№ 33
АВГУСТ 2017
ЭЖ ЮРИСТ

РЕГЛАМЕНТ ЕС О ПЕРСОНАЛЬНЫХ ДАННЫХ

Пока российский бизнес привыкает к повышенным административным штрафам за нарушение законодательства в области персональных данных по ст. 13.11 Кодекса Российской Федерации об административных правонарушениях, Европейский союз готовится ввести в действие Регламент № 2016/679 «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (далее – Регламент). Особенностью Регламента является его экстерриториальность. Дело в том, что действие Регламента распространяется не только на резидентов ЕС, но и на третьих лиц. Крупным российским компаниям вряд ли удастся проигнорировать новые правила: штраф за их нарушение велик – до 20 млн евро, или 4% от мирового годового оборота за финансовый год. О том, как Регламент повлияет на российский бизнес, а также о том, как российскому бизнесу подготовиться к введению в действие Регламента и чем грозит его несоблюдение, пойдет речь в статье.

Светлана ЖЕРДИНА,
юрист Группы международных проектов,
юридическая фирма Vegas Lex,
г. Москва

Татьяна ДВЕНАДЦАТОВА,
юрист Группы международных проектов,
юридическая фирма Vegas Lex,
г. Москва

Вячеслав ЧМЫХОВ,
юрист Коммерческой группы,
юридическая фирма Vegas Lex,
г. Москва

Распространяется ли действие Регламента на вашу компанию?

Если в вашей компании обрабатываются персональные данные граждан ЕС, ответ на данный вопрос будет положительный.

Кроме того, согласно официальным комментариям к Регламенту компании-нерезиденты должны соблюдать положения Регламента, если они:

✓ используют официальный язык страны – участницы ЕС как в рамках описания товаров/услуг, так и при оформлении заказов;

✓ используют валюту страны – участницы ЕС при расчетах с клиентами;

✓ непосредственно указали на сайте, что товары/услуги предлагаются гражданам ЕС.

Требования Регламента. Все требования Регламента можно условно разделить на четыре основных типа требований:

– по учреждению должностей в компании;

– ведению внутренней документации;

– обеспечению прав и свобод граждан ЕС при обработке их персональных данных;

– взаимодействию с надзорными органами ЕС в сфере обработки персональных данных.

Далее кратко рассмотрим каждый из элементов выделенных типов требований.

Требования по учреждению новых должностей в компании. Первый тип требований связан с учреждением в компании должностей представителя в ЕС и инспектора по защите персональных данных. Санкции за отсутствие хотя бы одной из должностей в компании выражаются в возможных штрафах в размере до 10 млн евро, или 2% от мирового годового оборота за финансовый год.

Представитель компании в ЕС должен решать все вопросы, связанные с обработкой персональных данных европейских граждан. Он должен осуществлять взаимодействие как с субъектами персональных данных, так и с надзорными органами ЕС в сфере обработки персональных данных. Регламент предписывает, что представитель должен физически располагаться на территории ЕС. Представителя назначать не нужно, если обработка персональных данных носит случайный характер, не включает в себя масштабную обработку особых категорий персональных данных или масштабную обработку персональных данных, связанных с судимостями и уголовными преступлениями, а также обработку, которая предположительно не приведет к риску для прав и свобод физических лиц. Кроме того, органы государственной власти и правительственные учреждения также не обязаны назначать представителя в ЕС.

Инспектор по защите персональных данных (Data privacy officer) должен быть назначен в компании согласно ст. 37 Регламента. Инспектором может выступать как сотрудник компании, так и независимый консультант, действующий на основании заключенного договора об оказании услуг.

Основными функциями инспектора являются:

✓ информирование оператора относительно обязанностей, предусмотренных Регламентом;

✓ контроль за соблюдением оператором Регламента;

✓ контроль методов обработки персональных данных оператором;

✓ консультирование оператора относительно оценки воздействия на защиту персональных данных;

✓ взаимодействие с надзорными органами ЕС.

Стоит отдельно отметить, что Регламент не содержит требований для инспектора физически находиться на территории ЕС. Регламент также не запрещает объединять функции инспектора и представителя в одном лице.

Требования по ведению внутренней документации. Второй тип требований связан с необходимостью принятия и ведения в компании определенной внутренней документации. При этом документы должны быть составлены на языке одной из стран – участниц ЕС. Санкции за несоответствие хотя бы одному из указанных требований выражаются в возможных штрафах в размере до 10 млн евро, или 2% от мирового годового оборота за финансовый год (таблица 1).

Требования по обеспечению прав и свобод. Третий тип требований включает в себя обязанность оператора по обеспечению следующих основных прав субъектов:

✓ права на информацию;

✓ права на внесение и удаление персональной информации.

За несоответствие этим требованиям Регламента оператор может быть привлечен к ответственности в виде штрафа в размере до 4% от мирового годового оборота за последний финансовый год, или до 20 млн евро (таблица 2).

Взаимодействие с надзорными органами ЕС. Четвертый тип требований связан с обязанностью оператора взаимодействовать с надзорными государственными органами ЕС в сфере обработки персональных данных.

Краткое описание данного типа требований представлено в таблице 3.

Ключевые рекомендации российскому бизнесу. Для начала российским компаниям нужно определить, распространяется ли на них действие Регламента. Как отмечалось выше, Регламент содержит несколько случаев, когда операторам не нужно, например, назначать представителя в ЕС.

Если Регламент распространяет свое действие на компанию, пора приступать к активной подготовке, так как до вступления Регламента в силу остается меньше года (Регламент вступает в силу в мае 2018 года), а работы предстоит достаточно много.

Во-первых, следует провести аудит существующих в компании процессов сбора и обработки персональных данных и выявить потенциальные риски.

