МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

INTEGRITY. COMPLIANCE.
SAMSUNG

Исполнение ФЗ-242
Практика переноса сервисных БД

Samsung Electronics Russia
2015

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Содержание:

Обеспечение исполнения требований ФЗ-242

1. Предварительная работа и оценка рисков
2. Организационные шаги
3. Работа по проекту
   - Оценка систем
   - Взаимодействие с регуляторами
   - Техническое решение
   - Миграция
4. Q&A

INTEGRITY. COMPLIANCE.
SAMSUNG

Предварительная работа
Оценка рисков

INTEGRITY. COMPLIANCE.
SAMSUNG

Выявление и информирование

Задача: довести реальность проблемы до топ-менеджмента.

- Ответственный за организацию обработки ПДн
- Compliance
- Комитет по управлению регуляторными рисками
  - оценка риска
  - влияние на бизнес-процессы
  - финансовая составляющая

Внешний консалтинг

Готова ли компания доверить проект целиком сторонним консультантам?

Сложности

Размер компании: 1
- распределенная структура
- иностранное руководство
- режим коммерческой тайны
- глобальные корпоративные политики
- обособленность IT-подразделений

Отсутствие единого толкования закона 2
- «трудности перевода»
- шум в СМИ

Широкая проблематика темы 3
- затронуты разные отделы
- нет единого «уполномоченного» центра

Организационные шаги

Создание рабочей группы

Большое количество затрагиваемых процессов требует создания единого координационного центра.

Состав

“Big boss”: формальный руководитель группы, основной административный ресурс

Core
- Ответственный за организацию обработки ПДн
- Compliance
- Юрист
- IT администратор
- ИБ (ответственный за безопасность ПДн)

Из постоянного состава назначается:

• руководитель группы

• ответственный за связь с регуляторами

Полномочия

В зависимости от сложившейся практики управления:

- Официальный приказ
- Информирование руководителей подразделений на совещании, встрече, и т.д.
- Необходимые NDA и допуск к конфиденциальной информации

Работа по проекту

INTEGRITY. COMPLIANCE.
SAMSUNG

- Управление и контроль проектом, как принято в компании
- Подключение необходимых специалистов на различных этапах
- Регулярное информирование руководства и контроль бюджета

ОЦЕНКА СИСТЕМ

1

- Перечень ИСПДн
- Оптимизация
- Финальный список
- Регуляторы

ТЕХНИЧЕСКОЕ РЕШЕНИЕ

2

- Оценка объемов
- Варианты размещения
- Оценка бюджета
- Тех проект
- Тендеры / закупки

МИГРАЦИЯ

3

- Подготовка инфраструктуры
- Запуск и тестирование
- Перенос архивов
- Изменения в документации

Оценка систем

- Передача данных в HQ – необходимость
- Трансграничная передача данных не запрещена
- БД, в которой при сборе происходит обработка ПДн, должна быть в России*

Этапы оценки

Необходимо взаимодействие IT и Compliance. Двойственное понимание термина «система» как IT элемента и как ИСПДн.

- Цель сбора
- Место сбора
- Взаимодействие IT-систем
- Оптимизация
- Исключения (пп. **2***,3,4,8 ч.1 ст.6 ФЗ-152)

Результат

Резюме по каждой системе.
Перечень БД и неотделимых IT-элементов для переноса.
Консультации с регуляторами

Взаимодействие с регуляторами

INTEGRITY. COMPLIANCE.
SAMSUNG

Регуляторы:

- Министерство связи и массовых коммуникаций РФ
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
- Федеральная служба по техническому и экспортному контролю
- Федеральная служба безопасности Российской Федерации

Способы взаимодействия:

- Официальный письменный запрос
- Участие в тематических мероприятиях
- Организация прямых встреч
- Онлайн ресурсы:
  - http://minsvyaz.ru/ru/personaldata/
  - http://pd.rkn.gov.ru/faq/
  - Регионы: http://35.rkn.gov.ru/p5668/ (Вологодская обл.)

Практика взаимодействия

РОСКОМНАДЗОР

- Научно-практический комментарий 2015 г.
- Многочисленные конференции
- Встреча с руководством
- Рабочие консультации

- Детальный вопрос – детальный ответ
- Готовность к сотрудничеству и диалогу



Техническое решение

INTEGRITY. COMPLIANCE.
SAMSUNG

1 Расширение имеющейся инфраструктуры

2 Аренда дата-центра

3 Создание дата-центра

Оценка вариантов решения

- Объемы данных
  - Прогнозы развития
  - Необходимость переноса архива
- Требования к защите:
  - Законодательство
  - Корпоративные политики
  - Требования ИБ
- Перспективы бизнеса

Выбор дата-центра

- Tier III и выше (Uptime Institute)
- Соответствие требованиям законодательства
- Доступность
- Только от собственника
- Соответствие корпоративным требованиям
- Стоимость

Выбор оборудования

- Эксперты из HQ
- Корпоративные стандарты
- Проверка соответствия требованиям Российского закона*
- Доступность на территории России и тех.поддержка

Тех. проект
Бюджет и утверждение

→

Тендеры
В соответствии с внутренними политиками

→

Закупки
Подписание договоров

Миграция

INTEGRITY. COMPLIANCE.
SAMSUNG

Подготовка инфраструктуры

Монтаж и установка технических средств

Установка и тестирование ПО

2 системы работают в параллельном режиме

Перенос архива

Отключение дублирующей системы

Российский сегмент отключен от системы за рубежом

Изменения в документации по ПДн

- Ответственный за организацию обработки ПДн должен подать изменения в Роскомнадзор

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

INTEGRITY. COMPLIANCE.
SAMSUNG

Q&A

Samsung Electronics Russia 2015

Контакты: Цветков Алексей
a.tswetkov@samsung.com