Association of European Businesses

CHALLENGES TO EXISTING BUSINESS MODELS: IT LEGISLATION CHANGES

23 October 2014

AEB OFFICE

Association
of European
Businesses

Edgars Puzo

Chairman of the AEB IT-Telecom Committee, Chairman of the Intercommittee Working Group on Data Protection, Atos

WELCOME ADDRESS

AEB Open Event: Challenges to Existing Business Models: IT Legislation Changes, 23 October 2014, MOSCOW

Dmitry Zykov

Senior Associate, Head of Data Protection Group, Pepeliaev Group

Personal data: data processing new requirements and possible problems in the law enforcement

AEB Open Event: Challenges to Existing Business Models: IT Legislation Changes, 23 October 2014, MOSCOW

Pavel Sadovsky

Senior Associate, EPAM

Requirements to the storage of personal data: legal regulations in other jurisdictions

AEB Open Event: Challenges to Existing Business Models: IT Legislation Changes, 23 October 2014, MOSCOW

АДВОКАТСКОЕ БЮРО
ЕГОРОВ
ПУГИНСКИЙ
АФАНАСЬЕВ
И ПАРТНЕРЫ

Требования к хранению персональных данных: правовое регулирование в других юрисдикциях

Павел САДОВСКИЙ
руководитель практики IP/TMT АБ «Егоров, Пугинский, Афанасьев и Партнеры»

23.10.2014

РАЗЛИЧИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПД

- Различные подходы к правовому регулированию персональных данных *(свобода слова (США) VS конституционное право на защиту частной жизни (ЕС))*
- Регулирование передачи персональных данных в иностранные государства *(ограничение трансграничной передачи персональных данных; категории персональных данных, передача которых требует принятия особых мер)*;
- Ответственность за нарушение правил обработки персональных данных *(дифференциация размеров штрафов)*
- Права субъектов персональных данных и категории персональных данных *(право на уведомление об обработке персональных данных; права на корректировку и удаление персональных данных);*

ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ЕВРОПЕЙСКОМ СОЮЗЕ

- Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.);
- Директива Европейского Парламента и Совета Европейского Союза 95/46/EC от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных;
- законодательство государств-членов Европейского Союза

ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ЕВРОПЕЙСКОМ СОЮЗЕ

- защита фундаментальных права и свободы физических лиц (*защита права на неприкосновенность частной жизни применительно к обработке персональных данных*).
- выделение «контроллера персональных данных» и «обработчика (оператора) персональных данных»;
- применяется к персональным данным в любой форме: устной, письменной, электронной (в том числе, полученным через Интернет);
- трансграничная передача данных в третьи страны возможно только если указанные страны обеспечивают адекватный уровень защиты;
- уведомление государственного органа, уполномоченного в сфере ПД, о начале обработки персональных данных;
- ответственность в форме крупных штрафов (в среднем около € 300,000);

Персональные данные *- <u>любая</u> информация, связанная с субъектом данных;*
Субъект персональных данных *-лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификационный номер или на один или несколько факторов, отличительных для его физического, психологического, экономического, культурного или социального состояния*

ПД В США VS ПД В ЕС

США	*ЕВРОПЕЙСКИЙ СОЮЗ*
Отсутствие единого акта, унифицирующего правовое регулирование персональных данных (ПД) на федеральном уровне. Наличие ряда федеральных актов, регулирующих отдельные вопросы персональных данных (например, *The Children's Online Privacy Protection Act; The Federal Trade Commission Act; The Electronic Communications Privacy Act*).	Наличие директивы, унифицирующей основные принципы обработки ПД на территории государств-членов Европейского Союза (ЕС).
Противоречивое и неполное законодательство отдельных штатов.	Относительная гармонизация законодательств государств-членов ЕС.
Законодательство в основном сконцентрировано на защите данных несовершеннолетних и на регулировании сбора и обработки ПД при осуществлении коммерческой деятельности.	Законодательством определены категории персональных данных, на которые распространяется правовое регулирование.
На федеральном уровне отсутствует запрет на транснациональную передачу ПД.	Транснациональная передача ПД разрешена только в страны с адекватной защитой ПД.
Ответственность в форме возмещения убытков и расходов на юридические услуги	Административная ответственность в форме штрафов. В отдельных странах более строгая ответственность (например, в Финляндии – тюремное заключение на 1 год).

