GDPR. Нужно ли его выполнять в России?

Издание: Хабрахабр, 30 мая 2018 г.

Спикер: Алиса Горинова, старший консультант департамента консалтинга и аудита компании «Информзащита»

Что такое GDPR?

25 мая 2018 года вступил в силу Общий регламент по защите персональных данных Европейского союза (англ. General Data Protection Regulation, GDPR; далее – GDPR, Регламент). Многие считают, что GDPR распространяется только на европейские организации или компании, обрабатывающие персональные данные (ПДн) на территории Европейского союза. Но на самом деле Регламент является экстерриториальным и распространяется на организации, не находящиеся на территории Евросоюза.

В Регламенте, как и в Федеральном законе Российской Федерации №152-ФЗ «О персональных данных», используются понятия и подходы, сформулированные в Конвенции о защите физических лиц при автоматизированной обработке персональных данных.
Основной упор в Регламенте идет на защиту прав и свобод физических лиц при обработке их персональных данных.

Российские организации, попадающие под действие GDPR, оказываются «меж двух огней»: им требуется соответствовать как российскому законодательству, так и новому европейскому Регламенту. В этой статье мы постараемся раскрыть, кому в России нужно выполнять требования GDPR, зачем, и какие могут быть последствия их невыполнения.

На кого распространяется GDPR?

Согласно статье 3 Регламента, GDPR распространяется на:

1. Обработку ПДн в ходе деятельности оператора, либо обработчика (лица, которому оператор поручил обработку ПДн) на территории Европейского Союза (ЕС), вне зависимости от того, где производится обработка – на территории ЕС или за её пределами.

2. Обработку ПДн оператором или обработчиком, находящимся за пределами территории ЕС, если обработка связана с:

a. предложением товаров или услуг (платных или бесплатных) субъектам ПДн, находящимся на территории ЕС;

b. мониторингом действий (поведения, активности) субъектов ПДн на территории ЕС.

3. Обработку ПДн оператором, находящимся за пределами территории ЕС, если к нему применимо законодательство страны-члена ЕС в соответствии с международным публичным правом.

Если с операторами, очевидно попадающими под пункт 1 (нужно находиться на территории ЕС) и пункт 3 (дипломатические миссии и консульства стран-членов ЕС) всё более-менее ясно, то пункт 2 вызывает много вопросов, поскольку именно он определяет применимость GDPR к российским компаниям.

Для того, чтобы найти ответы на эти вопросы, помимо основного текста Регламента стоит также обратить внимание на то, что у GDPR есть преамбула, в которой раскрывается, чем руководствовался законодатель при установлении в GDPR описанных норм. В том числе в пункте 23 преамбулы говорится о том, как нам определить, что оператор (либо обработчик данных) предлагает товары или услуги лицам, находящимся на территории ЕС. Факторами, позволяющими установить направленность деятельности на территорию ЕС может считаться использование при предложении и продаже товаров или услуг **языка** либо **валюты** государства-члена ЕС, упоминание клиентов или пользователей, находящихся на территории ЕС. А в пункте 24 преамбулы говорится, что под мониторингом действий субъекта ПДн подразумевается отслеживание пользователей сети Интернет, включая возможное последующее создание профилей физических лиц, в частности, с целью анализа либо прогнозирования предпочтений, поведения и т.п.

При этом в статье 2 GDPR указано, что **Регламент не применяется к деятельности, не попадающей под действие законодательства ЕС.**

Из вышеуказанного можно определить следующие критерии непосредственной применимости GDPR к российской организации:

1. Организация находится на территории ЕС (является филиалом или представительством российской компании).
2. Организация не находится на территории ЕС, но осуществляет деятельность физически на территории ЕС, и эта деятельность включает в себя обработку ПДн (к примеру, транспортная компания с доставкой грузов из России физическим лицам в ЕС).
3. Организация систематически предлагает товары с доставкой в ЕС с возможностью оплаты в евро (польских злотых, шведских кронах и т.п.).
4. Организация предлагает услуги физическим лицам на одном из официальных языков ЕС, есть сайт на таком языке. Для оплаты услуг можно использовать валюту стран ЕС либо оплата не требуется.
5. Организация собирает и анализирует информацию о посетителях сайтов с территории ЕС, а результаты анализа использует самостоятельно либо продает (передает) иным лицам.

