

Как в дальнейшем передавать персональные данные предприятиям за пределами ЕС? 1/40/20

Приняв одно из важнейших на сегодняшний день решений (решение от 16 июля 2020 года по делу № C-311/18 «Комиссар по защите данных против *Facebook Ireland & Maximillian Schrems*), в котором подчеркиваются основные права на тайну частной жизни в связи с отправкой персональных данных в третьи страны, Суд Европейского союза (СЕС) еще раз подтвердил, как важно поддерживать высокий уровень защищенности персональных данных, отправляемых из стран ЕЭЗ в третьи страны. Решение вызвало ряд вопросов о юридической обоснованности отправки персональных данных в третьи страны. Поскольку в решении акцентируется отправка данных в США, в данной статье мы выясним, как действовать предприятиям сейчас, когда решение вступило в силу.

Требования осуществлять безопасную обработку и защиту данных физических лиц в соответствии с Общим регламентом о защите данных (ОРЗД) относятся к любым действиям, совершаемым с данными физических лиц. Предприятиям, планирующим отправлять данные за пределы ЕЭЗ, необходимо считаться с тем, что к такого рода обработке данных предъявляются дополнительные требования, чтобы данные вообще могли обрабатываться.

Ранее Европейская комиссия признала, что Соглашение о правилах обмена конфиденциальной информацией между ЕС и США (Privacy Shield) обеспечивает надлежащий уровень защиты персональных данных, передаваемых американским предприятиям из ЕС. После вступления в силу решения СЕС становится ясно, что ситуация изменилась. Несмотря на то что цель Privacy Shield – защищать любые персональные данные резидента ЕС, которые в коммерческих целях передаются предприятиям США, в дальнейшем обеспеченных им гарантий может быть слишком мало, чтобы это было законно.

В первую очередь предприятию важно понимать, какие персональные данные передаются или могут передаваться американскому предприятию и с какой целью. В основном персональные данные передаются для деловых нужд, собираются и используются в США для последующей обработки (к примеру, имя и фамилия клиента или сотрудника, номер телефона, адрес электронной почты или любая другая информация, позволяющая идентифицировать физическое лицо). Таким образом предприятие ЕС или, к примеру, филиал какого-либо американского предприятия или его партнерское предприятие в Европе передает персональные данные американскому предприятию для дальнейшей обработки в США. Как правило, такие сделки заключаются при покупке товаров и услуг в Интернете, использовании социальных СМИ и услуг облачных вычислений либо во время работы на предприятиях ЕС, которым, к примеру, услуги, связанные с управлением персоналом, предоставляет некое американское предприятие (например, материнская компания в США).

Предприятия, передающие данные таким образом, ранее считали, что Privacy Shield обеспечивает высокий уровень защиты. Не опасаясь нарушений в области защиты данных, предприятия осуществляли обработку персональных данных, передавая их американским предприятиям при условии, что получатель персональных данных их обрабатывает (например, хранит или передает дальше) согласно строгим условиям защиты данных и мерам, предусмотренным Privacy Shield. В настоящий момент СЕС отменил Определение Европейской комиссии №2016/1250 о надлежащей защите, обеспечиваемой Соглашением о правилах обмена конфиденциальной информацией между ЕС и США, но считает действительным Определение Европейской комиссии №2010/87 о

стандартных договорных оговорках относительно передачи персональных данных обработчикам, зарегистрированным в третьих странах.

Несмотря на то что стандартные договорные оговорки все еще в силе, СЕС подчеркивает необходимость сохранить уровень защиты данных, по сути равноценный гарантированному ОРЗД уровню защиты. Предприятие, отправляющее персональные данные в третьи страны (в том числе в США), обязано проверить, обеспечивают ли страны, в которые отправляются данные, надлежащую защиту, принимая соответствующие ОРЗД меры.

Во-вторых, понимая, что это за данные и можно ли их отправлять в третью страну (в том числе в США), предприятие должно сделать вывод о том, как ему в дальнейшем обеспечивать выполнение требований согласно указанному в ОРЗД и решении СЕС:

- сторонам, участвующим в передаче данных и их дальнейшей обработке, необходимо стараться обеспечить дополнительные меры безопасности в целях снижения рисков, в частности, осуществлять шифрование данных, а также, в отдельных случаях, – анонимизацию или псевдонимизацию отправляемых данных, обеспечивая доступ к данным только предприятию, которое отправило их в США;
- предприятию ЕС, передающему персональные данные предприятию в третьей стране, необходимо оценить, каким образом их получатель соблюдает требования, соответствующие ОРЗД, и удостовериться в том, что данным обеспечены предусмотренные ОРЗД права;
- предприятию необходимо оценить своих деловых партнеров в третьих странах, а также оценить и документировать необходимость передачи персональных данных, полагаясь на разумные механизмы передачи данных и выбирая таких поставщиков услуг, которые снижают риски, связанные с передачей данных.

Органы власти США уже указали, что после решения СЕС более 5300 крупных и малых европейских и американских предприятий больше не могут полагаться на Privacy Shield как на основание для отправки персональных данных из Европы в США. Предприятия должны быть готовы к тому, что надзорные учреждения будут проводить проверки с целью удостовериться в том, что предприятия внедрили еще более строгие меры по защите данных и отправке в третьи страны. Кроме того, необходимо понимать, что, если продолжать работать как прежде в ожидании действий надзорных учреждений, последствия могут быть непредсказуемыми, а размер штрафа может достигать 4% от годового оборота предприятия.