YOU & PARTNERS

GREEN LIGHT CONSULT

international consulting & legal services

АЛЕРТ

Новые стандарты ЕС в сфере защиты персональных данных: чего ждать российскому бизнесу?

Москва | София | 2018

GREEN LIGHT CONSULT
international consulting & legal services

Новые стандарты ЕС в сфере защиты персональных данных: чего ждать российскому бизнесу?

1. Что такое General Data Protection Regulation (GDPR) и что изменилось с его принятием.

25 мая 2018 года вступает в силу новое регулирование ЕС в сфере защиты персональных данных - General Data Protection Regulation (GDPR). GDPR – это нормативный акт ЕС, имеющий статус регламента Европейского парламента и Совета Европейского Союза, далее в тексте - Регламент[1]. Его цель - повышение уровня защищенности персональных данных[2] на территории и, в некоторых случаях, - за пределами территории ЕС. В этой связи Регламент расширяет круг прав граждан в отношении их персональных данных, а также прав, обязанностей и ответственности лиц, оперирующих этими данными.

Регламент распространяет свое действие на всех лиц - субъектов персональных данных, независимо от их гражданства и постоянного места жительства, если они находятся на территории ЕС.

Регламент действует на территории всего Европейского Союза[3], а также, в отдельных случаях, за его пределами. Обязательства и ответственность, предусмотренные Регламентом, распространяются в первую очередь, на организации, учрежденные в ЕС, а также подразделения иностранных организаций, функционирующие в ЕС.

Оперирование персональными данными (ПД), подпадающее под действие Регламента, охватывает разнообразные действия, связанные с получением, обработкой, сохранением, передачей ПД, как для

Регламент имеет экстерриториальное действие, то есть его требования распространяются на организации, учрежденные и работающие исключительно за пределами ЕС.

[1] Полное наименование - Регламент N 2016/679 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)» (Принят в г. Брюсселе 27.04.2016)

[2] К персональным данным Регламент относит любую совокупность данных о человеке, которая позволяет идентифицировать его как личность, в том числе, в тех случаях, когда такая идентификация возможна на основе сопоставления разрозненных данных. К ПД относятся имя, дата рождения, персональный номер, данные документов, кредитных карт, почтовый адрес, адрес места жительства, электронный адрес, телефонный номер, фото и видео-материалы, сведения о поведении и действиях и т.п.

[3] Помимо стран ЕС, Регламент распространяет свое действие на страны ЕЭП, включая такие страны, как Исландия, Лихтенштейн и Норвегия. В данном материале для краткости будет использоваться только аббревиатура ЕС.

собственных целей, так и для целей передачи данных иным лицам, независимо от объема данных и размера организации. Так, например, любая компания, ведущая работу с клиентами - физическими лицами, находящимися в ЕС, либо с базами, содержащими данные европейских потребителей, оперирует ПД с точки зрения Регламента.

Регламент имеет прямое действие, т.е. может применяться независимо от имплементирующего национального законодательства, и предусматривает возможность применения к компаниям таких санкций, как запрет на обработку данных, а также штраф в размере до 4% годового оборота или 20 млн. евро.

Контроль за соблюдением Регламента и привлечение к ответственности за его нарушение будет осуществляться компетентными органами, действующими как на общеевропейском уровне, так и на уровне стран ЕС. На общеевропейском уровне компетентным судом по применению Регламента является Суд Европейского Союза (European Court of Justice).

2. Какие обязанности возлагает Регламент на лиц, оперирующих персональными данными?

Объем требований, устанавливаемых Регламентом, не одинаков для всех операторов ПД. На компании, которые, в частности, обрабатывают данные на профессиональной или систематической основе, имеют дело с большими объемами персональных данных, с данными, носящими особо конфиденциальный характер, либо данными, обработка которых может иметь правовые последствия для субъектов ПД, возлагаются дополнительные обязанности, связанные с подготовкой и ведением специализированной документации, а также назначением ответственных за GDPR должностных лиц.

Важно отметить, что Регламент содержит не столько конкретные указания по поводу того, какие действия необходимо предпринять, сколько устанавливает общие принципы защиты персональных данных, которыми следует руководствоваться. На их основе компании должны вырабатывать собственные решения в области защиты персональных данных. В этом процессе, помимо европейского законодательства и судебной практики, компаниям следует опираться на национальное законодательство.

GREEN LIGHT CONSULT
international consulting & legal services

Ниже приведены 10 ключевых принципов, предусмотренных Регламентом:

1. Обработка[4] персональных данных (ПД) должна осуществляться строго в соответствии с законом, в легитимных целях и на основе принципа **прозрачности для субъекта ПД**;
2. Допустимо собирать, обрабатывать и хранить лишь такой **минимум** ПД, который обоснован требованиями законодательства, либо необходимостью, вытекающей из защиты интересов организации, признаваемых легитимными;
3. Характер обрабатываемых ПД и их объем должны **соответствовать** данным целям; ПД, изначально собранные для одной цели, не могут использоваться для другой;
4. **Согласие** граждан на обработку персональных данных должно соответствовать ряду критериев, в том числе, быть информированным, конкретным и активным;
5. ПД должны **сохраняться** на протяжении минимально возможного срока, который должен быть обоснован в каждом отдельном случае требованиями закона, либо иными конкретными легитимными целями, после чего данные должны удаляться;
6. Компании обязуются **информировать** граждан об их правах в сфере защиты ПД, а также **выполнять требования** граждан, основанные на их правах в сфере ПД, например, об удалении ПД («право на забвение»);
7. Лицо, обрабатывающее ПД, носит ответственность за их сохранность, точность и **актуальность** и за последствия искажения и нарушения целостности данных;
8. Компании обязаны **уведомлять** надзорный орган, а также, в некоторых случаях, граждан об утечке, искажении, либо уничтожении их ПД в течение 72 часов с момента, когда им стало известно об утечке данных;
9. «**Профайлинг**»[5] - компания должна гарантировать, что решения, оказывающие влияние на права гражданина (например, решение об отказе в выдаче кредита), будут приниматься не автоматизированным способом, а с участием человека, а также обеспечить возможность обжалования таких решений;
10. **Маркетинг** – граждане должны иметь возможность отказаться от получения сообщений рекламного характера с использованием их ПД.