На организации, попадающие под пункты 2-5, GDPR действует в том объеме, в котором производится обработка ПДн лиц, находящихся на территории ЕС.

К примеру, обработка ПДн в рамках кадрового учета, если все сотрудники организации работают на территории России, не попадает под регулирование GDPR, а указанные в критериях бизнес-процессы – попадают.
Организации, обрабатывающие ПДн по поручению оператора, являющегося субъектом регулирования GDPR, попадают под действие GDPR в объеме, зависящем от того, какая часть обработки передана по поручению. Если организация осуществляет часть процессов обработки (к примеру, сбор ПДн, анализ ПДн и т.п.), она попадает под действие GDPR. Если организация предоставляет услуги хостинга (ЦОД), на неё непосредственно распространяются только те требования GDPR, которые к ней предъявит оператор.

Также мы хотим обратить внимание, что следующие случаи, часто встречающиеся в материалах про GDPR, не являются критериями применимости Регламента:

1. Гражданство субъектов ПДн не влияет на применимость GDPR (к примеру, наличие работников-граждан стран ЕС не означает, что организация попадает под GDPR);
2. Доступность веб-сайта организации на территории ЕС не означает автоматическую применимость GDPR. Если организация не осуществляет профилирование, и собираемая статистика не привязывается к конкретным пользователям, её деятельность не должна попадать под GDPR.
3. Если оказание услуги осуществляется вне пределов ЕС (например, номер в гостинице, находящейся в России, можно забронировать удаленно с территории ЕС), организация не должна попадать под действие GDPR, поскольку ее деятельность не осуществляется на территории ЕС и не попадает под действие законодательства ЕС.

В случае, если у Вас остались сомнения о применимости Регламента к вашей организации, Вы можете обратиться в ЗАО НИП «Информзащита», и мы поможем вам определить, как и какие требования GDPR вашей организации нужно соблюдать.

Контроль за соблюдением GDPR в России и последствия невыполнения требований

В целях защиты прав субъектов ПДн в каждой из стран ЕС созданы государственные органы по защите прав субъектов ПДн (в тексте Регламента – Supervisory Authorities, в общей практике такие органы называются Data Protection Authorities (DPA)). В числе прочих, DPA наделены согласно ч.1 ст.58 GDPR следующими полномочиями:

- запрашивать любую информацию, касающуюся обработки ПДн;
- проводить аудиты защищенности ПДн;
- получать от оператора и обработчика доступ ко всем ПДн и ко всей информации, необходимой для выполнения своих задач;
- получать доступ к любым помещениям оператора и обработчика, в том числе к любому оборудованию и средствам обработки данных.

Конкретные процедуры контроля устанавливаются странами ЕС самостоятельно. При выявлении нарушений положений Регламента DPA, в числе прочего, согласно ч.2 ст.58 GDPR могут:

- выдать предупреждение либо замечание оператору или обработчику о том, что текущий порядок обработки ПДн нарушает положения Регламента;
- выдать предписание о необходимости выполнения запроса субъекта, о необходимости информирования субъекта о нарушении безопасности ПДн;
- потребовать привести операции по обработке ПДн в соответствие с Регламентом в определенный срок;
- наложить временное или постоянное **ограничение на обработку**, включая **запрет на обработку;**
- выдать предписание об удалении либо уточнении ПДн;
- **наложить административный штраф** вместе с иными мерами либо вместо них;
- потребовать **прекратить передачу ПДн в третью страну** либо в международную организацию.

Регламентом устанавливается необходимость для организаций, расположенных вне ЕС, назначить представителя в ЕС, через которого будет осуществляться взаимодействие DPA с организацией, но при этом подчеркивается, что ответственность за обработку ПДн несет не представитель, а сама организация.

GDPR не раскрывает процедуру контроля за соблюдением Регламента организациями, расположенными вне ЕС и не назначившими представителя, а также каким образом организации, расположенные вне ЕС, будут нести ответственность за нарушения правил обработки ПДн.

Мы провели с DPA стран ЕС ряд интервью по вопросам контроля за соблюдением GDPR вне ЕС. Ответы были различными, но в целом ясности не появилось. Один из представителей DPA сделал оговорку, что такие случаи будут регулироваться во взаимодействии с DPA стран нахождения оператора либо обработчика. Сегодняшняя геополитическая ситуация и позиция руководителя Роскомнадзора А. Жарова по вопросу необходимости соответствия российских организаций GDPR вносят некоторые сомнения, что попытки такой кооперации DPA стран ЕС с Роскомнадзором будут продуктивны.

