

Работа из дома и безопасная рассылка электронных писем (2) 3/2/21

Любое предприятие, государственное или муниципальное учреждение или даже индивидуальный коммерсант, который обрабатывает персональные данные жителей ЕС/ЕЭЗ, позволяющие идентифицировать физических лиц, подчиняется требованиям Общего регламента о защите данных ЕС (ОРЗД). Данной статьей мы завершаем тему, начатую в прошлом году.

Маркетинговые мероприятия и рассылка коммерческих уведомлений

В целях соблюдения принципов обработки данных, предусмотренных статьей 5 Общего регламента о защите данных (ОРЗД), предприятию важнее всего обеспечить законную, добросовестную и прозрачную для субъекта данных обработку. Данные физических лиц можно обрабатывать только при условии соблюдения всех принципов, предусмотренных статьей 5. Это означает, что предприятие должно быть честным по отношению к субъекту данных (физическому лицу) и способ обработки должен опираться на недвусмысленное общение с субъектом данных.

Шесть законных оснований, позволяющих предприятию обрабатывать (обобщать, хранить, использовать и т.д.) данные физических лиц, перечислены в статье 6 ОРЗД. Согласно подпункту «а» пункта 1 данной статьи, субъектом данных дано согласие на обработку его персональных данных в одной или нескольких конкретных целях. Согласие должно быть получено недвусмысленно и после понятного физическому лицу и полного разъяснения сути планируемой предприятием обработки, а именно:

- согласие должно быть свободно предоставленным, конкретным, информированным и недвусмысленным;
- требование о предоставлении согласия должно быть четко отделено от других вопросов и написано ясным и понятным языком;
- физическое лицо может отозвать ранее данное согласие, когда пожелает, и предприятие обязано незамедлительно обеспечить реализацию такого права при отсутствии оснований, по которым предприятие не может этого обеспечить;
- дети младше 13 лет могут дать согласие только с разрешения родителей;
- необходимо сохранить документальные доказательства предоставления согласия.

Подпунктом «f» пункта 1 статьи 6 ОРЗД предусматривается, что обработка персональных данных необходима для соблюдения законных интересов администратора данных или третьего лица, таким образом, предприятие осуществляет обработку в своих законных интересах. Однако в случае использования этого юридического обоснования необходимо помнить о том, что основные права и свободы субъекта данных могут стоять выше законных интересов предприятия, поэтому применение такого юридического обоснования и осуществление обработки данных могут оказаться невозможными.

В целях соблюдения своих законных интересов предприятие может отправлять коммерческие уведомления на адрес электронной почты юридического лица без предварительного согласия, однако используя действительный адрес электронной почты, на который получатель уведомления может отправить требование прекратить коммуникацию. Такой порядок необходимо соблюдать и при отправке коммерческих уведомлений физическим лицам, при этом их содержание должно

отвечать требованиям статьи 8 закона «Об услугах информационного общества».

ОРЗД никоим образом не запрещается отправлять коммерческие уведомления по электронной почте и использовать адреса электронной почты физических лиц в маркетинговых целях. Однако при хорошем маркетинге получатель уведомления захочет повторно получить по электронной почте информацию, например, о предоставляемых предприятием услугах. В ОРЗД разъясняются условия предоставления согласия и установлено требование к предприятиям просить разрешения на отправку коммерческих уведомлений. Предприятие нарушает требования ОРЗД только в том случае, если потребитель не имеет возможности отказаться от получения коммерческих уведомлений или предприятие игнорирует такой отказ либо отправляет информацию получателю, который не давал согласия на ее получение и не пользовался аналогичными услугами ранее.

Безопасность электронной почты

Согласно подпункту «f» пункта 1 статьи 5 ОРЗД, персональные данные следует обрабатывать таким образом, чтобы обеспечить их надлежащую безопасность, в том числе защиту от неразрешенной или незаконной обработки, а также от случайной утери, уничтожения или порчи, применяя соответствующие технические или организационные меры.

Шифрование электронной почты – одна из технических мер, которые можно принять, чтобы обеспечить безопасность сведений, обрабатываемых через электронную почту. В свою очередь, организационные меры связаны с правилами внутреннего распорядка и инструкциями предприятия, а также с организацией обучения. С помощью фишинговых электронных писем хакеры пытаются завладеть доступом к учетной записи или устройству пользователя, вводя в заблуждение или используя вредоносное ПО. Если получатель электронного письма нажимает на ссылку или скачивает приложенный файл, это действие может позволить нападающему получить доступ к устройству и зачастую к другим устройствам предприятия и учетным записям пользователей электронной почты – таким образом, ошибка одного работника может представлять угрозу для большого объема данных. Не сумев доказать надзорному учреждению факт внедрения соответствующих технических и организационных мер, предприятие будет вынуждено уплатить значительный штраф за несоблюдение требований ОРЗД, а также выплатить компенсации физическим лицам (субъектам данных) за несоблюдение их прав.

Для снижения риска нарушений предприятию важно информировать своих работников о безопасности электронной почты, одновременно внедряя такие технические и организационные меры, которые наилучшим образом защищают персональные данные, чтобы свести к минимуму размер возможного штрафа.