Новое в европейском законодательстве о персональных данных: риски и рекомендации для российского бизнеса

ИЮЛЬ 2017

VEGAS LEX

Весной 2016 года в рамках Европейского союза (далее – "ЕС") завершилась глобальная реформа законодательства о персональных данных (далее – ПД). Результатом реформы стало принятие Регламента ЕС № 2016/679 "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных" (далее – Регламент), который вступает в силу в мае 2018 года. Ключевой целью реформирования стала необходимость унификации регулирования персональных данных в рамках ЕС, что позволит добиться единого подхода во всех странах-участницах ЕС и обеспечить беспрепятственное и эффективное взаимодействие европейских операторов ПД между собой.

Нововведения ЕС в сфере ПД породили ряд последствий, в том числе финансового характера, выражающиеся в возможных штрафах вплоть до 20 млн евро или 4% от мирового годового оборота за финансовый год. Такие последствия применимы не только к европейским компаниям, но и к российским, обрабатывающими ПД европейских граждан. Положения Регламента, ставшие поводом для беспокойства, потенциальные риски и практические рекомендации бизнесу подробно обозначены в данном аналитическом обзоре.

I. На кого распространяются требования нового Регламента

1. **Организации, учрежденные в ЕС (резиденты ЕС).**

2. **Организации, учрежденные вне ЕС (нерезиденты ЕС),** но обрабатывающие ПД граждан ЕС. К таким организациям могут относиться компании из третьих стран (не членов ЕС), реализующие товары/услуги европейским гражданам. Сюда включаются, например, онлайн-сервисы, интернет-магазины, социальные сети, дата-центры. Согласно официальным комментариям к Регламенту, обязанность соответствовать положениям Регламента возникает также и у компаний-нерезидентов, которые: 1) используют официальный язык страны-участницы ЕС как в рамках описания товаров/услуг, так и при оформлении заказов, 2) используют валюту страны-участницы ЕС при расчетах с клиентами и 3) непосредственно указали на сайте, что товары/услуги предлагаются гражданам ЕС.

3. **Организации, собирающие и обрабатывающие ПД в рамках мониторинга поведения граждан ЕС.**

Таким образом, Регламент распространяет свое действие не только на резидентов ЕС, но и на организации, включая российские, обрабатывающие ПД европейских граждан.

II. Новые правила Регламента и штрафные санкции

Ввиду того, что Регламент носит экстерриториальный характер, российским компаниям, осуществляющим обработку ПД европейских граждан, необходимо будет соответствовать ряду новых требований. Особое внимание следует уделить значительному расширению ответственности за несоответствие нормам в области защиты ПД. Так, Регламент ввел высокий размер штрафов вплоть до 20 млн евро или до 4% от глобального годового оборота за предыдущий финансовый год (в зависимости от того, какая сумма больше). В то же время стоит отметить, что надзорный орган может ограничиться выговором в адрес нарушителя в случае, если характер нарушения незначительный и не влечет за собой угрозу защите персональных данных граждан.

III. Ключевые бизнес-рекомендации

1. **Ограничение деятельности по сбору ПД европейских граждан.**

Российская компания при осуществлении сбора ПД граждан Европейского Союза обязана руководствоваться положениями Регламента. Чтобы избежать необходимости соблюдения нового Регламента, следует ограничить сбор и обработку ПД ев-

ропейских граждан, полностью исключив эти действия с ПД к 2018 году.

2. Принятие ряда дополнительных организационно-управленческих и технических мер.

Если компания не готова отказаться от сбора и обработки ПД граждан ЕС, то в таком случае рекомендовано поэтапно провести ряд мер по обеспечению соответствия процессов обработки данных требованиям Регламента, а именно:

- Создание рабочей группы, с включением в нее специалистов из отделов IT, HR (если компания обрабатывает ПД европейских экспатов в рамках трудовых отношений), юридического департамента и представителей отделов, ответственных за обработку ПД в компании.