АДЕКВАТНАЯ ЗАЩИТА ПРАВ СУБЪЕКТА ПД

- Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (**статья 12);**
- Приказ Роскомнадзора от 15.03.2013 N 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных»
    - Государства - стороны Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (государства –члены Советы Европы, Королевство Марокко (не ратифицировало), Восточная Республика Уругвай);
    - Иные государства: Австралия; Аргентинская Республика; Государство Израиль; Канада; Королевство Марокко; Малайзия; Мексиканские Соединенные Штаты; Монголия; Новая Зеландия; Республика Ангола; Республика Бенин; Республика Кабо-Верде; Республика Корея; Республика Перу; Республика Сенегал; Тунисская Республика; Республика Чили; Специальный административный район Гонконг Китайской Народной Республики; Швейцарская Конфедерация

Германия: создание внутренних IT-систем и хранение ПД

- Предложение создать внутреннюю европейскую инфраструктуру, позволяющую хранить и обрабатывать персональные данные европейцев на территории Европейского Союза (не включая Соединенное Королевство);

- Фактически процесс локализации персональных данных на территории Германии уже локализован благодаря деятельности компании Deutsche Telecom: компания внедряет систему «немецкой почты», гарантирующую хранение всех данных на территории Германии.

- В соответствии со схемой Deutsche Telecom гражданство (местоположение) пользователя определяется по его IP адресу.

Китай

- Данные, относящиеся к частной жизни граждан КНР, охраняются в соответствии с Конституцией КНР, Гражданским Кодексом КНР, Законом о гражданской ответственности, Правилами защиты прав пользователей в области связи и сети Интернет и др. нормативными актами).
- Категории персональных данных дифференцируются в зависимости от законов, под регулирование которых они попадают (*данные пользователей сети Интернет; данные о состоянии здоровья населения и т.д.*).
- Ограничение установлено для отдельных категорий данных, в частности – для персональных данных, которые собираются коммерческими банками (банковская тайна относится к персональным данным).
- Китайская народная республика на основе внутреннего законодательства периодически направляет уведомления в крупные американские компании (Windows, Apple) с требованием локализовать хранение персональных данных на территории Китая. В случае отказа, китайские власти временно блокируют сервисы.

Индия: курс на локализацию серверов

- Сейчас трансграничная передача данных возможна, если (1) лицо, которому ПД передаются, обеспечивает защиту ПД в соответствии с индийским законодательством; (2) между контроллером ПД и субъектом ПД заключен соответствующий договор; (3) субъект ПД выразил свое согласие на такую передачу.
- Концепция Национального Совета по Безопасности Индии от февраля 2014 г.:
  - Локализация серверов, хранящих персональные данные;
  - Ограничения на копирование персональных данных и их трансграничную передачу в иностранные юрисдикции.
- Предполагается, что требования будут распространятся на все данные, исходящие с территории Индии.

Бразилия: альтернативное регулирование

- Принятие бразильского «Билля о правах в сфере Интернет» (Marca Civil da Internet) в апреле 2014 г.
- Экстерриториальное действие бразильского права в отношении обработки персональных данных граждан Бразилии в иностранных юрисдикциях;
- Наложение штрафов в размере 10% от годовой прибыли или запрет на осуществлении деятельности на территории Бразилии для операторов, деятельность которых осуществляется не в соответствии с бразильским правом.
- Возможность принятия Закона о защите персональных данных, в соответствии с которым вводятся ограничения на хранение данных бразильских граждан за границей, а также копирование данных на иностранные серверы.

Другие страны

- В Индонезии в 2012 были приняты поправки, в соответствии с которыми все провайдеры, оказывающие «публичные услуги», должны хранить данные на территории Индонезии (Постановление № 82). Отсутствуют официальные разъяснения понятия «публичные услуги» в контексте новых правил. В соответствии с другим законом Индонезии под ними понимаются «любые услуги, способствующие благополучию населения». Пока иностранные компании исходят из подобной широкой формулировки.
- Комиссия по финансовым услугам Республики Корея рассматривает возможность ограничить трансграничную передачу данных, относящихся к финансовому положению физических лиц. Предполагается, что данная информация подлежит хранению исключительно на территории Республики Корея.

СПАСИБО ЗА ВНИМАНИЕ!

