Информация для клиентов

Что должно содержать положение о защите персональных? Вышел проект разъяснений по вопросам прозрачности в соответствии с GDPR:

В конце прошлого года Рабочая группа по ст. 29 («Рабочая группа») распространила проект подробных разъяснений («Разъяснения») по вопросам прозрачности в соответствии с Генеральным регламентом ЕС о защите персональных данных, GDPR («Регламент о защите данных»), вступающим в силу в мае 2018 года. Данные Разъяснения, окончательный вариант которых будет подготовлен по завершении консультаций, содержат толкование Рабочей группы в отношении той обязательной информации, которая в целях соблюдения требований о прозрачности, должна быть предоставлена субъекту данных в виде положения о защите персональных данных или в иной форме.

Одно из прямых требований Регламента о защите данных касается порядка извещения предприятиями и организациями субъекта данных об использовании его персональных данных в момент сбора данных или получения согласия, обычно в виде положения или уведомления о защите персональных данных. Сделать все правильно на этом этапе крайне важно. Предприятиям и организациям потребуется внимательно изучить действующую редакцию своего положения о защите персональных данных и прочие материалы и рассмотреть вопрос о необходимости их корректировки не только в свете Регламента о защите данных, но также и для учета требований, изложенных в Разъяснениях, развивающих действующие положения Регламента о защите данных. Хотя Разъяснения не имеют обязательной силы, надзорные органы в сфере защиты данных могут с неодобрением отнестись к предприятиям и организациям, не соблюдающим без уважительной причины рекомендаций Разъяснений, в связи с тем, что представители всех органов ЕС в сфере защиты данных входят в Рабочую группу. Предприятия и организации, не соблюдающие обязанности в отношении информирования по Регламенту о защите данных, могут быть оштрафованы на

наибольшую из следующих сумм: сумму до 4% от глобального годового оборота или 20 млн евро.

РАЗЪЯСНЕНИЯ РАБОЧЕЙ ГРУППЫ

Во первых: какую информацию предприятия и организации должны включить в свое положение о защите персональных данных?

- *Данные о личности и контактную информацию организации, контролирующей данные/специалиста по защите персональных данных* (в соответствующих случаях[1]): это позволяет субъекту данных легко определить организацию, контролирующую данные, *а также, когда это возможно и целесообразно, должно быть указано несколько методов для связи с организацией, контролирующей данные (номер телефона, адрес электронной почты, почтовый адрес и т.д.).*
- *Цель и правовые основания для обработки данных*: компаниям следует указывать правовые основания для обработки данных вместе с указанием цели обработки данных. В Разъяснениях не оговаривается, должно ли в положении о защите персональных данных быть указано правовое основание для обработки каждой категории данных (имена, номера телефонов, адреса электронной почты и т.д.).
- *Законные интересы*: если правовым основанием обработки данных организацией, контролирующей данные, или третьим лицом является необходимость соблюдения законных интересов, то конкретные законные интересы следует изложить субъекту данных понятным языком. В качестве передовой практики предприятиям и организациям также следует рассмотреть вопрос о предоставлении субъекту данных информации о том, как организация, контролирующая данные, поддерживает баланс своих собственных интересов с интересами субъекта данных. Предприятиям и организациям следует внимательно отнестись к реализации данного требования на практике. Краткое изложение «критерия соблюдения баланса» доступным языком может показаться непростой задачей, но в случаях где это целесообразно, оно стоит того, чтобы, например, продемонстрировать приверженность принципу подотчетности по Регламенту о защите данных.
- *Получатели и категории получателей персональных данных, включая третьих лиц и организации, совместно контролирующие персональные данные и получающие персональные данные для обработки*: по умолчанию информация должна быть предоставлена по всем указанным получателям. Во многих случаях, например, когда организация, контролирующая данные, привлекает различные организации для обработки данных, которые могут меняться время от времени, данная задача может оказаться обременительной и не всегда осуществимой. Если

[1] Рабочая группа подготовила специальные разъяснения в отношении специалистов по защите персональных данных (РГ 243, последняя редакция подготовлена и принята 5 апреля 2017 г.).

организация, контролирующая персональные данные, принимает решение об указании категории получателей вместо конкретных организаций, то контролирующая организация должна быть в состоянии объяснить свое решение и предоставить в положении о защите персональных данных как можно больше сведений, таких как информация о типе получателя персональных данных (с указанием осуществляемых им видов деятельности) отрасли, секторе и подсекторе, а также месте нахождения получателя.

- *Передача данных в третьи страны вместе с принимаемыми мерами защиты, а также где можно ознакомиться с описанием указанных мер защиты* (например, по ссылке): в положении о защите персональных данных должны быть указаны основания для передачи данных за пределы Европейской экономической зоны (например, в силу обязательных корпоративных правил, на основании решения о достаточности мер или стандартных положений договора или в порядке исключения) вместе с перечнем третьих стран, куда будет осуществляться передача данных. В Разъяснениях указано, что перечень должен быть исчерпывающим.