- Аудит процессов сбора и обработки ПД в компании. Цель данного этапа – определение применимости положений Регламента к деятельности компании и выявление потенциальных рисков. В рамках аудита необходимо четко определить:

  - круг ПД, обрабатываемых компанией, и установление факта использования при этом иностранных серверов;
  - круг субъектов, чьи ПД обрабатываются компанией (есть ли среди ПД данные европейцев);
  - механизмы защиты ПД, имеющиеся у компании, включая технические меры безопасности (например, порядок шифрования);
  - круг внутренних актов, регулирующих процессы сбора и обработки ПД.

- Усовершенствование процессов сбора ПД и соответствующей внутренней документации. На данном этапе необходимо внедрить дополнительные меры безопасности, назначить необходимых должностных лиц и утвердить дополнительные внутренние акты компании в сфере защиты ПД либо обновить уже существующие.

- Взаимодействие с подрядчиками. Рекомендуется проанализировать текущие договорные взаимоотношения с партнерами, обрабатывающими ПД европейских граждан от имени компании (либо от своего имени, но в интересах компании). На данном этапе рекомендуется внести в договоры соответствующие положения о разграничении ответственности при обработке ПД граждан ЕС, а также установить дополнительные гарантии соблюдения норм Регламента на взаимной основе.

Ниже приведем таблицу, содержащую новые требования, штрафные санкции за несоответствие и рекомендации. За повторное нарушение повторно налагаются штрафные санкции в размере до 4% от мирового годового оборота за последний финансовый год либо до 20 млн евро.

№ п/п	Статья Регламента	Требования	Санкции за несоответствие	Рекомендации
1	ст. 27	Назначение представителя в ЕС, отвечающего за обработку ПД европейских граждан.	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро.	Представителем в ЕС может быть как сотрудник компании, трудоустроенный в филиале компании, так и независимый консультант, располагающийся в ЕС. Разработать внутрикорпоративное положение о Представителе в ЕС по вопросам защиты ПД.

2	ч. 3 ст. 7	Способ отзыва согласия субъекта на обработку ПД должен быть идентичен способу его предоставления.	До 4% от мирового годового оборота за последний финансовый год либо до 20 млн евро.	Обеспечить техническую возможность отзыва согласия субъектом ПД аналогично способу, которым такое согласие было получено.
3	ст. 5 ст. 6	Получение отдельного согласия субъекта на обработку ПД в отношении каждой отдельной цели сбора и обработки ПД.	До 4% от мирового годового оборота за последний финансовый год либо до 20 млн евро.	Пересмотреть формы текущих согласий на обработку ПД, тематически разграничив текст согласия в зависимости от целей сбора. Например, онлайн-магазин собирает ПД для 1) направления товара заказчику, 2) для рассылки рекламной информации и 3) сбора статистической информации. Каждая цель сбора ПД должна быть отдельно поименована в согласии с указанием корреспондирующего ей набора обрабатываемых ПД.
4	ст. 34	Незамедлительное уведомление субъекта ПД об утечке данных.	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро.	Дополнить текущие Политики обработки ПД разделом, посвященным порядку уведомления субъекта ПД в случаях утечки данных, либо разработать отдельный внутренний регламент.
5	ст. 13 ст. 14	Обязанность предоставить по запросу субъекта ПД информацию об операторе, целях обработки ПД, сроках хранения ПД и категории получателей ПД.	До 4% от мирового годового оборота за последний финансовый год либо до 20 млн евро.	Дополнить текущие Политики обработки ПД положениями о правах субъекта на получение указанной информации с указанием сроков предоставления, а также разработать внутренний акт, определяющий алгоритм обработки запроса субъекта и дальнейших действий.
6	ст. 16 ст. 17 ст. 18	Незамедлительное изменение, удаление или ограничение пользования ПД по запросу субъекта.	До 4% от мирового годового оборота за последний финансовый год либо до 20 млн евро.	Дополнить текущие Политики обработки ПД положениями о правах субъекта на изменение, удаление и ограничение пользования своими данными с указанием сроков выполнения запроса. Разработать внутренний акт, определяющий алгоритм обработки такого рода запросов и дальнейших действий оператора ПД.

