"Не так страшен волк, как его рисуют"

или GDPR и Закон Украины "О защите персональных данных": найди 10 отличий

Ирина Козлова

Ведущий специалист департамента информационной безопасности финансового сервиса NovaPay ("Пост Финанс")

Тема внедрения правил GDPR в секторе предоставления финансовых услуг остается все такой же актуальной. В частности, этот вопрос касается особенностей применения норм Регламента финансовыми компаниями как на территории Европы, так и на территории Украины.

Так, финансовые компании, которые зарегистрированы на территории Украины и осуществляют деятельность в финансовой сфере, в том числе и на территории ЕС, или которые осуществляют мониторинг поведения субъектов персональных данных в контексте GDPR на территории ЕС, подпадают под требования нового европейского регламента, а значит, обязаны разрабатывать и внедрять комплекс организационных и технических мероприятий для возможности отвечать требованиям GDPR.

Что же это за зверь такой – GDPR?

GDPR – Регламент Европейского Союза по обработке персональных данных. Опубликован в 2016 году, вступил в силу с 25 мая 2018 года. Данный регламент заменил Директиву по Защите Данных 1995 года (N 2008/95/EC).

Регламент расширил базовые понятия персональных данных – теперь это не просто информация, относящаяся к идентифицированному человеку (субъекту которого можно 100% идентифицировать), но и данные, которые имеют косвенные признаки идентификации для человека, например, местоположение, физиология, генетика.

Также в Регламенте прописаны четкие требования к сбору и обработке персональных данных (ПД), права субъектов на свои ПД, требования к передаче ПД, организационные мероприятия по обработке ПД и, наверное, самое важное – то, чего все так боятся, – штрафы.

По моему мнению, основные принципы Регламента заключаются в:

1. Законных основаниях для получения и обработки ПД;
2. Честности и прозрачности обработки ПД;
3. Необходимости определения законных и надлежащих целей обработки ПД;
4. Определении сроков хранения ПД, которые обрабатываются;
5. Получении такого количества ПД, которого будет достаточно для реализации поставленных целей – так называемая минимизация ПД;
6. Возможности доказать соответствие своей деятельности требованиям GDPR.

Несоблюдение вышеперечисленных требований (даже одного из них) может повлечь при-

менение к финансовой компании штрафных санкций, которые заключаются в наложении штрафов в размере от 10 до 20 млн евро или от 2% до 4% от годового оборота.

Вы скажете, да мы же в Украине живем, у нас есть свой Закон "О защите персональных данных", какой тут GDPR? Все верно, у нас есть Закон, родителем которого является Директива №95, но есть одна большая проблема: если вы работаете в Украине, но у вас есть клиенты в ЕС и данные вы получаете из ЕС – вы должны соответствовать GDPR.

Для наглядности предлагаю вам сравнительный анализ Европейского Регламента GDPR и Закона Украины "О защите персональных данных".

История	
ЕС	**Украина**
Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера №108	Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера №108, ратификация
Директива 95/46/ЕС	Закон Украины "О защите персональных данных"
GDPR (General Data Protection Regulation) – Общий регламент по защите данных	
Протокол о внесении изменений в Конвенцию №108 о защите частных лиц в отношении автоматизированной обработки данных личного характера. Привязка к GDPR. Общее число подписей - 33 страны	

Персональные данные	
GDPR	**Закон Украины**
	

Сфера покрытия	
ЕС	**Украина**
	
Страны, которые обрабатывают ПД субъектов, которые находятся на территории ЕС	

Субъект ПД имеет право на:	
GDPR	**Закон Украины**
Доступ к своим ПД, цель обработки, категории ПД	Доступ к своим ПД, цель обработки, категории ПД
Информацию о третьих лицах, получивших доступ к ПД	Информацию о третьих лицах, получивших доступ к ПД
Защиту ПД и сроки хранения	Защиту ПД и сроки хранения
Внесение исправлений или удаление своих ПД	Внесение исправлений или удаление своих ПД
Возражение против обработки	Возражение против обработки
Представительство (передачу полномочий)	Представительство (передачу полномочий)
Подачу жалобы к надзорному органу	Подачу жалобы к надзорному органу
Отзыв своего согласия на обработку	Отзыв своего согласия на обработку
Эффективные средства судебной защиты в отношении контролера и обработчика	Эффективные средства судебной защиты
Эффективные средства судебной защиты против надзорного органа	
Получение копии своих данных по запросу	
Переносимость своих данных	
Обращение к DPO	
Компенсацию материального или нематериального ущерба	
Уведомление об утечке данных	

