DATA FUSION

FIRST RUSSIAN DATA FORUM

Дополнительные меры защиты персональных данных в странах мира

Карен Казарьян

Генеральный директор Института исследований интернета

Европейский союз

Обязательные меры: *в соответствии с GDPR*

Рекомендуемые меры: *Руководство 4/2019, рекомендации ENISA, и ряд стандартов ISO*

РЕГУЛЯРНОСТЬ ПРОЦЕДУР ПРОВЕРКИ

Раз в три года, либо чаще, а также при значительном изменении технологических процессов или чувствительности данных

ПРИНЦИПЫ НАЗНАЧЕНИЯ ШТРАФА ЗА УТЕЧКУ ПД

Несоблюдение обязательных требований – отягчающее обстоятельство,
Добровольный аудит – смягчающее, при этом надзорный орган может проводить расследование в форме аудита и ревизию выданных сертификатов

ТИПЫ НАКАЗАНИЙ

Предписание что необходимо изменить
Временный запрет на обработку данных или полный запрет на обработку определённых категорий
Штраф с учётом отягчающих и смягчающих обстоятельств

США

Обязательные меры:

«Закон о финансовой модернизации» (Gramm-Leach-Bliley Act, GLBA), «Закон о добросовестном предоставлении кредитной информации» (The Fair Credit Reporting Act, FCRA), «Закон о мобильности и подотчетности медицинского страхования» (Health Insurance Portability and Accountability Act, HIPAA). «Закон о защите приватности детей в онлайн-среде» (Children's Online Privacy Protection Act, COPPA).

Рекомендуемые меры:

- ✓ Отдельные федеральные нормативные акты включают положения, предполагающие разработку отраслевыми ассоциациями и другими объединениями собственных руководящих принципов саморегулирования (напр., программа Safe Harbor в COPPA).
- ✓ в США действует несколько систем добровольной сертификации для организаций, собирающих и обрабатывающих персональные данные пользователей.
- ✓ NIST SP 800-122, рекомендации по методам обеспечения безопасности персональных данных, в том числе, техники де-идентификации и обезличивания.

РЕГУЛЯРНОСТЬ ПРОЦЕДУР ПРОВЕРКИ

В зависимости от штата и сферы

ПРИНЦИПЫ НАЗНАЧЕНИЯ ШТРАФА ЗА УТЕЧКУ ПД

- характер и серьезность нарушения,
- продолжительность нарушений, их регулярность и преднамеренность,
- размер активов, обязательств и собственного капитала ответчика.

В рамках прецедентного права добровольные меры имеют существенное значение при рассмотрении дел и могут в принципе привести к оправданию нарушителя.

ТИПЫ НАКАЗАНИЙ

Штраф или запрет деятельности

Великобритания

Обязательные меры:

- ✓ В настоящее время все существенные обязательства операторов и обработчиков данных (процессоров) в UK GDPR и GDPR ЕС совпадают.

Рекомендуемые меры:

- ✓ Национальная система сертификации Cyber Essentials,. Схема предназначена для демонстрации того, что организация обладает минимальным уровнем защиты в области кибербезопасности посредством ежегодных аудитов для подтверждения соответствия сертификационным критериям.
- ✓ Статья 129 DPA дает ICO право использовать аудиты не только как форму расследования, но и как добровольную проверку организаций на предмет соблюдения надлежащей практики.

РЕГУЛЯРНОСТЬ ПРОЦЕДУР ПРОВЕРКИ

Ежегодно

ПРИНЦИПЫ НАЗНАЧЕНИЯ ШТРАФА ЗА УТЕЧКУ ПД

Досудебно: оценка серьёзности нарушения по уровням (низкий, средний, высокий, очень высокий), преднамеренности, расчёт стартового диапазона штрафа, оценка платёжеспособности нарушителя, оценка эффективности, соразмерности и сдерживающего воздействия.

Смягчающее - сотрудничество с органами в сфере кибербезопасности по общим вопросам безопасности государства и данных.

ТИПЫ НАКАЗАНИЙ

Оборотный штраф, который может быть значительно снижен при наличии смягчающих обстоятельств

Бразилия

Обязательные меры:

- ✓ «Общий закон о защите персональных данных Бразилии»
- ✓ «Основы соблюдения гражданских прав в онлайн-среде» (Marco Civil da Internet).

Рекомендуемые меры:

- ✓ В сфере медицины и здравоохранения действует «Кодекс медицинской этики»
- ✓ В соответствии с требованием статьи 53 LGPD, которая обязывает надзорный орган разработать и опубликовать методологию расчета размера штрафа, ANPD в октябре 2021 года представил «Регламент проведения расследований и применения административных санкций» .

