Информация для клиентов

Разъяснения по Регламенту о защите данных Администрации специального уполномоченного Великобритании по защите информации: что предприятиям и организациям следует знать и делать

НЬЮ-ЙОРК
Джереми Фейгельсон
jfeigelson@debevoise.com

ЛОНДОН
Джейн Швец
jshvets@debevoise.com

Кристофер Гаррет
cgarrett@debevoise.com

Роберт Маддокс
rmaddox@debevoise.com

Администрация специального уполномоченного Великобритании по защите информации («ICO») распространила проект подробных разъяснений по использованию согласия в качестве основания для обработки персональных данных по Генеральному регламенту ЕС о защите данных («Регламент о защите данных»), вступающему в силу 25 мая 2018 г. До 31 марта 2017 г также открыто обсуждение данных разъяснений.

Предприятия и организации, на которые с мая 2018 года будет распространяться действие Регламента о защите данных, должны: (i) обеспечить подготовку к вступлению в силу Регламента о защите данных в соответствии с разъяснениями ICO и (ii) рассмотреть возможность использования открытого обсуждения для формирования толкования ICO Регламента о защите данных и обеспечить защиту прав физических лиц в соответствии с ним без чрезмерного обременения бизнеса в рамках ограничений, предусмотренных Регламентом о защите данных.

РЕГЛАМЕНТ О ЗАЩИТЕ ДАННЫХ И ПРЕДОСТАВЛЕНИЕ СОГЛАСИЯ

Принятие Регламента о защите данных знаменует собой кардинальный пересмотр подходов к регулированию защиты информации в ЕС и за его пределами (в тех случаях, когда предприятия за пределами ЕС предлагают товары и услуги или контролируют деятельность физических лиц, находящихся в ЕС). И предприятиям, находящимся в ЕС, и тем, которые ориентируются на ЕС, необходимо подготовиться к исполнению расширенных требований по

защите данных, предусмотренных Регламентом о защите данных. Кроме того, весьма вероятно, что правительство Великобритании примет законодательство, полностью повторяющее или очень похожее на Регламент о защите данных, которое будет действовать после выхода Великобритании из состава ЕС. Таким образом, соблюдение Регламента о защите данных, скорее всего, будет актуально даже для тех предприятий и организаций, которые работают исключительно на территории Великобритании.

Для соблюдения Регламента о защите данных большинству предприятий не потребуется изобретать велосипед. Регламент о защите данных основывается на многих действующих правовых нормах и передовом опыте. Тем не менее, выделение недостаточных ресурсов на подготовку к вступлению в силу Регламента о защите данных может дорого обойтись. Компании, допустившие нарушение новых норм, могут быть оштрафованы на сумму до 4% от годового оборота по всему миру или 20 млн евро, в зависимости от того, какая из сумму будет являться большей.

Хотя согласие физического лица остается юридическим основанием для обработки персональных данных, Регламент о защите данных ужесточает требования к получению такого согласия – оно должно быть «предоставлено добровольно, быть конкретным, информированным и недвусмысленным» в форме «заявления» или «явных подтверждающих действий».

Формы согласия с уже поставленными галочками в соответствующих клетках, которым регулирующие органы ЕС никогда не благоволили, очевидным образом уйдут в прошлое. Какие еще произойдут изменения?

РАЗЪЯСНЕНИЯ ICO

Во-первых, предприятиями и организациям необходимо убедиться в том, что имеющиеся у них согласия достаточны. Согласия, полученные по действующему режиму защиты персональных данных, сохраняют силу при условии соответствия новым требованиям Регламента о защите данных. В случае несоответствия необходимо получить новые согласия или задействовать альтернативные основания для обработки данных (и сообщить об этом основании соответствующему физическому лицу).

Предприятиям и организациям следует иметь в виду, что согласие контрагента по договору должно быть получено отдельно от других договорных условий и по общему правилу не должно являться предварительным условием оформления подписки на получение услуг. Так, например, это означает, что при совершении сделки через Интернет согласие на направление в дальнейшем

маркетинговых материалов должно быть получено в виде галочки в специальной клетке, отдельной от клетки для предоставления согласия на саму сделку.

