Как убедиться в соответствии деятельности предприятия Регламенту о защите данных? (2) 1/33/20

Окончание статьи об Общем регламенте о защите данных, опубликованной на прошлой неделе.

Информирование о действиях, совершенных предприятием в отношении обработки персональных данных пользователей/клиентов

Предприятиям необходимо подготовить понятные описания процессов и целей получения данных, поясняющие, для чего происходит сбор, дальнейшая обработка и хранение данных в течение определенного периода. Эти процессы включают категории данных, сроки и проверку удаленных данных. Предприятия обязаны описать меры безопасности, принимаемые для защиты этих данных.

Согласно Регламенту о защите данных, физические лица обладают рядом прав:

1. правом быть информированным;
2. правом доступа;
3. правом на исправление данных;
4. правом на удаление данных;
5. правом ограничить обработку данных;
6. правом на переносимость данных;
7. правом возразить против конкретной обработки данных;
8. правами, связанными с автоматизированным принятием решений и профилированием.

Действия в случае нарушения принципов защиты данных

Вероятность нарушений в области защиты данных является причиной для пересмотра имеющихся процессов обработки данных, в особенности у предприятий э-коммерции. Регламент о защите данных обязывает все предприятия сообщать надзорному учреждению о нарушениях в области защиты данных, если выполняются критерии относительно обязанности оповещения. Оповестить надзорное учреждение необходимо в течение 72 часов с момента, когда стало известно о нарушении. Если характер нарушения может ущемить права индивида, о произошедшем также необходимо сообщить клиенту и/или пользователю домашней страницы предприятия. При этом каждое предприятие обязано регистрировать нарушения в области защиты данных независимо от характера нарушения.

Основные вопросы, которые должны быть ясны относительно защиты данных:

- Пересматривает ли предприятие свои ИТ-системы и процессы, чтобы предотвратить вероятность нарушений в области защиты данных и решить связанные с ними проблемы?
- Известно ли предприятию о присущем ему «высоком риске» согласно критериям нарушений в области защиты данных, в отношении которых у предприятия существует обязанность уведомлять надзорное учреждение?
- Разработан ли на предприятии порядок оповещения о нарушениях в области защиты

данных, соответствующий всем требованиям Регламента о защите данных?
- Внедрена ли на предприятии внутренняя система оповещения о возможных нарушениях в области защиты данных?

Если предприятие ведет свою деятельность за пределами ЕС

Согласно принятым в ЕС законам о защите данных, в том числе требованиям Регламента о защите данных, персональные данные разрешается передавать только в третьи страны, которые гарантируют определенный уровень защиты данных, отвечающий требованиям Регламента о защите данных, которые предъявляются к странам-участницам. Третьи страны, в которые передаются персональные данные, обязаны поддерживать соответствующий уровень защиты данных, и всем предприятиям, в том числе предприятиям э-коммерции, необходимо соблюдать требования Регламента о защите данных независимо от местонахождения предприятия.

Заключение

Каждому предприятию важно понимать, что требования Регламента о защите данных распространяются на все персональные данные, связанные с идентифицированным или идентифицируемым лицом. Эта информация включает в себя следующие персональные данные: имя, дату рождения, данные кредитной карты, банковские сделки, социальные средства связи и даже фотографии, а также существенное количество других данных, которые могут перейти в распоряжение предприятия при первом посещении клиентом/пользователем домашней страницы предприятия. Используемые предприятием cookie-файлы и IP-адреса, имеющие отношение к клиенту/пользователю, тоже являются персональными данными, на обработку которых распространяются все требования Регламента о защите данных.

Также нельзя забывать, что действие Регламента о защите данных распространяется на все предприятия, предлагающие товары и/или услуги гражданам ЕС, т.е. на любое предприятие, включая предприятия э-коммерции, использующее данные проживающих в ЕС физических лиц.