119017, Россия, Москва,
ул. Большая Ордынка,
д. 40, стр. 4

Тел.: +7 (495) 935 80 10
Факс: +7 (495) 935 80 11
www.epam.ru

Павел Садовский,
pavel_sadovsky@epam.ru

Denis Seleznev

General Director, 1 Forma

Practical steps in preparing IT system for the work according to 242 FL

AEB Open Event: Challenges to Existing Business Models: IT Legislation Changes, 23 October 2014, MOSCOW

Практические шаги подготовки информационной системы к работе в соответствии с 242-ФЗ

Денис Селезнёв,

Генеральный директор,
1Форма

Первая Форма
система управления

ИТ архитектура – инвентаризация

- Где мы обрабатываем персональные данные?
- Технологические возможности обработки персональных данных – ЦОД, ресурсы и программное обеспечение
- Каналы связи – достаточность и резервирование
- Резервное копирование и планы восстановления
- Какое ещё прикладное программное обеспечение мы используем для обработки персональных данных?

Правовая позиция и регламенты

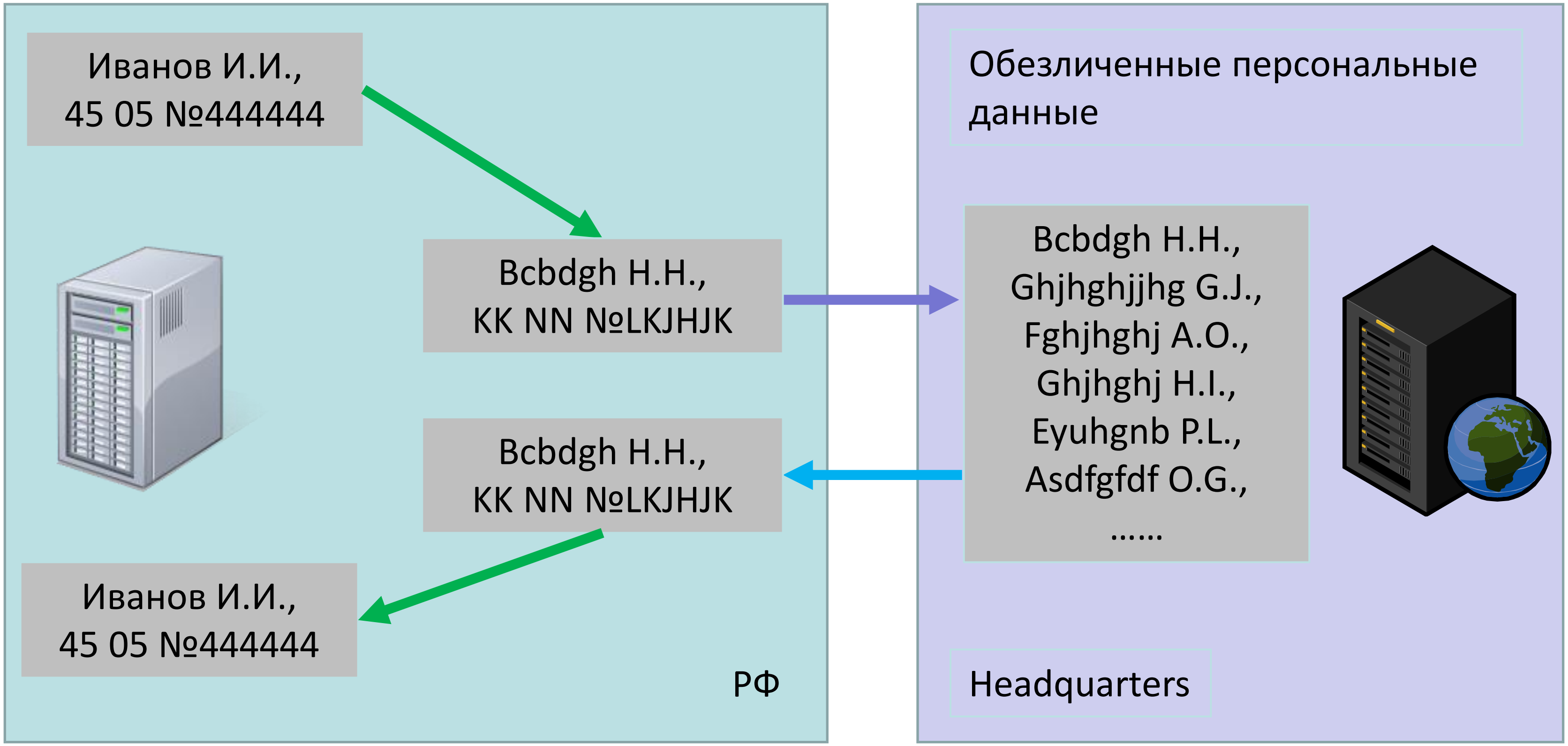
- Кто в организации несёт ответственность за исполнение 242-ФЗ?
- В рамках каких договорных отношений с «третьей стороной» мы можем нарушить 242-ФЗ?
  - Операторы связи
  - Дата центры (ЦОД)
  - Облачные провайдеры
  - Shadow IT
- Каким образом будут выявлены и задокументированы нарушения 242-ФЗ?