7	ст. 20	Передача ПД в структурированном машиночитаемом формате по запросу субъекта.	До 4% от мирового годового оборота за последний финансовый год либо до 20 млн евро.	Дополнить текущие Политики обработки ПД положениями о правах субъекта на получение своих данных в структурированном виде с указанием сроков выполнения запроса. Разработать внутренний акт, определяющий алгоритм обработки такого рода запросов и дальнейших действий оператора ПД.
8	ст. 49	Предоставление субъекту ПД полного описания рисков, связанных с трансграничной передачей его данных.	До 4% от мирового годового оборота за последний финансовый год либо до 20 млн евро.	Дополнить текущие формы согласий, содержащих возможность трансграничной передачи, описанием указанных рисков и методов их минимизации/устранения.
9	ст. 9	Сбор и обработка особых категорий ПД.	До 4% от мирового годового оборота за последний финансовый год либо до 20 млн евро.	Определить, осуществляется ли компанией сбор и обработка особых категорий данных. В случае положительного ответа следует либо исключить сбор особых категорий ПД, либо обеспечить наличие отдельных согласий субъектов на сбор и обработку таких категорий ПД.
10	ст. 30	Ведение письменного учета действий по обработке ПД.	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро.	Обеспечить ведение журнала учета действий с ПД граждан ЕС. Рекомендуется вести указанных журнал в электронном, машиночитаемом формате, отделив действия в отношении граждан РФ от действий в отношении европейских граждан.
11	ч. 5 ст. 33	Ведение реестра инцидентов в сфере ПД.	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро.	Обеспечить ведение журнала учета инцидентов в сфере ПД. Рекомендуется вести указанный журнал в электронном, машиночитаемом формате.
12	ст. 32	Внедрение процедуры регулярной проверки и оценки эффективности технических и организационных мер безопасности ПД.	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро.	Разработать и внедрить Положение о порядке проведения внутренних проверки и оценки эффективности мер безопасности обработки ПД, назначив ответственного.

13	ст. 32 ст. 35	Наличие задокументированной оценки потенциальных рисков при обработке ПД.	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро.	Провести полный анализ механизмов защиты ПД с целью выявления потенциальных рисков и принятия мер по их устранению/минимизации.
14	ст. 36	Предварительное консультирование с надзорным органом в случае негативной оценки рисков при обработке ПД.	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро.	Разработать Положение о взаимодействии с надзорным органом ЕС в сфере защиты ПД, в котором необходимо предусмотреть формат взаимодействия и определить, в каких случаях компания обязана консультироваться с органом.
15	ст. 33	Уведомление надзорного органа о любых инцидентах в сфере ПД.	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро.	Предусмотреть алгоритм подачи уведомления надзорному органу в разработанном Положении о взаимодействии с надзорным органом ЕС в сфере защиты ПД.
16	ст. 26	Наличие соглашения между лицами, осуществляющими совместную обработку ПД.	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро.	Пересмотреть текущие контракты с подрядчиками, обрабатывающими ПД, в том числе пункты об ответственности и гарантиях соблюдения правил Регламента. Рекомендуется проявлять осмотрительность при выборе новых подрядчиков в части соответствия их процессов требованиям Регламента.
17	ст. 58	Обязательное выполнение требований надзорного органа.	До 4% от мирового годового оборота за последний финансовый год либо до 20 млн евро.	Предусмотреть алгоритм выполнения требований надзорного органа в разработанном Положении о взаимодействии с надзорным органом ЕС в сфере защиты ПД.
18	ст. 37	Назначение инспектора по защите ПД	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро.	Инспектором может быть как сертифицированный сотрудник компании, так и сертифицированный независимый консультант. Инспектором может быть то же лицо, что Представитель в ЕС. Разработать и внедрить положение об Инспекторе по вопросам защиты ПД.

Контакты

АЛЕКСАНДРА ВАСЮХНОВА
Партнер, Руководитель Группы Технологий и Инвестиций
vasukhnova@vegaslex.ru

ТАТЬЯНА ДВЕНАДЦАТОВА
Юрист Группы международных проектов
dvenadtsatova@vegaslex.ru

СВЕТЛАНА ЖЕРДИНА
Юрист
Группы международных проектов
zherdina@vegaslex.ru

ВЯЧЕСЛАВ ЧМЫХОВ
Юрист
Коммерческой группы
chmykhov@vegaslex.ru