Практическая оценка рисков обработки персональных данных

При запуске и изменении бизнес-процессов

ФАКТЫ / МЕРЫ / РЕШЕНИЕ



Анастасия Солдатова
DPO ВТБ Лизинг

Знание нормы нужно перевести в условия работы

Юридический вывод

Цель и основание обработки
Роли участников
Применимые требования



Реализация

Что передаёт система
Кто и как получает доступ
Чем подтвердить ограничение



СОГЛАСОВАНИЕ ДОЛЖНО ОБЪЯСНЯТЬ, ЧТО РЕАЛИЗОВАТЬ И КАК ПРОВЕРИТЬ

«Нам всего лишь открыть доступ»



Первоначальный запрос:

подключить новую команду
к записям обращений

При уточнении появляются:

выгрузка, внешняя расшифровка,
аналитика работы сотрудников

ОДНА ЗАЯВКА МОЖЕТ СОДЕРЖАТЬ НЕСКОЛЬКО РАЗНЫХ ИЗМЕНЕНИЙ

Маршрут данных определяет вопросы проверки

1

Запись

Какие обращения?
Кто выбирает файл?

2

Передача

Какой получатель?
Какие посредники?

3

Расшифровка

Где аудио и текст?
Кто имеет доступ?

4

Применение

Для какой задачи?
Когда удалить копии?

НУЖНЫ ФАКТЫ, КОТОРЫЕ СПОСОБНЫ ИЗМЕНИТЬ ВЫВОД

Глубина проверки зависит от изменения

Короткая проверка	Углублённая проверка
Стандартная роль в ранее оценённом процессе	Новый получатель или внешний сервис
Цель и операции остаются в проверенных границах	Новая цель или влияние результата на человека
Есть подтверждения действующих ограничений	Массовая выгрузка или неподтверждённые ограничения

МАЛЫЙ ОБЪЁМ ПИЛОТА САМ ПО СЕБЕ НЕ ОЗНАЧАЕТ НИЗКИЙ РИСК

Нарушение, неизвестность и риск требуют разных действий

Нет обязательного условия

Изменить правовую или фактическую модель

!

Не хватает фактов

Установить получателей, операции и условия

?

Возможен вред

Оценить последствия и подобрать меры



ОДИН КРАСНЫЙ СТАТУС НЕ ОБЪЯСНЯЕТ, ЧТО ИМЕННО ДЕЛАТЬ

Один сервис создаёт разные сценарии риска

Событие	Последствие	На что воздействовать
Доступ к чужой записи	Раскрытие содержания разговора	Выборка и права доступа
Ошибка расшифровки	Неверный ответ или вывод о человеке	Сверка с аудио и правила использования
Копия остаётся после задачи	Дальнейшее ненужное использование	Срок и механизм удаления

ПРОВЕРЯЕМ ПОСЛЕДСТВИЯ ОБРАБОТКИ, ДАЖЕ ЕСЛИ ВНЕШНЕЙ УТЕЧКИ НЕТ

Одно событие имеет несколько последствий

СОБЫТИЕ: СОТРУДНИК ПОЛУЧИЛ ДОСТУП К ЧУЖОЙ ЗАПИСИ РАЗГОВОРА

Регуляторные

Жалоба и проверка обстоятельств.
Меры реагирования при наличии оснований.

Финансовые

Расходы на расследование, исправление
и дополнительный контроль.

Операционные

Приостановка передачи записей.
Ручная проверка и задержки в работе.

Репутационные

Снижение доверия клиентов
и партнёров к работе с их данными.

ОЦЕНКА СВЯЗЫВАЕТ ВРЕД ЧЕЛОВЕКУ С ПОСЛЕДСТВИЯМИ ДЛЯ КОМПАНИИ

Учебный пример. Возможные последствия зависят от обстоятельств

«Без расшифровки проект не решает задачу»

Исходный вариант



Общий архив

Доступ всех групп

Весь архив
Все функции сразу

Вариант для проверки



Группа А



Группа Б

Только назначенные обращения
Поиск по тексту без оценки сотрудников

СРАВНИВАЕМ СПОСОБЫ ПОЛУЧИТЬ НУЖНЫЙ РЕЗУЛЬТАТ

Временная мера должна выдерживать реальную нагрузку

Что улучшили

Изоляция групп ограничивает доступ к чужим обращениям.

Результат подтверждаем тестом.

Что осталось

Ручной выбор файла может привести к ошибочной передаче.

Нужна проверка подборки.

