РОССИЙСКИЙ БИЗНЕС НЕ ЗАЩИТИТСЯ ОТ GDPR

ЗАВТРА, 25 МАЯ 2018 ГОДА, ВСТУПАЕТ В СИЛУ НОВЫЙ ЕВРОПЕЙСКИЙ РЕГЛАМЕНТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ — GENERAL DATA PROTECTION REGULATION (GDPR). НА КОНФЕРЕНЦИИ, ПОСВЯЩЕННОЙ ТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, КОТОРУЮ ОРГАНИЗОВАЛ ИД «КОММЕРСАНТЪ» В САНКТ-ПЕТЕРБУРГЕ, ЭКСПЕРТЫ РЫНКА ОБСУДИЛИ, КАК НОВЫЙ РЕГЛАМЕНТ ОТРАЗИТСЯ НА ОТЕЧЕСТВЕННОМ БИЗНЕСЕ. АЛЕКСЕЙ КИРИЧЕНКО

GDPR — это новый европейский регламент по защите персональных данных, единый для 28 стран Евросоюза. Постановление принято Европейским парламентом и Советом ЕС в апреле 2016 года и вступает в силу 25 мая 2018 года после двухлетнего переходного периода. Новый регламент предоставляет гражданам ЕС инструменты для полного контроля над своими персональными данными.

В GDPR выделены понятия контролера и обработчика персональных данных. Первый определяет цели и средства обработки, а второй по поручению контролера обрабатывает персональные данные. Контролером и обработчиком могут выступать физические или юридические лица, государственные органы, агентства. В целях безопасности обработки контролер и обработчик должны использовать псевдонимизацию и криптографическую защиту персональных данных, средства для обеспечения постоянной конфиденциальности и своевременного восстановления доступа к ним в случае природного или технического инцидента. Также они обязаны уведомлять надзорные органы об утечке персональных данных и сообщать об этом субъекту данных.

За невыполнение закона на компании накладывается штраф до €20 млн или до 4% от годового мирового оборота за предыдущий финансовый год — в зависимости от того, что больше.

Системное регламентирование вопросов защиты персональных данных в ЕС существует с 1995 года, когда была принята директива № 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных». Начальник отдела информационных технологий департамента проектирования компании «Газинформсервис» Сергей Коловангин отмечает, что цель принятия GDPR — это модернизация директивы №95/46 с учетом всех изменений, которые произошли в IT. По словам господина Коловангина, принципиальное изменение, которое носит новый регламент, это экстерриториальность и наднациональность. «Защитные меры принимаются независимо от национальности и места жительства субъекта персональных данных. А организации, учрежденные в ЕС, обязаны выполнять требования вне зависимости от факта обработки персональных данных на территории ЕС»,— объясняет он.

АЛЕКСАНДР КОРЯКОВ

GDPR НАПРЯМУЮ ЗАТРОНЕТ РОССИЙСКИЙ БИЗНЕС, ЧЬИ УСЛУГИ ОРИЕНТИРОВАНЫ НА ЕВРОПЕЙСКИЙ ИЛИ МЕЖДУНАРОДНЫЙ РЫНОК

ЧТО ДЕЛАТЬ БИЗНЕСУ? GDPR напрямую затронет российский бизнес, чьи услуги ориентированы на европейский или международный рынок. К примеру, это дочерние предприятия и филиалы российских компаний в ЕС. Даже если компания не учреждена в ЕС, но предоставляет различные товары и сервисы европейцам, она тоже попадает под регулирование. Это, к примеру, продажа путевок в интернете, онлайн-кинотеатры и музыкальные сервисы, а также оказание услуг мобильной связи в европейском роуминге. Также GDPR применим к компаниям, чьи сайты и приложения собирают персональные данные пользователей.

Партнер, руководитель практики «Интеллектуальная собственность и информационные технологии» петербургского офиса юридической фирмы «Борениус» Павел Савицкий рассказал, в каких случаях у российских компаний появляется обязанность назначить своего представителя в ЕС. «Когда обработка персональных данных людей на территории ЕС носит не системный, спорадический характер, то этих представителей можно не назначать. Но если для компании это часть бизнеса (к примеру, у нее есть магазин, она торгует на Европу и получает персональные данные жителей), тогда нужно назначать представителя»,— отмечает господин Савицкий.

