Через десять дней в силу вступает GDPR - что можно успеть предпринять?

rus.db.lv, 15/05/2018, Rus.db.lv

До момента, когда Общий регламент по защите данных (GDPR) вступает в силу, осталось всего 10 дней. Поэтому юристы и IT-специалисты советуют несколько основных вещей, которые можно успеть привести в порядок за оставшийся срок. Важно понимать, что это не означает, что предприятие будет полностью готово к GDPR.

“Готовность предприятий к GDPR и соответствие ему - это цель, которая не достигается за один раз. Технологии развиваются, вместе с ними меняются возможности кибер-преступников получать доступ к данным, поэтому и юридические, и IT-процессы (и их соответствие с GDPR) будет необходимо время от времени пересматривать и после 25 мая. В свою очередь, тем, кто только начал этот путь, скорее всего, внутреннюю подготовку придется продолжать после упомянутой даты” - поясняет представитель IT-компании “Squalio” Марек Грушкевиц.

“Squalio” совместно с бюро присяжных адвокатов “Sorainen” разработали продукт GDPR Ready, который объединяет юридическую и IT-компетентность накануне введения новых правил, поэтому эксперты предприятий поясняют, что еще можно успеть сделать за 10 дней, оставшихся до вступления регламента в силу.

Адвокат компании “Sorainen” Иева Андерсоне о юридических моментах, которые еще можно успеть привести в порядок:

●Мини-аудит собственными силами - опрос департаментов или работников, чтобы выяснить, какие персональные данные они собирают и обрабатывают, а главное - для чего. Это позволяет хотя бы на элементарном уровне узнать цель сбора данных и правовое основание.

●Если в какой-то момент вы не получаете ответ на вопрос “Зачем нужны эти данные?”, то лишние данные лучше уничтожить, анонимизировать или псевдонимизировать. Таким образом будет соблюден принцип минимизации и условие, что данные нельзя хранить дольше, чем они обоснованно необходимы.

●Подготовить информативные сообщения новой формы об обработке данных, указывая в них информацию, отмеченную в 13 пункте нового Регламента. Например, уточнить и дополнить сообщения о видеонаблюдении.

●Связаться с главными договорными партнерами, которые обрабатывают данные от имени и по заданию вашего предприятия (например, маркетинговые предприятия, которым переданы клиентские данные для повышения активности продаж), и договориться о порядке, как подготовить поправки к договорам, чтобы отражать требования нового Регламента.

●Улучшить и дополнить политику конфиденциальности предприятия, если такая уже есть. Если такой нет - можно подготовить упрощенную версию, которая отражает то, как предприятие обрабатывает личные данные своих клиентов и партнеров.

“Личными данными считаются любые данные, которые позволяют идентифицировать конкретного индивида. Например: имя, фамилия, персональный код, контактная информация, личное фото, IP-адрес, файлы cookies, место нахождения, политические или философские взгляды, религия, биометрические данные, состояние здоровья и так далее”, напоминает Андерсоне.

В то же время Грушкевиц подчеркивает самые существенные аспекты IT, на которые следует обратить внимание:

●Убедитесь о безопасности устройств, конечно, установите антивирусы и брандмауэры, потому что в конечном счете одна из целей GDPR - снизить утечку данных и несанкционированный доступ к персональным данным. Очень пригодиться могут, например, Bitdefender, ESET и другие.

●Пересмотрите, используется ли на предприятии лицензионное и актуальное программное обеспечение. Возможно, может показаться, что нелицензионные программы “дешевле”, однако долговременные риски гораздо выше. Нелицензионные программы могут скрывать в себе скрытые зловредные “сюрпризы” - например, шпионские программы, вирусы и т.д. Использование нелицензионных программ также содержит высокий риск утечки данных. Даже в устаревшем ПО могут скрываться бреши.

●Выберите регистр данных, который содержит в себе информацию о том, данные какой персоны обрабатываются, кто и каким способом это осуществляет. Это позволит предприятию оперативно и понятно ответить на вопросы физических лиц о том, какие из их данных обрабатываются. Здесь может пригодиться автоматизированное решение Wisery.

●Согласно Регламенту, должна быть возможность по запросу частного лица удалить все его данные, если только нет легитимной причины для их хранения. Для осуществления этого процесса можно приобрести технологии для мониторинга структурированных и неструктурированных баз данных, например StoredIQ, IMB Guardium.

“В сущности - устройством, которое используется для работы, считается любое устройство, которое находится в помещениях конкретного предприятия, в том числе - личные смартфоны сотрудников и другие устройства. Тем более, если они синхронизированы с рабочей почтой или каким-нибудь облачным сервисом. Поэтому, памятуя о компьютерной безопасности, нужно помнить и о мобильных телефонах”, напоминает Грушкевиц.

Оба эксперта подчеркивают, что это “быстрые” решения, которые не заменяют полноценный юридический и IT-аудиты, которые позволяют подготовить решения, подходящие конкретному предприятию, как подразумевает предлагаемый совместный продукт “Sorainen” и “Squalio” - GDPR Ready.

* GDPR (General Data Protection Regulation — англ.) - Общий регламент о защите данных.

Rus.db.lv