

Privacy-совестливый оператор

Чтобы избежать штрафов за утечку, придется доказать сперва Роскомнадзору, а затем и суду, что хотя утечка и произошла, в этом нет вашей вины. Почему? Потому что все, что можно и нужно было сделать для предотвращения утечки и минимизации ее последствий, вы своевременно и в полном объеме сделали. Итого, есть две группы доказательств, которые необходимо собрать: (1) доказательства рутинных privacy-процедур по предотвращению утечек и (2) доказательства надлежащего реагирования на утечку для минимизации ее последствий. Этот чек-лист дает примеры доказательств из первой группы. Скоро поделимся примерами доказательств по второй.

Контроль

Артефакт и уровень соответствия

Зона ответственности

Регулярный контроль процессов обработки ПД

- План и акты внутренних проверок ПД
- Планы устранения выявленных нарушений
- Отчеты об устранении выявленных нарушений

DPO

Актуализация ЛНА, RoPA, сведений в реестре

- Ежегодные планы актуализации ЛНА
- Список триггеров актуализации RoPA и сведений в реестре РКН
- RACI-матрица с обязанностями по актуализации
- Отчеты об устранении выявленных нарушений

DPO

Контроль внедрения новых процессов, ИТ-систем

- Оповещение о наличии DPO и ИБ-отдела в компании и их роли
- Регулярные встречи с бизнес-командами и протоколы по итогам встреч
- Анкеты или чек-листы проверки новых ИТ-систем и процессов

DPO + ИБ

Контроль

Артефакт
и уровень соответствияЗона
ответственности

Privacy-контроль контрагентов

- Стандартные оговорки о ПД в договоры с контрагентами
- Регламент privacy-проверки новых контрагентов
- Заполненные анкеты новых контрагентов и их обновление
- Иные артефакты проверки контрагентов (переписка и т.п.)
- Privacy-playbook по привлечению контрагентов

DPO

Внедрение и периодический контроль системы защиты ПД

- Модель угроз ИСПД
- Акт определения УЗ
- Проект СЗПД
- Описание применяемых средств и мероприятий по защите ПД в системах
- Политика в области ИБ
- Регламент мониторинга и предотвращения инцидентов
- Акты оценки эффективности
- Приказ о внедрении конкретных СЗИ и эксплуатационной документации
- Регламент обновления и актуализации средств защиты
- Результаты пентестов и аудитов ИБ

ИБ

Минимизация обрабатываемых ПД

- Акты / журналы уничтожения ПД
- Описи дел, переданных в архив и акты архивации
- Описание и/или чек-листы бизнес и функциональных требований
- Одобрение состава собираемых ПД от DPO
- Privacy-playbook по уничтожению ПД

DPO

Контроль**Артефакт**
и уровень соответствия**Зона**
ответственности

Контроль доступа к данным

- Матрицы доступов и порядок их актуализации
- Порядок предоставления учетных записей третьим лицам
- Двухфакторная аутентификация
- Регламент создания и блокировки учетных записей
- Лог-файлы действий в системах

ИБ

Проверка знаний работников

- Планы проведения тренингов / учений
- Материалы тренингов / учений
- Результаты проведения тренингов / учений
- Листы / логи прохождения тренинга
- Акты о проведении внеочередных контролей работников, проваливших учения
- Результаты «пересдачи»

DPO + ИБ

Внедрение и тестирование рабочих процедур и контролей по реагированию на инциденты

- Процедура информирования РКН и иных регуляторов об инциденте
- Акты о проведении учений по реагированию на инциденты
- Privacy-playbook по процедурам реагирования в случае утечки ПД

DPO + ИБ

Настоящий документ не является результатом оказания юридических услуг. Если вам необходима полноценная консультация, мы будем рады помочь.



Артем Дмитриев
Управляющий партнер

artem.dmitriev@comply.ru
t.me/artymitriev
+7 (961) 806 27-76

Comply.

ООО «Комплаенс Офис»
Comply.ru info@comply.ru
t.me/comply_ru