Сергей Коловангин выделяет пять шагов на пути к успешному выполнению требований GDPR. Первый шаг касается изучения данных. «Когда вы приняли решение о необходимости соответствия GDPR, проведите инвентаризацию и изучите информационные потоки, их привязку к тем информационным системам, в которых у вас обрабатываются данные, чтобы понять, где могут быть узкие места»,— говорит господин Коловангин. Особенно важно понимание путей передачи данных третьим лица, отмечает он.

Второй шаг касается определения минимального объема отчетности, которая требуется контролеру и обработчику персональных данных. Весь перечень отчетности представлен в статье 30 GDPR и включает такие пункты, как цель обработки персональных данных, перечень их получателей, сроки удаления различных категорий данных. Третий шаг касается жизненного цикла данных. Для всех информационных систем безопасность обрабатываемых данных должна быть заложена по умолчанию, говорит господин Коловангин. Хранение данных должно осуществляться с учетом прав субъекта на их получение и перенос, а удаление — с учетом права субъекта на забвение данных.

В-четвертых, важно минимизировать риски при взаимодействии с третьими лицами. «В отчетности, которую требует регулятор, должно быть представлено обоснование передачи данных третьим лицам. Если обосновать компания не может, то это станет основанием для выдачи ей замечания со стороны регулятора в ЕС», — отмечает господин Коловангин. Последний пункт — это назначение ответственных сотрудников в компании за реализацию GDPR. Этот сотрудник будет заниматься реализацией технических мероприятий, взаимодействием с ЕС, составлением отчетности.

«Самое сложное требование, на мой взгляд,— это взаимодействие с регуляторами. Оно обусловлено прежде всего языковым барьером и особенностями регулировании на национальном уровне в странах ЕС. Если у компании большое количество филиалов в странах, то это может привести к назначению до 28 специалистов, что потребует огромных трудозатрат юридических департаментов или привлечения соответствующих специалистов»,— говорит эксперт.

В ЧЕМ ОТЛИЧИЯ В России бизнес также обязан заботиться о защите персональных данных. В 2006 году в ступил в силу федеральный закон № 152 «О персональных данных», штраф за несоблюдение которого составляет до 75 тыс. рублей. При этом он имеет несколько различий с GDPR.

Как отмечает Павел Савицкий, в России не реализовано право на переносимость данных. «Это значит, что я могу попросить организацию, у которой есть мои персональные данные, перенести их в другое место или выдать мне их, чтобы я перенес самостоятельно. Google, например, это реализовал»,— говорит он. Также в ЕС, в отличие от России, компаниям необходимо уведомлять надзорный орган об утечках в течение 72 часов. «Регулятор должен дать рекомендации, что делать. И если компания выполнит рекомендации и в остальном она соответствует закону, то штрафов можно избежать. В 152-ФЗ, если компания обнаружила утечку, то может сама ее устранить и никуда не обращаться»,— говорит господин Савицкий.

Сергей Коловангин считает, что Роскомнадзор, проанализировав GDPR, с большой долей вероятности захочет внести изменения в 152-ФЗ и его подзаконные нормативные акты, чтобы наша документация соответствовала европейскому подходу. «Это делается не столько по желанию самого регулятора, сколько потому, что Россия подписала Евроконвенцию по защите прав физически лиц»,— поясняет он.

Гендиректор компании «Индид» Алексей Баранов рассказал, что многие из технологий, которые необходимы для соответствия GDPR, уже есть в инфраструктуре российских компаний. К таким технологиям относятся шифрование почтовых сообщений на смартфонах и дисков ноутбуков, аутентификация сотрудников в офисе должна осуществляться по биометрии или смарт-карте, а при удаленном доступе она должна быть многофакторной (одноразовые пароли, SMS, брелоки).

«Многие вещи, которые от компании требует GDPR, будут полезны и в России. Наши реалии таковы, что все больше информационных систем мы будем использовать, все больше данных там хранить. Они становятся очень важным активом, и нам их нужно лучше защищать»,— подчеркнул господин Баранов. ■