РЕГУЛЯРНОСТЬ ПРОЦЕДУР ПРОВЕРКИ

Нет (по мере мониторинга и необходимости)

ПРИНЦИПЫ НАЗНАЧЕНИЯ ШТРАФА ЗА УТЕЧКУ ПД

Смягчающие:
- доказанное применение внутренних механизмов и процедур, направленных на минимизацию ущерба вследствие нарушения безопасности персональных данных в соответствии со статьей 48 (2) (II) LGPD;
-внедрение правил надлежащей практики и управления;
- оперативное принятие корректирующих мер;
- пропорциональность тяжести нарушения и интенсивности воздействия.

ТИПЫ НАКАЗАНИЙ

2% от оборота компании или группы компаний с верхней планкой 50 млн. риалов (около 600 млн рублей)
Предупреждение с установлением корректирующих мер
Запрет на обработку ПД или приостановка до устранения нарушений ИБ

Индия

Обязательные меры:

- Privacy Rules предусматривают, что одним из стандартов, которым организация может следовать для обеспечения защиты персональных данных, является международный стандарт ISO/IEC 27001 «Информационные технологии - Методы и средства обеспечения безопасности - Системы менеджмента информационной безопасности - Требования».

Рекомендуемые меры:

- Стандарт IS 17428, который Бюро по стандартизации в области конфиденциальности данных Индии выпустило в 2021 году. Стандарт дает описание структуры для разработки, внедрения, поддержки и обновления методов управления конфиденциальностью данных.

РЕГУЛЯРНОСТЬ ПРОЦЕДУР ПРОВЕРКИ

Нет

ПРИНЦИПЫ НАЗНАЧЕНИЯ ШТРАФА ЗА УТЕЧКУ ПД

Нет

ТИПЫ НАКАЗАНИЙ

Штраф 100 000 рупий и (или) заключение сроком до 1 года, а также компенсация ущерба субъекту по решению суда в случае если утекшие данные относятся к тайнам или спецкатегориям

Южная Корея

Обязательные меры:

- «Закон о защите персональной информации» (Personal Information Protection Act, PIPA) в совокупности с подзаконными актами и руководствами, выпущенными надзорными органами.

Рекомендуемые меры:

- На основании 13 ст. PIPA – Отраслевые кодексы по защите персональных данных. Система сертификации (Personal information & Information Security Management System, ISMS-P) действует с 2018 года, пройти ее может любая организация, которая хочет повысить свой уровень защиты персональных данных и снизить риски внутренних и внешних нарушений.

РЕГУЛЯРНОСТЬ ПРОЦЕДУР ПРОВЕРКИ

Раз в 3 года

ПРИНЦИПЫ НАЗНАЧЕНИЯ ШТРАФА ЗА УТЕЧКУ ПД

- Предписание
- Приостановка обработки
- Меры против должностных лиц

Надзорный орган может принять во внимание любые усилия оператора по обеспечению безопасности данных, а также меры, предпринятые для снижения последствий и статус резидента.

ТИПЫ НАКАЗАНИЙ

Нарушение обязательных требований относительно принятия мер по обеспечению безопасности - штраф в размере до 20 млн корейских вон
Штраф в размере 3% от годового оборота

Надзорный орган может принять во внимание любые усилия оператора по обеспечению безопасности данных, а также меры, предпринятые для снижения последствий и статус резидента.

DATA FUSION

FIRST RUSSIAN DATA FORUM

Вывод

Добровольные оценки соответствия повышенным требованиям по информационной безопасности являются важным механизмом в большинстве рассмотренных стран.

В свою очередь, чтобы стимулировать операторов персональных данных инвестировать в информационную безопасность посредством аудитов на соответствие повышенным требованиям в области информационной безопасности, государство берёт на себя обязательства смягчать либо исключать ответственность оператора в случае утечки при условии соответствия обязательным требованиям и подтверждённому таким аудитом соответствию дополнительным требованиям.

Такой подход позволяет существенно повысить защищённость персональных данных и сократить количество утечек.

Выводы и рекомендации

Учёт последствий для нарушителя

Учёт финансового состояния нарушителя при назначении суммы штрафа судом; и сдерживающего влияния на рынок

Добровольные обязательства

Введение механизма добровольного аудита, признание успешного прохождения такого аудита основанием для смягчения ответственности

Оценка и аудит

Разработка системы оценки в рамках добровольного аудита (основа - одобренные регулятором стандарты и методы сертификации (в том числе ISO)

Минимизация ущерба

Использование добровольных механизмов минимизации ущерба субъектам (кодексы, отраслевые соглашения, лучшие практики и тд)

При соблюдении всех мер информационной безопасности (обязательных и дополнительных), уведомлении контролирующего органа и содействии минимизации ущерба от утечки – освобождение от ответственности

DATA FUSION

FIRST RUSSIAN DATA FORUM

Спасибо за внимание!