Тем не менее, для многих коммерческих целей, таких как обработка данных заказчика для передачи товаров или оказания услуг, а также персональных данных работников в рамках трудовых отношений, согласие не требуется, поскольку можно (и следует) руководствоваться другими положениями Регламента о защите данных, а именно, необходимостью исполнения договора или законными интересами работодателя.

Во-вторых, текст запроса на предоставление согласия должен быть тщательно проработан и составлен с учетом конкретных обстоятельств. Организациям следует заранее обращать внимание физических лиц на запрос о предоставлении согласия и хранить их отдельно от общих условий. В качестве минимальных требований в запросе должно быть указано наименование организации, осуществляющей обработку данных, причины сбора данных, а также каким образом и кто будет использовать данные. В запросе на предоставление согласия должно быть разъяснено, что физическое лицо вправе отозвать свое согласие в любой момент, и изложен порядок его отзыва.

Подобная прозрачность имеет исключительно важное значение. Так, например, ICO подчеркивает, что предприятиям и организациям следует называть физическим лицам третьих лиц, которые будут осуществлять обработку их персональных данных. С точки зрения ICO, указание общей категории организаций является неприемлемым, поскольку не обеспечивает физическим лицам достаточной степени надзора и контроля за своими данными.

В-третьих, организациям следует обеспечить, чтобы принятый ими порядок получения согласия предоставлял физическим лицам реальную возможность выбора и осуществления контроля за тем, как будет осуществляться обработка их данных. ICO полагает, что согласие будет трудно, хотя и не совсем уж невозможно, получить в рамках трудовых отношений, учитывая неравенство в положении работодателя и работника. Тем самым становится затруднительным получение действительного согласия по трудовому договору. Вместо этого работодателям необходимо воспользоваться другими основаниями для обработки персональных данных своих работников, такими как необходимость исполнения трудового договора или соблюдения законных интересов работодателя. В противном случае они могут столкнуться с трудностями при доказывании того, что согласие было «предоставлено добровольно».

Аналогичным образом, организации могут столкнуться со сложностями при использовании согласия в качестве основания для обработки данных в тех случаях, когда они все равно обрабатывают данные на других основаниях, если согласие предоставлено не было. Использование «запасных» положений в тех случаях, когда действительность согласия сомнительна, может привести к нарушению требований о справедливости и прозрачности Регламента о защите данных.

Таким образом, организациям следует определить для себя, является ли согласие наиболее подходящим и эффективным основанием для обработки каждой отдельной категории персональных данных, находящихся под их контролем. В тех случаях, когда предприятия и организации прибегают к другим основаниям для обработки данных, помимо согласия, им следует документально оформлять их и сообщать об этих основаниях в соответствии с требованиями Регламента о защите данных, например, с помощью уведомления о конфиденциальности.

В-четвертых, необходимо периодически проверять, сохраняют ли имеющиеся согласия юридическую силу. Как отмечено выше, по Регламенту о защите данных физические лица имеют право отозвать свое согласие в любой момент, и обработка данных на основании отозванного согласия должна быть прекращена (требование не распространяется на обработку данных до момента отзыва согласия).

ICO также выступает за упреждающую работу организаций, осуществляющих обработку данных, по администрированию согласий. Так, например, она рекомендует организациям в большинстве случаев обновлять согласия каждые два года. В связи с этим предприятиям и организациям следует рассмотреть вопрос о внедрении системы предупреждения о возможной необходимости получения нового согласия.

В-пятых, предприятиям и организациям следует в полном объеме документально оформлять согласия на случай проведения проверки. По Регламенту о защите данных организации, использующие согласие для обработки данных, должны быть в состоянии доказать, что физическое лицо на самом деле дало согласие. В документации, касающейся ведения деятельности, должно быть отражено, какие физические лица предоставили свое согласие, какая информация им была предоставлена, когда и каким образом они дали согласие и было ли согласие отозвано ими. Так, например, в документации должна храниться копия формы согласия физического лица с проставленной датой, а также экземпляр положения или уведомления о защите частной информации, действовавшего на соответствующую дату.

В-шестых, следование рекомендациям в действующей в настоящее время редакции не обязательно гарантирует соблюдение требований в будущем. ICO допускает, что 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» готова оказать содействие организациям, желающим принять участие в обсуждении, организованном ICO, и 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.

* * *

Если у вас возникнут какие-либо вопросы, просим вас обращаться к нам за разъяснениями.