Специальный юридический вестник март 2018

Выпуск № 03/SLA

Экстерриториальные правила защиты персональных данных ЕС (GDPR)

Уважаемые друзья,

В связи с вступлением в силу в мае 2018 года Экстерриториальных правил защиты персональных данных ЕС (англ. General Data Protection Regulation (Regulation (EU) 2016/679), далее – «GDPR» или «Правила»), компании, осуществляющие деятельность за пределами ЕС, уже сейчас задаются вопросами применимости к ним положений GDPR.

GDPR потенциально могут иметь последствия для компаний за пределами ЕС

В каких случаях GDPR применяются к компаниям, находящимся за пределами ЕС?

Прежде всего нужно отметить, что положения Правил применяются к обработке персональных данных в контексте деятельности, осуществляемой учреждением собственника или оператора персональных данных[1], расположенного на территории ЕС, вне зависимости от того, производится ли обработка персональных данных в ЕС, или за его пределами[2]. Применимость GDPR в данном случае возможна в отношении штаб-квартир компаний, расположенных за пределами ЕС, осуществляющих обработку персональных данных работников их филиалов в ЕС, а также в отношении технических средств обработки, находящихся вне ЕС.

Также, положения GDPR применяются к обработке персональных данных субъектов, которые находятся на территории ЕС [3] - (далее – «СПД»), собственником или оператором, располагающимся вне территории ЕС, при условии, что обработка связана с:

1. Предложением товаров или услуг СПД (как на платной, так и на бесплатной основе) (далее – «Критерий 1»)

или

2. «Мониторингом поведения» СПД, осуществляемого на территории ЕС (далее – «Критерий 2»).

GDPR предусматривает наложение штрафов даже на компании, зарегистрированные вне ЕС, в случае их нарушения, в размере до 4% от ежегодной мировой прибыли нарушителя или 20 миллионов евро, в зависимости от того, какая величина больше.

Какие действия могут быть квалифицированы как «Предложение товаров или услуг» СПД?

При условии, что собственник/оператор персональных данных и СПД могут территориально располагаться в разных местах, предложение товаров или услуг, скорее всего, будет осуществляться в электронном виде.

Ключевым аспектом при определении применимости Критерия 1 является факт намерения предложить товары или услуги СПД. Преамбула GDPR (Recitals) содержит комментарии касательно «очевидности» факта предложения собственником/оператором товаров или услуг СПД в одной или нескольких странах-членах ЕС. Доказательство намерения маловероятно, к примеру, в случае наличия простого доступа к официальному веб-сайту собственника / оператора.

Однако, соответствие Критерию 1 возможно при условии, что:

- официальный веб-сайт доступен на одном из официальных языков ЕС, не являющемся официальным языком страны -

---

[1] *GDPR закреплены дефиниции терминов «собственник» (data controller) и «оператор» (data processor) персональных данных. Первыми являются лица (включая государственные органы), самостоятельно или совместно с другими лицами, определяющие цель и средства обработки персональных данных; последними – лица (включая государственные органы), проводящие обработку персональных данных от имени собственника.*

[2] *Статья 3.1 GDPR.*

[3] *Статья 3.2 GDPR.*

учреждения такой компании, и существует возможность оформления заказов товаров/услуг на таком языке; и
- на веб-сайте цены предлагаемых товаров/услуг указаны в национальной валюте страны-члена ЕС; а также
- веб-сайт прямо упоминает заказчиков или пользователей, располагающихся в ЕС.

Что означает «Мониторинг поведения»?

Преамбула GDPR (Recitals) устанавливает, что в целях определения, является ли деятельность по обработке «мониторингом поведения» СПД, необходимо установить, отслеживаются ли действия физических лиц в интернете, включая потенциальное использование в дальнейшем техник обработки персональных данных посредством отслеживания профиля физического лица, в целях принятия решений в отношении данного лица или в целях проведения анализа или прогнозирования персональных предпочтений, поведения и отношения данного лица.

Представляется, что:

- использование cookies для отслеживания общей онлайн-активности пользователей, находящихся в ЕС, на их официальных веб-сайтах[4], а также
- осуществление сбора информации об IP адресах пользователей, в частности, со сбором иных данных, которые вместе с IP адресами, могут идентифицировать пользователей, посещающих их официальные вебсайты (при соблюдении определенных условий, установленных в Правилах)

вероятнее всего, будут признаваться как «поведенческий мониторинг» СПД.

Ввиду положений Преамбулы, упомянутых выше, ясно, что для применения GDPR к компаниям, расположенным вне ЕС, требуется элемент намеренного мониторинга. Применение Правил в отношении ненамеренного сбора без последующего профилирования маловероятно.

Представители по вопросам защиты персональных данных

Во многих случаях, компании, расположенные вне ЕС, к которым применяются GDPR, будут иметь обязательства по назначению представителя в ЕС. Однако, назначение такого представителя требуется лишь в одной стране-члене ЕС, в которой располагаются СПД, чьи персональные данные обрабатываются в связи с предложением таким СПД товаров/услуг, или те СПД, которые подверглись поведенческому мониторингу.

Санкции

Существенные штрафы, в размере 4% от ежегодной мировой прибыли нарушителя или 20 миллионов евро, в зависимости от того, какая величина больше, могут быть наложены на компании, не соблюдающие положения GDPR.

Однако, несмотря на значительные размеры штрафов и экстерриториальное применение Правил, последние не содержат списка конкретных механизмов привлечения нарушителей норм GDPR, зарегистрированных вне территории ЕС, к ответственности.