Надзорный орган	
ЕС	**Украина**
Европейский омбудсмен или Евроомбудсмен, англ. Euro-Ombudsman 28 государств - членов ЕС В каждой из стран свой Надзорный орган	Уполномоченный Верховной Радой Украины по правам человека, омбудсмен

Безопасность данных	
ЕС	**Украина**
Псевдонимизация и криптографическая защита	Ст. 24.: Владельцы, распорядители ПД и третьи лица обязаны обеспечить защиту этих данных от случайной потери или уничтожения, незаконной обработки, в том числе незаконного уничтожения или доступа к персональным данным
Конфиденциальность, целостность и доступность данных	Ст.5: Персональные данные могут быть отнесены к конфиденциальной информации (КИ) законом или ответственным лицом
Своевременное восстановление доступности данных	Ст.11 ЗУ "Об информации": "К конфиденциальной информации о физическом лице относятся, в частности, данные о его национальности, образовании, семейном положении, религиозных убеждениях, состоянии здоровья, а также адрес, дата и место рождения"
Регулярная проверка и оценка эффективности технических и организационных мер	Защита КИ осуществляется согласно действующему законодательству Украины
Законодательная база, одно из: - пояснения 29 Рабочей группы - ISO 29100:2018. Концепция защиты ПД - ISO 29101:2018. Концепция архитектуры, обеспечивающей защиту - документы из серии NIST, CNIL и т.д.	

Трансграничная передача	
ЕС	**Украина**
Действующее решение Еврокомиссии о том, что иностранный субъект (третья страна) обеспечивает должный уровень защиты ПД	Обеспечение надлежащего уровня защиты в случаях, установленных законом или международным договором Украины
При наличии надлежащих гарантий (со стороны контролера или обработчика), например: Корпоративные правила (структура компании, передача и категории ПД, защита и сроки хранения ПД)	Страны ЕС
Возможна только с согласия субъекта после того, как он был проинформирован	Страны, которые подписали 108 Конвенцию
Защита жизненно важных интересов субъекта	С согласия субъекта ПД

Преступление и наказание	
ЕС	**Украина**
до 10 млн евро	Административный кодекс Украины ст.18839, 18840 - от 1700 до 34 тыс. грн
до 20 млн евро	Криминальный кодекс Украины ст.182 - от 8500 до 17 тыс. грн - исправительные работы до 2-х лет - арест до 6 месяцев - ограничение свободы до 3-х лет
до 2% годового оборота компании за весь предыдущий финансовый год	
до 4% годового оборота компании за весь предыдущий финансовый год	

Реалии	
ЕС	**Украина**
Современный Регламент по защите ПД	5 октября 2017 года принято постановление Кабинета министров Украины "О выполнении Соглашения об ассоциации между Украиной, с одной стороны, и Европейским Союзом, с другой стороны" № 1106, которым утвержден План мероприятий по выполнению Соглашения
108 Конвенция +	Пунктом 11 Плана мероприятий предусмотрены задачи по совершенствованию законодательства о защите персональных данных с целью приведения его в соответствие с Регламентом
Пояснения 29 Рабочей группы по каждому из пунктов Регламента	В Секретариате Уполномоченного создан Координационный совет по совершенствованию законодательства о защите ПД
	При Координационном совете создан международный проект Twinning по совершенствованию законодательства о защите ПД

Суммируя вышесказанное, следует отметить, что, когда финансовая компания ориентирует свою деятельность на европейский рынок и стремится обслуживать клиентов на территории ЕС, ей стоит задуматься: как корректно разработать и внедрить все организационные и технические меры, которые помогут противостоять новым вызовам, которые определяются GDPR

Согласно Регламенту, можно выделить основные необходимые организационные мероприятия:

1. Проведение Data mapping і Gap assessment, что позволит определить виды и количество ПД, а также потоки информации с персональными данными и откуда они приходят.
2. Необходимо установить, насколько часто и в каком количестве используется методология автоматического принятия решения, включая составление профиля.
3. Проведение DPIA – Data Protection Impact Assessment (оценка рисков или же оценка на воздействие).
4. Компании следует назначить Data Protection Officer (DPO), если она обрабатывает большое количество данных.
5. Разработать документы, которые бы по своему содержанию соответствовали основным принципам GDPR, а также обеспечивали возможность для субъектов ПД реализовывать свои права, определенные Регламентом. Основной документ – Privacy and Data Protection Policy (политика конфиденциальности и защиты персональных данных). Этот документ должен быть в открытом доступе на официальном сайте компании, что является фундаментальным шагом в процессе подготовки соответствия финансовой компании к принципам GDPR.