Предприятия отрасли fintech обязаны соблюдать требования и после удара, нанесенного COVID-19 (2) (3/28/20)

Продолжение статьи, опубликованной в предыдущих еженедельных Новостях.

Регулирование GDPR		Ссылка на статью GDPR	Санкция
Согласие субъекта данных	Согласие субъекта данных необходимо предприятию fintech для использования необязательных cookie-файлов (например, cookie-файлов для учета статистики посещаемости домашней страницы Google Analytics). Согласие, полученное от субъекта данных, является добровольным и недвусмысленным, предусматривающим право субъекта данных возразить против осуществляемой обработки данных.	Статьи 13, 14 и 25	До 20 миллионов евро или до 4% от общемирового оборота
Оценка рисков	Предприятие *fintech* проводит оценку рисков, а в случае обработки данных с высокой степенью риска проводит также оценку влияния. К примеру, оценке влияния необходимо подвергнуть обработку данных, в основе которой лежит профилирование и автоматическое принятие решений. Данные оценки по необходимости актуализируются.	Статья 35	До 10 миллионов евро или до 2% от общемирового оборота
	Предприятие *fintech* обеспечивает предоставление субъекту данных права возразить против осуществляемого профилирования или автоматического принятия решений.	Статья 22 (1)	До 20 миллионов евро или до 4% от общемирового оборота
Безопасная обработка данных	Предприятие *fintech* внедрило соответствующие меры безопасности и технические решения. К примеру, предприятие соблюдает изданные Европейским банковским учреждением технические стандарты https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2 или другие стандарты (например, ISO 27701:2019).	Статья 32	До 10 миллионов евро или до 2% от общемирового оборота
	Предприятие *fintech* строго соблюдает принципы обработки данных GDPR (например, не хранит персональные данные дольше, чем это необходимо или предусмотрено нормативными актами). Предприятие *fintech* не использует данные, не получает к ним доступ и не хранит их в других целях, кроме предоставления, например, услуги информации о счете, которую недвусмысленно запросил пользователь платежных услуг.	Статья 5	До 20 миллионов евро или до 4% от общемирового оборота
	Предприятие *fintech* разрабатывает документ в области ИТ, который определяет основные принципы обеспечения безопасности информационных ресурсов и анализа рисков, физической и логической защиты информационных ресурсов, эксплуатации информационных систем и действий в случае инцидентов безопасности.	Статья 24 (2) и Статья 32	До 10 миллионов евро или до 2% от общемирового оборота
	При разработке нормативных технических стандартов аутентификации и коммуникации необходимо систематически оценивать и учитывать аспект конфиденциальности и защиты частной жизни, чтобы выявить риски, связанные с каждой из доступных технических возможностей, а также то, какие средства защиты можно внедрить, чтобы свести угрозу безопасности данных к минимуму.	Статья 32	До 10 миллионов евро или до 2% от общемирового оборота
Третьи страны и серверы ИС, расположенные в них	Предприятие *fintech* обязано уведомлять субъектов данных о возможности обработки данных за пределами ЕС/ЕЭЗ (например, обязанность информирования субъектов данных в командировках, при бронировании гостиницы или авиабилета, запросе визы).	Статьи 13, 14 и 44	До 20 миллионов евро или до 4% от общемирового оборота
	Предприятие *fintech* предусматривает дополнительные требования к безопасности, если данные отправляются за пределы ЕС/ЕЭЗ или если серверы ИС находятся за пределами ЕС/ЕЭЗ.	Статья 44	До 20 миллионов евро или до 4% от общемирового оборота
Обработка персональных данных особых категорий	Не путать: данные особых категорий согласно GDPR не являются «сензитивными платежными данными» согласно PSD2!		
	Если *предприятие* fintech обрабатывает данные особых категорий, на это следует запросить согласие субъекта данных.	Статья 9	До 20 миллионов евро или до 4% от общемирового оборота
	Предприятию *fintech* разрешается обрабатывать информацию о судимости субъекта данных, только если такая обработка предусматривается нормативными актами.	Статья 10	До 20 миллионов евро или до 4% от общемирового оборота
Организация обучения	Предприятие *fintech* проводит регулярное информирование и обучение работников, участвующих в процессе обработки.	Пункт «б» части первой статьи 39	До 10 миллионов евро или до 2% от общемирового оборота
Оповещение об инциденте	В течение 72 часов с момента выявления инцидента	Статья 33	До 10 миллионов евро или до 2% от общемирового оборота

(Окончание – в следующих Коротких сообщениях)