---

[4] Согласно судебной практике ЕС, информация о просмотрах пользователем страниц и другом использовании интернета может классифицироваться в качестве персональных данных.

Очевидно, что практическая реализация данной части GDPR возможна только в рамках межгосударственного сотрудничества.

В 2015 году Казахстан и ЕС заключили Соглашение о расширенном партнерстве и сотрудничестве (далее – «Соглашение»), согласно которому стороны несут соответствующие обязательства для обеспечения высокого уровня защиты персональных данных посредством обмена передовым опытом и практикой.[5] Полагаем, что вместе с присоединением Казахстана к Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных[6] и к Дополнительному протоколу к ней, будет создана база для взаимодействия органов и обеспечения соблюдения норм GDPR.

Важность проведения анализа политик по соблюдению законодательства в области персональных данных

В то время как действующий в Казахстане Закон о персональных данных и их защите в основном преследует общие с GDPR принципы обеспечения защиты персональных данных, в последнем случае, однако, соответствующие процессы урегулированы в меньшей степени и определены нечетко (в части обязательства о назначении лица, ответственного за защиту персональных данных, анонимности/шифрования или других способов защиты персональных данных (при трансграничной передаче) и т.д).

В свете Правил, если компания имеет каких-либо клиентов в ЕС, она должна будет обеспечить соблюдение положений GDPR в отношении всей клиентской базы, или обеспечить возможность идентификации резидентов ЕС среди своих клиентов, в целях обеспечения соблюдения положений Правил в отношении лишь данной группы клиентов. В зависимости от размера клиентской базы, разработка и поддержка двух параллельных систем и политик в отношении резидентов ЕС и нерезидентов ЕС может представляться непрактичной и потребовать больших расходов, в то время как неправильная классификация клиента может повлечь существенные санкции. Разработка системы, соответствующей положениям Правил, а также локальным законодательным требованиям, представляется оптимальным решением. Компании должны обеспечить понимание руководящими работниками последствий применения норм Правил и необходимости проведения анализа стандартных договоров, внутренних политик и процедур в области защиты персональных данных, включая трудовые политики, политики по вопросам информационных технологий, и другие регламенты, касающиеся отдельных клиентов на соответствие как положениям GDPR, так и нормам Закона о персональных данных и их защите.

---

[5] Статья 237 Соглашения о расширенном партнерстве и сотрудничестве между Европейским Союзом и его государствами-членами, с одной стороны, и Республикой Казахстан, с другой стороны (Астана, 21 декабря 2015 года)
[6] Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.; CETS # 108)

Соответствует ли ваша компания требованиям в области защиты персональных данных?

B

- Сбор какого рода персональных данных осуществляет ваша компания? В какой юрисдикции находятся субъекты персональных данных?
- Проводятся ли на периодичной основе внутренние и независимые проверки документов компании на предмет соблюдения законодательства в сфере защиты персональных данных?

D

- Определены ли роли и задачи в сфере защиты персональных данных ответственных работников вашей компании?
- Был ли проведен юридический анализ рисков, связанных с соблюдением вашей компанией положений GDPR?

A

- Позволяют ли внутренние процессы вашей компании, быстро и эффективно реагировать на нарушения в области защиты персональных данных?

C

- Производится ли мониторинг законодательства на предмет важных изменений в сфере защиты персональных данных?

Как «Делойт» может помочь

Команда «Делойт Лигал» будет рада предоставить более подробные консультации по любым вопросам, возникшим у вас после ознакомления с данным вестником. Контакты основных членов команды указаны ниже.

Члены команды «Делойт Лигал» будут рады оказать вам юридические консультационные услуги в сфере защиты персональных данных, включающие:

01 Правовой обзор соблюдения компанией норм в области защиты персональных данных

02 Подготовка дорожной карты в целях соответствия требованиям по защите персональных данных

03 Подготовка политик по соблюдению законодательства в сфере защиты персональных данных

04 Юридический консалтинг по вопросам защиты персональных данных

- Специальный юридический вестник — представляет собой обзор последних значимых нововведений и дополнений в различные нормативно-правовые акты Казахстана. «Делойт» не принимает на себя обязательств или ответственности за использование информации, содержащейся в Специальном юридическом вестнике.
- Информация, содержащаяся в Специальном юридическом вестнике, содержит комментарии и выводы, основанные исключительно на информации, полученной из открытых источников.
- Несмотря на то, что в Специальном юридическом вестнике затрагиваются отдельные аспекты правового характера, Специальный юридический вестник не является юридическим заключением по вопросам, рассмотренным в нем.
- Целью Специального юридического вестника является предоставление тематической информации общего характера. «Делойт» не принимает управленческих решений за лиц, ознакомившихся со Специальным юридическим вестником, а также не несет ответственности за решения, принятые на основании представленных в Специальном юридическом вестнике данных. Наши выводы носят исключительно информационный характер. Лица, ознакомившиеся со Специальным юридическим вестником, самостоятельно несут ответственность за принятие решений о внедрении или отказе от внедрения рекомендаций и консультаций, если таковые содержатся в Специальном юридическом вестнике.

Свяжитесь с нами:

Алматы/Астана

Агайша Ибрашева
Тел.: +7(727) 258 13 40
Факс: +7(727) 258 13 41
Email: aibrasheva@deloitte.kz

Виктория Тян
Тел.: +7(727) 258 13 40
Факс: +7(727) 258 13 41
Email: vtyan@deloitte.kz

Кэролайн Армитаж
Тел.: +7(727) 258 13 40
Факс: +7(727) 258 13 41
Email: carmitage@deloitte.kz

deloitte.kz