Хочется обратить внимание, что указанные в GDPR многомиллионные штрафы, которыми больше всего пугают операторов – это верхняя планка. GDPR говорит о том, что налагаемые штрафы (и иные санкции) должны быть соразмерны нарушению, эффективны и предупреждающими повторные нарушения. Конкретные размеры штрафов будут определяться индивидуально, с учетом большого количества факторов. Многомиллионный штраф может быть наложен на организацию в том случае, если она сознательно и злостно нарушала права субъектов, тщательно это скрывая и получая от такой обработки ПДн высокую прибыль.

Наиболее вероятным (но не единственным) и существенным последствием невыполнения GDPR для российских организаций, не имеющих представительств либо дочерних организаций на территории ЕС (а также назначенного представителя по вопросам обработки ПДн), является не штраф, а блокирование сайта организации на территории ЕС либо отдельных государств-членов ЕС. Несмотря на то, что возможность блокирования сайта не прописана напрямую в GDPR, она представляется закономерным способом ограничения обработки ПДн в целях предупреждения повторных нарушений, в особенности при отсутствии иных возможностей влияния на оператора.

Зачем российским организациям соответствовать GDPR?

Выполнение GDPR имеет и иные преимущества для организаций помимо очевидной возможности избежать возможных санкций со стороны DPA ЕС.

Прежде всего это повышение общего уровня ИБ и управления данными в организации. Зачастую в процессе приведения к соответствию требованиям по защите ПДн организация впервые создает реестр существующих у нее бизнес-процессов, понимает имеющиеся потоки данных, создает схему сети, описывает существующую систему защиты информации. Эти действия становятся фундаментом для защиты не только ПДн, но и иных видов конфиденциальной информации, а также для оптимизации бизнес-процессов.

Если организация обрабатывает ПДн, переданные ей контрагентом, попадающим под действия GDPR, контрагент будет требовать от нее соответствия требованиям GDPR, предъявляемым к обработчикам ПДн. Соответствие GDPR позволит сервис-провайдеру расширить доступный рынок предоставления услуг на территорию ЕС, а также предоставлять услуги тем российским организациям, которые попадают под требования GDPR.

Требование об обязательном соответствии GDPR может исходить от головной компании при применимости GDPR к организациям группы компаний, с которыми российская организация обменивается ПДн. Но в таком случае целесообразно, во-первых, уточнить, действительно ли обрабатываются ПДн лиц, находящихся на территории ЕС, а во-вторых, если они обрабатываются, распространять требования Регламента на те процессы, в которых производится обработка таких ПДн, а не на всю организацию.

GDPR устанавливает необходимость соблюдения многочисленных прав субъектов ПДн и обеспечения прозрачности обработки ПДн для субъектов. По сравнению с ФЗ «О персональных данных» GDPR более подробно разъясняет, как информировать субъектов ПДн об обработке их ПДн, а также о том, как они могут реализовывать свои права в отношении этой обработки.

Отражение этих вопросов обработки ПДн в Политике обработки ПДн, а также при сборе информации об обработке ПДн, позволяет повысить прозрачность деятельности организации и обеспечить большее доверие со стороны всех субъектов ПДн.

Резюме

Если ваша организация расположена в России – это ещё не значит, что GDPR к ней не применим. Проверить применимость требований Регламента к вашей организации можно с помощью указанных выше критериев.

Регламент вступил в силу только что, и по данным компании Symantec 80% организаций в ЕС не соответствуют требованиям GDPR. Каким образом к российской организации в связи с нарушениями GDPR могут быть применены санкции со стороны ЕС, пока неясно, но тем не менее, к Регламенту стоит относиться серьезно.

В завершение хотим отметить, что с большой вероятностью в скором времени для единообразия с европейским законодательством в российском законодательстве об обработке ПДн появятся формулировки, схожие с требованиями GDPR.

Автор: Алиса Горинова, старший консультант департамента консалтинга и аудита компании «Информзащита». Если у вас остались вопросы, мы готовы с вами пообщаться. Ждем ваших писем на адрес a.gorinova@infosec.ru.

Подробнее: https://habr.com/company/infosecurity/blog/412729/