Как убедиться в соответствии деятельности предприятия Регламенту о защите данных? (1) 1/32/20

Недавно СМИ всколыхнули сообщения о применении крупнейшего в истории Латвии штрафа (150 000 евро) к предприятию, работающему в сфере э-коммерции, за нарушения, связанные с несоблюдением требований Общего регламента о защите данных. Учитывая обстоятельства предприятия, на которые в своем решении указала Государственная инспекция данных, в этой статье мы расскажем о требованиях, которые обязано соблюдать любое предприятие, обрабатывающее персональные данные на интернет-страницах, чтобы избежать предусмотренного регламентом штрафа.

Нормы регламента

Требования Регламента о защите данных распространяются на все предприятия, предлагающие товары или услуги гражданам ЕС, и применяются к любому предприятию э-коммерции, использующему данные проживающих в ЕС физических лиц. Требования Регламента о защите данных распространяются на все базы данных, содержащие пользовательскую информацию, например, данные кредитных карт и данные о покупках.

Согласно Регламенту о защите данных, штраф за обнаруженные нарушения, включая то, за которое наложено взыскание в Латвии, может составлять до 20 миллионов евро или, как в случае конкретного предприятия, – до 4% от его глобального оборота в предыдущем финансовом году.

На что следует обратить внимание при обработке данных пользователей на интернет-страницах?

Несоответствие Регламенту о защите данных может причинить не только крупный финансовый ущерб, но и вред репутации предприятия, сокращая возможности привлечения клиентов и продолжения предпринимательской деятельности.

Уведомление о конфиденциальности на домашней странице

Уведомление о конфиденциальности является общедоступным документом, в котором должно быть описано, как предприятие применяет принципы защиты данных. Согласно Регламенту о защите данных, текст Уведомления о конфиденциальности должен быть сжатым, наглядным и недвусмысленным, а также написанным простым языком, чтобы доходчиво уведомить любое физическое лицо, посещающее домашнюю страницу предприятия, об осуществляемой предприятием обработке данных.

Скорее всего, большинство предприятий уже разместили на своих домашних страницах Уведомление о конфиденциальности и обратили внимание на следующие аспекты:

- Обновляло ли предприятие с 2018 года Уведомление о конфиденциальности в соответствии с нынешней ситуацией, чтобы оно охватывало все персональные данные,

собранные с момента посещения пользователем конкретной домашней страницы?
- В Уведомлении о конфиденциальности должны быть указаны ясные цели, в которых предприятие использует персональные данные (например, для нужд маркетинга и бухгалтерского учета).
- В Уведомлении о конфиденциальности должны быть ясно указаны права пользователей домашней страницы, относящиеся к персональным данным пользователей и их использованию.
- Каждая цель обработки данных должна иметь правомерное основание, о котором предприятие уведомляет пользователя.
- Должна быть указана информация о том, кто и каким образом может осуществлять обработку конкретных данных.
- Пользователю должно быть совершенно ясно, на каком основании обрабатываются его персональные данные – на основании согласия, закона или договора. Необходимо обратить внимание на то, что в зависимости от цели обработки персональных данных юридическое основание может меняться и данная информация должна быть недвусмысленно указана на домашней странице.

Получает ли предприятие перед сбором данных согласие посетителей домашней страницы и имеющихся клиентов?

Цель Регламента о защите данных – обеспечить клиентам/пользователям полный контроль над использованием их данных в Интернете, в том числе в э-коммерции. Согласие является одним из наиболее существенных элементов защиты данных.

Например, предприятие э-коммерции должно иметь законные решения для получения согласия и дальнейшей обработки данных на его основании. Уведомление о конфиденциальности должно содержать всю необходимую информацию, относящуюся к сбору, обработке, хранению и использованию данных клиентов/пользователей. В ходе обработки данных физических лиц из бланков, в процессах регистрации, из электронных писем и всплывающих окон (баннеров) пользователю нужно обеспечить возможность дать или отозвать согласие на использование этих данных.

Основные вопросы об обработке данных, которые должны быть понятны в случае согласия:

- Юридическим обоснованием для получения персональных данных является согласие или есть и другое юридическое обоснование для их обработки?
- Порядок получения согласия субъекта данных соответствует всем критериям, связанным с э-коммерцией и установленным Регламентом о защите данных?
- Предприятие может подготовить информацию, например, для передачи надзорному учреждению, доказывающую, что сбор и обработка данных имеют юридическое основание?
- Предприятие документирует все случаи, в которых данные обрабатываются на основании согласия физического лица?
- Предприятие пересмотрело свои процедуры получения согласия и регулярно их пересматривает/обновляет?
- Есть ли возможность прекратить обработку данных и удалить записи, получив соответствующий запрос от субъекта данных?

(Окончание – в следующих Коротких сообщениях.)