МЕРА ПОЛЕЗНА, ЕСЛИ ВЫПОЛНИМА И ВЛИЯЕТ НА ПРИЧИНУ РИСКА

Проверяем и разрешённое, и запрещённое действие

//01 **Своё обращение**
Открывается и решает рабочую задачу

//02 **Чужая запись**
Недоступна другой группе

//03 **Ссылка и выгрузка**
Сохраняют ограничение доступа

//04 **Завершение хранения**
Работает порядок удаления



СКРЫТОЕ ПОЛЕ НА ЭКРАНЕ НЕ ДОКАЗЫВАЕТ ОГРАНИЧЕНИЕ ЭКСПОРТА

Условия запуска должны быть исполнимыми

Условие	Кто подтверждает	Что сохраняем
Объём и участники	Владелец процесса	Описание выбранного сценария
Основания и договорная модель	DPO и юристы	Вывод по конкретной обработке
Изоляция и маршрут	Назначенные ИТ и ИБ специалисты	Результаты проверки
Ручной контроль передачи	Владелец процесса	Порядок и проверка выполнимости

В РАБОЧЕМ РЕШЕНИИ НУЖНЫ КОНКРЕТНЫЕ ИСПОЛНИТЕЛИ И СРОКИ

Остаточный риск требует решения и контроля

Остаточный риск - риск, который сохраняется после принятых мер

Задача	Кто участвует	Что фиксируем
Оценить оставшийся риск	DPO и юристы с ИТ, ИБ и владельцем процесса	Сценарий, последствия, меры и их ограничения
Принять решение о запуске	Уполномоченный руководитель или коллегиальный орган	Границы запуска, условия и решение по риску
Выполнить меры	Назначенные исполнители	Сроки и подтверждения выполнения
Отслеживать и пересматривать	Назначенный владелец риска во взаимодействии с DPO, ИТ и ИБ	Контрольные показатели, дата и основания пересмотра

Выход за пределы полномочий требует передачи решения выше

Пример распределения ролей. Адаптируется к полномочиям в компании

Согласование фиксирует границы решения

Объём	Расшифровка назначенных обращений для поиска
Условия	Основания, изоляция, передача и хранение подтверждены
Остаточный риск	Ошибка ручного выбора файла или получателя
Пересмотр	Новый объём, цель, получатель или функциональность

ИТОГ ОБЪЯСНЯЕТ: ЧТО ЗАПУСКАЕМ, ПОЧЕМУ И ПРИ КАКИХ ОГРАНИЧЕНИЯХ

Расширение запуска требует новой проверки мер

//01

До расширения

Проверить ошибки передачи и контроль.

Оценить меры при новой нагрузке.

//02

Условия остановки

Нарушена изоляция пространств.

Контроль не справляется
с объёмом передачи.

ОТСУТСТВИЕ ЖАЛОБ НЕ ЗАМЕНЯЕТ ПОДТВЕРЖДЕНИЕ РАБОТЫ МЕР

Проверка завершена, когда решение можно объяснить

ФАКТЫ УСТАНОВЛЕНЫ

ТРЕБОВАНИЯ РАССМОТРЕНЫ

УСЛОВИЯ ВЫПОЛНЕНЫ И ПОДТВЕРЖДЕНЫ

ОСТАВШИЕСЯ ОГРАНИЧЕНИЯ ПОНЯТНЫ



Почему допустим этот вариант и что потребует пересмотра?

ОБСУДИМ ВАШИ ВОПРОСЫ

Вопросы для первичной проверки изменения

Что выяснить	Для чего выясняем
Что изменилось в задаче и операциях?	Определить границы новой оценки
Какие данные и чьи интересы затронуты?	Оценить состав и последствия
Куда идут данные и кто их использует?	Проверить получателей и маршрут
Какие копии остаются и на какой срок?	Охватить завершение обработки
Какие прежние выводы ещё применимы?	Не повторять проверку без причины

Карточка решения по конкретному варианту

Поле	Что записать
Сценарий	Цель, операции, системы, участники и объём
Условия до запуска	Мера, исполнитель, срок, подтверждение
Остаточный риск	Событие, последствия, действующие ограничения
Полномочия	Кто принимает решение и на каком основании
Пересмотр	Дата, изменение объёма или функций, критерий остановки

Источники и границы применения

01 / Правовая проверка конкретного процесса

152-ФЗ: цели, основания, роли и условия обработки проверяются отдельно.
Эта презентация не устанавливает правомерность конкретной услуги.

02 / Методические ориентиры

NISTIR 8062, § 3.2 - последствия обработки для человека.
EDPB Guidelines 4/2019 - эффективность и пересмотр мер.
Зарубежные подходы не представлены как обязательные нормы РФ.

КЕЙС И КАРТОЧКА РЕШЕНИЯ - АВТОРСКИЙ СИНТЕЗ, НЕ ОПИСАНИЕ ВНЕДРЕНИЯ