Ближайшие шаги

- Определить список приложений и баз данных, которые должны находится на территории РФ.
- Создать проект и бюджет технического решения. ЦОД, каналы связи, ресурсы на обслуживание.
- Провести инвентаризацию договорной базы.

- Использовать DLP решения для анализа распространения персональных данных за пределы РФ
- Рассмотреть быстрые программные решения по обезличиванию персональных данных

Обезличивание данных в РФ, хранение за рубежом



Иванов И.И.,
45 05 №444444

Bcbdgh H.H.,
KK NN №LKJHJK

Bcbdgh H.H.,
KK NN №LKJHJK

Иванов И.И.,
45 05 №444444

РФ

Обезличенные персональные данные

Bcbdgh H.H.,
Ghjhghjjhg G.J.,
Fghjhghj A.O.,
Ghjhghj H.I.,
Eyuhgnb P.L.,
Asdfgfdf O.G.,
……

Headquarters

Association of European Businesses

Alexander Bobryshev

IT Business Analyst, GM-Russia

Changes in the IT model of foreign company due to the new law implementation

AEB Open Event: Challenges to Existing Business Models: IT Legislation Changes, 23 October 2014, MOSCOW

Александр Бобрышев

Бизнес-аналитик, GM Russia & CIS

Планирование изменений IT-модели работы иностранного предприятия в связи с принятием закона 242-ФЗ

Открытые вопросы закона, требующие уточнения

- В законе 242-ФЗ нет упоминания о категориях персональных данных, на которые распространяется действие закона. Означает ли это, что закон распространяется на все 4 категории персональных данных, включая обезличенные или общедоступные персональные данные граждан РФ?

- Попадают ли под действие закона контактные данные контрагентов, или скажем, сотрудников компании, давших согласие на размещение персональных данных в соответствующих общедоступных источниках персональных данных? (Статья 8 152-ФЗ)

План действий по изменению IT-ландшафта

1. Идентификация систем, содержащих персональные данные, страна размещения, ответственные лица со стороны ИТ и бизнеса.
2. Как используются персональные данные в системе?
3. Риск-анализ, оценка последствий для бизнеса.
4. Определение предлагаемого подхода по миграции.
5. Оценка стоимости и длительности каждого из проектов.
6. Принятие решения о переносе, начале проекта.

Выбор подхода для различных типов информационных систем, модель оценки

1. Определение, являются ли данные в системе персональными, необходимыми для переноса.
2. Удаление персональных данных из ИС.
3. Замена данных в корневой системе на идентификаторы; хранение соответствующих им персональных данных на территории РФ.
4. Перенос БД без ре-хостинга приложения.
5. Ре-хостинг ИС (или части приложения) на территорию РФ.
6. Переход на новое приложение, размещенное на территории РФ.
7. Изменение, остановка конкретного бизнес-процесса.

Перенос инфраструктурных подсистем на территорию РФ

- Каталоги аутентификации и авторизации
- Системы синхронизации каталогов
- Системы организации единого доступа
- Портальные решения
- Почтовые службы
- Мгновенные сообщения

Panelists

Taras Derkatsch, *Senior Associate, BEITEN BURKHARDT, AHK*

Andrey Slepov, *Senior Associate, BEITEN BURKHARDT, AHK*

Pavel Sundeev, *MTS*

Panelists

Alexander Onischuk, President, *RATEK*

Yury Dombrovsky, *Member of the Commission for telecommunications and information technologies - RSPP*

Panelists

Ron Lewin, ***Managing Director, TerraLink, Co-Chairman of Innovation & Technology Committee, AmCham***

Q&A