# Чек-лист 1 V. 1.3
# 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 всё, что можно и нужно было сделать для предотвращения утечки и минимизации ее последствий, вы своевременно и в полном объеме сделали.

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.

Ниже чек-лист с примерами доказательств первой группы, а здесь – второй.

| **Контроль** | **Артефакт** и уровень соответствия | **Зона** ответственности |
|---|---|---|
| Регулярный контроль процессов обработки ПД | • План и акты внутренних проверок ПД<br>• Планы устранения выявленных нарушений<br>• Отчеты об устранении выявленных нарушений | • DPO<br>• Legal |
| Актуализация ЛНА, RoPA, сведений в реестре | • Ежегодные планы актуализации ЛНА<br>• Список триггеров актуализации RoPA и сведений в реестре РКН<br>• RACI-матрица с обязанностями по актуализации<br>• Отчеты об устранении отклонений | • DPO<br>• Legal |
| Контроль внедрения новых процессов, ИТ-систем | • Оповещение о наличии DPO и ИБ-отдела в компании и их роли<br>• Регулярные встречи с бизнес-командами и протоколы по итогам встреч<br>• Анкеты или чек-листы проверки новых ИТ-систем и процессов | • DPO<br>• ИБ |

| Контроль | Артефакт<br>и уровень соответствия | Зона<br>ответственности |
|---|---|---|
| Privacy-контроль контрагентов | • Стандартные оговорки о ПД в договорах с контрагентами<br>• Регламент privacy-проверки новых контрагентов<br>• Заполненные анкеты новых контрагентов и их обновление<br>• Иные артефакты проверки контрагентов (переписка и т.п.)<br>• Privacy-playbook по привлечению контрагентов | • DPO |
| Внедрение и периодический контроль системы защиты ПД | • Модель угроз ИСПД (вкл. атаку хакера)<br>• Акт определения УЗ<br>• Проект СЗПД<br>• Описание применяемых средств и мероприятий по защите ПД в системах<br>• Политика в области ИБ<br>• Регламент мониторинга и предотвращения инцидентов<br>• Акты оценки эффективности<br>• Приказы о внедрении конкретных систем и средств защиты<br>• Регламент обновления и актуализации средств защиты<br>• Учет и фиксация расходов на защиту ПД<br>• Результаты пентестов и аудитов ИБ<br>• Аттестация ИСПД | • ИБ |
| Минимизация обрабатываемых ПД | • Акты / журналы уничтожения ПД (в том числе контрагентами)<br>• Описи дел, переданных в архив и акты архивации<br>• Описание и/или чек-листы бизнес и функциональных требований<br>• Одобрение состава собираемых ПД от DPO<br>• Privacy-playbook по уничтожению ПД | • DPO<br>• Legal |

| Контроль | Артефакт<br>и уровень соответствия | Зона<br>ответственности |
|---|---|---|
| Контроль доступа к данным | • Матрицы доступов и порядок их актуализации<br>• Порядок предоставления учетных записей третьим лицам<br>• Двухфакторная аутентификация<br>• Регламент создания и блокировки учетных записей<br>• Лог-файлы действий в системах | • ИБ |
| Проверка знаний работников | • Планы проведения тренингов / учений<br>• Материалы тренингов / учений<br>• Результаты проведения тренингов / учений<br>• Листы / логи прохождения тренинга<br>• Акты о проведении внеочередных контролей работников, проваливших учения<br>• Результаты «пересдачи» | • DPO<br>• ИБ |
| Внедрение и тестирование рабочих процедур и контролей по реагированию на инциденты | • Процедура информирования РКН и иных регуляторов об инциденте<br>• Акты о проведении учений по реагированию на инциденты<br>• Privacy-playbook по типам угроз / инцидентов | • DPO<br>• ИБ |
| Минимизация рисков | • Киберстраховка обработчика (в части рисков перед заказчиком)<br>• Адаптация ДИ и иных документов работников для управления уголовно-правовыми рисками<br>• Договоры с контрагентами включают нормы об эксцессе исполнителя и его последствиях | • DPO<br>• ИБ |



**Артем Дмитриев**
Управляющий партнер

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

Comply.

Comply.ru
info@comply.ru
t.me/comply_ru