрите меры по снижению риска. После того как вы определили риски и способы их снижения, вы должны принять эти меры. Для большинства компаний это означает пересмотр существующих мер по снижению рисков. «После инвентаризации приложений и завершения RoPA команда GDPR теперь может выявлять и исследовать любые риски, связанные с данными, и определять соответствующий уровень безопасности, который считается необходимым для защиты этих данных», — говорит Фишер.

Если ваша организация небольшая, при необходимости обратитесь за помощью. GDPR повлияет на небольшие компании, на некоторые более существенно, чем на другие. У них может не быть ресурсов, необходимых для удовлетворения потребностей. Можно привлечь внешние ресурсы для предоставления консультаций и технические эксперты, которые помогут им в этом процессе и сведут к минимуму внутренние сбои.

Планы реагирования на инциденты. GDPR требует, чтобы компании сообщали о нарушениях в течение 72 часов. Насколько хорошо группы реагирования минимизируют ущерб, напрямую повлияет на риск получения компанией штрафов за нарушение. Убедитесь, что вы можете адекватно сообщить и отреагировать на инцидент в течение установленного периода времени.

Настройте процесс постоянной оценки. Вам надо убедиться, что вы продолжаете соблюдать требования, а это потребует постоянного мониторинга и улучшения. Некоторые компании рассматривают возможность стимулирования и наказания, чтобы гарантировать, что сотрудники следуют новой политике. Согласно опросу Veritas Technologies , 47% респондентов, скорее всего, добавят обязательное соблюдение политики GDPR в контракты сотрудников. 25% процентов могут отменить бонусы или льготы в случае нарушения GDPR, а 34% говорят, что будут вознаграждать сотрудников за соблюдение GDPR.

Делайте все это с прицелом на улучшение своего бизнеса. Согласно опросу Varonis Systems, 74% респондентов считают, что соблюдение требований GDPR станет конкурентным преимуществом. Соблюдение требований повысит доверие потребителей. Что еще более важно, это технологические улучшения, необходимые для удовлетворения требований GDPR, которые должны обеспечить эффективность управления и защиты данных в организациях.

Источник: https://www.csoonline.com/article/562107/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html