Во-вторых, нужно усовершенствовать процессы сбора персональных данных, назначить определенных Регламентом должностных лиц, а также принять необходимые локальные акты, касающиеся обработки персональных данных, либо доработать существующие локальные акты. Кроме того, рекомендуется проанализировать текущие договорные взаимоотношения с партнерами, обрабатывающими персональные данные европейских граждан от имени компании (либо от своего имени, но в интересах компании). В договоры предлагается внести положения о разграничении ответственности при обработке персональных данных граждан ЕС, а также установить дополнительные гарантии соблюдения норм Регламента на взаимной основе.

Таблица 1

№	Требование	Описание
1	Ведение письменного учета (реестра) действий по обработке персональных данных (далее также – ПД)	Статья 30 Регламента предписывает оператору вести письменный учет всех действий, связанных с обработкой ПД. Данное требование не распространяется на организации со штатом менее 250 человек
2	Ведение учета (реестра) инцидентов в сфере ПД	В соответствии со ст. 33 Регламента оператор должен документировать любые утечки ПД, в том числе все относящиеся к утечке факты, последствия такой утечки и принятые корректирующие меры
3	Наличие задокументированной оценки потенциальных рисков при обработке ПД	Статья 35 Регламента закрепляет обязанность оператора провести оценку воздействия предусмотренного процесса обработки ПД на защиту ПД. Такая оценка рисков призвана выявить основные угрозы правам субъектов и должна как минимум включать в себя: 1) систематическое описание предусмотренных процессов обработки данных и целей обработки; 2) оценку необходимости и пропорциональности обработки данных относительно целей; 3) оценку рисков для прав и свобод субъектов данных; 4) меры, предусмотренные для устранения рисков

Таблица 2

№	Категория прав субъектов	Описание и рекомендации
1	Право на информацию	Оператор обязан сообщить субъекту в момент сбора у него ПД в числе прочего следующую информацию: – идентификационную информацию и контактные данные оператора и при необходимости его представителя; – контактные данные инспектора по защите ПД; – цели обработки ПД, а также юридическое основание для обработки; – законные интересы, преследуемые оператором или третьей стороной (если применимо); – получателей или категории получателей ПД; – намерение оператора передать персональные данные в третью страну или международную организацию; – срок, в течение которого будут обрабатываться ПД, либо критерии для его определения; – наличие права на исправление, удаление и ограничение обработки ПД; – наличие права на доступ к своим ПД; – наличие права на возражение против обработки ПД; – наличие права на получение своих ПД в структурированном, универсальном и машиночитаемом формате; – наличие права на отзыв своего согласия; – наличие права подачи жалобы в надзорный орган
2	Право на внесение и удаление персональной информации	Оператор обязан выполнить, в частности, следующие требования субъекта: – незамедлительно внести изменения в неточные данные, относящиеся к субъекту; – незамедлительно удалить данные, относящиеся к субъекту («право на забвение»); – ограничить обработку данных, если применяется одно из условий: а) точность ПД оспаривается субъектом данных; б) обработка ПД является незаконной, но субъект данных возражает против удаления ПД и требует ограничить их использование; в) оператору больше не требуются ПД для целей обработки, но они требуются субъекту ПД для обоснования, исполнения или ведения защиты по судебным искам; – предоставить ПД в структурированном и машиночитаемом формате

Таблица 3

№	Требование	Описание и рекомендации	Санкции за нарушение (штраф)
1	Предварительное консультирование с надзорным органом ЕС	В соответствии со ст. 36 Регламента оператор обязан проконсультироваться с надзорным органом до начала обработки ПД, если проведенная им оценка воздействия предусмотренного процесса обработки ПД на защиту данных указывает на то, что обработка может привести к возникновению высокой степени риска при непринятии мер для его снижения. В целях реализации указанного требования рекомендовано разработать Положение о взаимодействии с надзорным органом ЕС, закрепляющее формат такого взаимодействия и перечень случаев, когда компания прибегает к такого рода консультациям	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро
2	Уведомление в адрес надзорного органа об инцидентах в сфере обработки ПД	В случае утечки ПД оператор незамедлительно и при наличии соответствующей возможности в течение 72 часов после того, как ему стало известно об утечке, должен уведомить об этом надзорный орган. Исключение составляют случаи, когда утечка ПД, вероятно, не приведет к риску для прав и свобод физических лиц. Если уведомление направлено в надзорный орган позже, в таком уведомлении необходимо указать причины задержки. Уведомление в обязательном порядке должно содержать следующую информацию: – описание характера утечки ПД, в том числе по возможности указание категорий и приблизительного количества субъектов ПД и категорий и приблизительного количества записей ПД; – фамилию и контактные данные инспектора по защите ПД; – описание возможных последствий утечки ПД; – описание принятых или планируемых контролером мер для устранения нарушения, в том числе в соответствующих случаях мер по смягчению возможного отрицательного воздействия данного нарушения. Инспектор обязан документировать любые утечки ПД, в том числе все относящиеся к утечке ПД факты, последствия такой утечки и принятые корректирующие меры. В целях реализации указанного требования рекомендовано в разработанном компанией положении о взаимодействии с надзорным органом ЕС прописать алгоритм подачи таких уведомлений	До 2% от мирового годового оборота за последний финансовый год либо до 10 млн евро
3	Обязательное выполнение требований надзорного органа ЕС в сфере защиты ПД	В соответствии со ст. 58 Регламента надзорный орган обладает следственными, корректирующими, разрешительными и консультативными полномочиями. Операторы обязаны строго соблюдать требования надзорного органа	До 4% от мирового годового оборота за последний финансовый год либо до 20 млн евро