- *Срок хранения данных*: в Разъяснениях указано, что общего указания о хранении персональных данных в течение срока, необходимого для целей их обработки, недостаточно. Предприятия и организации могут воспользоваться предусмотренными законом требованиями или отраслевыми рекомендациями в качестве инструмента для оценки длительности хранения персональных данных, но первоочередная цель заключается в предоставлении субъекту персональных данных возможности оценки соответствующих сроков хранения в зависимости от категории предоставляемых данных. В случае хранения данных в связи с текущими коммерческими, деловыми или трудовыми отношениями указание точного срока хранения данных может оказаться невозможным, но субъект данных должен обладать достаточной информацией для определения данного срока.

- *Права субъектов данных*: в положении о защите персональных данных должна быть приведена информация о том, каким образом субъект данных может получить доступ, исправить, удалить, ограничить обработку или заявить возражения против обработки, а также перенести свои данные. Такие права должны быть явным образом доведены до сведения субъекта данных. Хотя об этом сказано в Разъяснениях, но прямо не требуется по Регламенту о защите данных, эта информация должна сопровождаться пояснениями, что подразумевают указанные права и как они могут быть реализованы.

- *Порядок отзыва субъектом данных согласия на обработку данных*: порядок не только должен быть включен в состав информации, предоставляемой субъектам данных, но предприятия и организации должны обеспечить возможность фактического отзыва согласия из своей системы так же просто, как оно было дано.

- *Право на обращение с жалобой*: субъекты данных должны быть извещены о своем праве на обращение с жалобой в соответствующий надзорный орган в случае нарушения (фактического или предполагаемого) Регламента о защите данных.
- *Использование обязательных полей*: в электронных формах должно быть ясно указано, какие поля являются обязательными, а какие необязательными для заполнения, а также последствия незаполнения обязательных полей. Так, например, в рамках трудовых отношений договором может быть предусмотрено требование о предоставлении работодателю определенной информации.

Во вторых: Регламентом о защите данных предусмотрено требование к предприятиям и организациям о предоставлении информации субъектам данных «кратким, ясным, вразумительным и легкодоступным» способом. Что это означает для положений о защите персональных данных на практике?

- Информация об обработке персональных данных субъекта персональных данных должна быть представлена рациональным и лаконичным образом для избежания «информационного истощения». Использование многоуровневых заявлений о защите персональных данных является хорошим способом обеспечения легкой навигации по положению о защите персональных данных и его удобства для пользователя. К иным способам, имеющимся в распоряжении бизнеса, оперирующего через интернет, относятся контекстуальные «всплывающие» уведомления, 3D touch или наплывающие уведомления, а также панели по защите персональных данных.
- Предприятия могут сделать доступ к своему положению о защите персональных данных простым и легким, разместив информацию на той же самой странице, на которой осуществляется сбор данных, и ясно обозначив его. В Разъяснениях указано, что объединение положения о защите персональных данных с прочими условиями или просто размещение ссылки на положение о защите персональных данных на первой странице сайта недостаточно.
- Положение о защите персональных данных должно быть простым для понимания. Предприятия и организации должны определить свою целевую аудиторию(-и) и уровень понимания ее среднего представителя, проявляя особую осторожность в тех случаях, когда товары или услуги предназначены для детей или уязвимых категорий населения. Для проверки понимания целевой аудиторией положения о защите персональных данных, относящегося к обработке их персональных данных, можно использовать панели пользователя.

В-третьих: предприятиям и организациям необходимо регулярно отслеживать соблюдение требования о прозрачности в течение всего срока обработки данных (например, при утечке данных), а не только в момент сбора данных у субъекта персональных данных или их получения иным образом.

В-четвертых, следование рекомендациям проекта Разъяснений в действующей редакции не обязательно гарантирует соблюдение требований в будущем. Рабочая группа опубликует обновленный текст Разъяснений вместе с разделом по часто задаваемым вопросам после завершения анализа результатов консультаций по вопросу прозрачности. Администрация специального уполномоченного Великобритании по защите информации будет и далее пересматривать свой подход по данному вопросу по мере выработки в будущем разъяснений ЕС и обобщения передового опыта после мая 2018 года. Предприятиям и организациям следует придерживаться такого же подхода для обеспечения соответствия меняющимся ожиданиям регулирующих органов после вступления в силу и реализации положений Регламента о защите данных.

Фирма «Дебевойз энд Плимптон ЛЛП» консультирует предприятия и организации, как в ЕС, так и за его пределами, по всем аспектам готовности предприятий и организаций к вступлению в силу Регламента о защите данных.

* * *

Мы будем рады ответить на любые ваши вопросы по данной тематике.

НЬЮ-ЙОРК

Джереми Фейгельсон
jfeigelson@debevoise.com

ФРАНКФУРТ

Д-р Томас Шурле
tschuerrle@debevoise.com

Д-р Фридрих Попп
fpopp@debevoise.com

ЛОНДОН

Джейн Швец
jshvets@debevoise.com

Кери Чейв
cchave@debevoise.com

Кристофер Гаррет
cgarrett@debevoise.com