[4] В данном списке под «обработкой» данных понимаются как действия по контролю, так и по обработке данных в соответствии с терминологией Регламента

[5] Использование в процессе деятельности организация профиля лица как набора его ПД, которые используются для принятия решений

3. Чего ждать российскому бизнесу?

Регламент гласит, что деятельность лица, не учрежденного в ЕС, подпадает под действие Регламента, если она связана:

- с предложением товаров, работ или услуг субъектам данных, которые находятся в ЕС, либо
- с мониторингом поведенческой активности лиц, находящихся в ЕС.

Таким образом, в первую очередь нововведения затронут российские телекоммуникационные компании, а также любые иные компании, если они предлагают товары и услуги на территории ЕС, и оперируют персональными данными субъектов, находящихся в ЕС. Возникает закономерный вопрос о том, как определить, предлагает ли компания, не зарегистрированная в ЕС, товары и услуги в ЕС? Регламент содержит на этот счет следующие критерии:

- использование компанией в рамках предложения товаров и услуг языка и валюты одного или нескольких государств-членов ЕС;
- возможность заказа товаров, работ, услуг на данном языке;
- упоминание покупателей и пользователей, находящихся в ЕС.

Помимо соблюдения требований Регламента, операторы ПД, учрежденные за пределами ЕС, обязуются назначить своих представителей в Европейском Союзе, которые будут действовать от их лица по вопросам, связанным с защитой ПД, и являться связующим звеном между компаниями и органами власти, компетентными контролировать исполнение Регламента на территории ЕС.

Российским компаниям также следует обратить внимание на требования Регламента, связанные с передачей ПД из Европейского Союза в третьи страны. Такая передача может иметь место в случае внутрикорпоративного трансфера данных и требует тщательной проработки политик компании в данной области.

Филиалы, представительства, обособленные подразделения

Поскольку Регламент распространяет свое действие не только на самостоятельные юридические лица, но и на иные образования, «установившиеся» на территории ЕС,

GREEN LIGHT CONSULT
international consulting & legal services

под его действие также попадают подразделения иностранных компаний в Европейском Союзе, включая филиалы и представительства. Даже в тех случаях, когда эти подразделения не работают непосредственно с физическими лицами на территории ЕС, они, как минимум, неизбежно будут оперировать их данными в рамках различных ситуаций, связанных с деятельностью подразделения.

В качестве примера, такое оперирование ПД будет иметь место в рамках трудовых отношений, ведь даже в тех случаях, когда сотрудники подразделения являются гражданами России, на них будут распространяться все права, а на подразделение – обязанности и ответственность, предусмотренные Регламентом, поскольку для целей Регламента не имеет значения ни гражданство, ни резидентство лица в ЕС, а лишь его местонахождение.

В случае если у Вас появились дополнительные вопросы в отношении содержания настоящего Алерта, Вы можете связаться с нами.

С уважением, команда You & Partners и Green Light Consult

Контакты: тел.: +7 (499) 673 07 03, e-mail: info@youandpartners.ru

тел.: +359 (88) 472 19 88, e-mail: info@bglegal.org

GREEN LIGHT CONSULT
international consulting & legal services

Приложение 1. Чек-лист: соответствие деятельности компании требованиям GDPR

Для того, чтобы обезопасить себя от рисков нарушения GDPR, российским органам власти и компаниям следует проверить свою деятельность на соответствие следующим параметрам:

№	Вопрос	Да	Нет	Вероятно
1	Является ли лицо контролером?			
2	Является ли лицо обработчиком данных?			
3	Подпадает ли деятельность лица под исключения, предусмотренные GDPR (сфера расследования преступлений, общественный интерес, защита жизненно важных интересов субъекта, иное)?			
4	Оказывает ли лицо услуги лицам на территории ЕС или обрабатывает ли лицо иным образом данные лиц на территории ЕС?			
5	Содержат ли действующие контракты условия о передаче (обработке) данных лиц на территории ЕС?			
6	Уведомляются ли субъекты данных об обработке их данных, в какой форме?			
7	Определены ли сроки и цели хранения данных?			
8	Получено ли (и в какой форме) согласие на обработку данных такими лицами?			

9	Разработаны ли внутренние регламенты по защите данных?			
10	Необходимо ли лицу нанять Представителя в Евросоюзе?			
11	Есть ли необходимость назначения Инспектора по защите данных?			
12	Ведется ли и как ведется контролером или обрабатывающим лицом учет обработки данных?			
13	Предоставлено ли субъекту данных право на доступ к данных и их удаление (забвение)?			
14	Заключен ли между контролером и обработчиком данных договор на обработку данных?			
15	Используются ли различные средства маркировки для защиты данных?			
16	Разработана ли политика по уведомлению надзорного органа и субъектов данных в случае утечки данных?			
17	Какие еще организационные и процедурные меры необходимо предусмотреть?			