OZON

«Мозаичный» подход международных компаний к организации обработки персональных данных в нескольких юрисдикциях

Михаил Ратушный,

Руководитель практики защиты персональных данных Ozon, Data Protection Officer, CIPP/E

Вопросы к обсуждению

01 **Экстерриториальный эффект национальных законов**

Тренд или вынужденная мера?

02 **Трансграничная передача и локализация персональных данных**

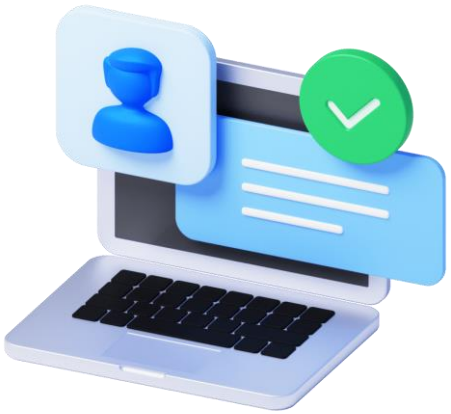
Национальные подходы и трудности

03 **Согласие на обработку персональных данных**

Истинная форма выражения воли субъекта или «каучуковое» основание

04 **Универсальные меры при работе с персональными данными**

Когда юрисдикция не имеет значения



Экстерриториальный эффект национальных законов

Основные критерии применимости

- наличие коммерческого предприятия (“establishment”) на территории целевой юрисдикции;
- таргетирование субъектов на территории целевой юрисдикции;
- мониторинг поведения субъектов на территории целевой юридискции

Проблематика

- «хромающие» отношения – несколько правопорядков «претендует» на одни и те же данные;
- разнонаправленность регуляторных требований (например, в части раскрытия информации о продавцах на маркетплейсе);
- архитектурные сложности с точки зрения обособления потоков данных;
- сложности в оформлении договорных отношений – необходимость учитывать одновременно несколько регуляторных требований, что не всегда возможно (например, в части обязанности принимать определенные технические меры)

Локализация персональных данных

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации (ч. 5 ст. 18 Федерального закона «О персональных данных»)

Первичная vs вторичная локализация

Требования о локальном хранении персональных данных в разных юрисдикциях

Вторичная локализация – последующее сохранение персональных данных в базах данных, локализованных на территории соответствующей юрисдикции*

Первичная локализация – такой сбор персональных данных, в результате которого персональные данные первоначально размещаются в базах данных, локализованных на территории соответствующей юрисдикции**

* Например, Закон Республики Казахстан «О персональных данных и их защите», а также п. 7 Положение о порядке предварительной идентификации пользователей интернет-ресурса, сетевого издания, утвержденного постановлением Совета Министров Республики Беларусь № 859

** Например, Закон Республики Узбекистан «О персональных данных», Федеральный закон «О персональных данных»

Согласие на обработку персональных данных: сходства и различия

01 В отдельных юрисдикциях является самым «слабым» основанием (например, ЕС или Республика Беларусь), в некоторых – единственным (Казахстан и Армения), а в некоторых – самым универсальным (Россия)

02 Проблема волеизъявления субъекта – активное согласие, согласие в виде бездействия и согласие в виде конклюдентных действий. Форма согласия

03 Уникальный режим персональных данных, разрешенных субъектом для распространения, в России – обязательность согласия на распространение персональных данных. Проблема соотношения с режимом «обязательного раскрытия персональных данных

07

Исключите присутствие «боевых» данных в тестовой среде

1. Тестовая среда = тестовые данные
2. Нет синхронизации с продуктивной средой либо синхронизация при условии полной обфускации данных

08

Управляйте доступами правильно

1. Модель управления доступами, соответствующая вашим потребностям
2. Централизация функции управления доступами (IDM & SSO)
3. Недопущение «ролевого» конфликта интересов
4. Отсутствие «человеческого» доступ в системы или внедрение принципов минимальных привилегий и временности доступов
5. Прямой доступ в базу и выгрузки из нее – всегда плохо

09

Знайте свои сервисы

1. Распределенное vs. централизованное хранение данных
2. Аудит сервисов до их запуска: обоснование цели и правовых оснований для обработки
3. Для внутренних сервисов – доступ только из корпоративной сети
4. Заранее установленные правила «общения» сервисов (MDM-системы и «потребляющие» системы, события и реагирование на них)
5. Реестр сервисов и метки типа «персональные данные»
6. Обучение разработчиков в доступной для них форме

10

Удаление данных

1. Удаление по запросу и автоматическое («по будильнику») удаление данных
2. Hard deletion vs. soft deletion vs. обфускация данных
3. В модели распределенного хранения данных – синхронизация в удалении
4. Неиспользуемые данные необходимо периодически удалять
5. Необходимость дальнейшего хранения для «архивных» целей – отдельная база с атрибутом «архив» с ограниченным доступом

OZON

Обрабатывайте персональные данные правильно!

E-mail: miratushniy@ozon.ru

LinkedIn: www.linkedin.com/in/mratushniy

TG: m_ratushnyy