Comply.

Чек-лист Privacy-совестливый оператор

v 1.3 / апрель 2026

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.

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.

Процедуры до утечки ПД

Чек-лист с примерами доказательств первой группы.

Базовый уровень Средний уровень Высокий уровень

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** • **Legal**
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 отклонений	• **DPO** • **Legal**
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 соответствия	Зона ответственности
Privacy-контроль контрагентов	• Стандартные оговорки о ПД в договорах 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 (вкл. атаку хакера) • 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 • Приказы о внедрении конкретных систем и средств защиты • Регламент обновления и актуализации средств защиты • Учет и фиксация расходов на защиту ПД • Результаты пентестов и аудитов ИБ • Аттестация ИСПД	• **ИБ**
Минимизация обрабатываемых ПД	• Акты / журналы уничтожения ПД (в том числе контрагентами) • 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** • **Legal**

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 типам угроз / инцидентов	• **DPO** • **ИБ**
Минимизация рисков	• Киберстраховка обработчика (в части рисков перед заказчиком) • Адаптация ДИ и иных документов работников для управления уголовно-правовыми рисками • Договоры с контрагентами включают нормы об эксцессе исполнителя и его последствиях	• **DPO** • **ИБ**

Реагирование на утечку ПД

Чек-лист с примерами доказательств второй группы.

Базовый уровень Средний уровень Высокий уровень

Контроль	Артефакт и уровень соответствия	Зона ответственности
Остановка утечки	• Приказ/распоряжение о принятии экстренных мер (отключение / консервация системы /сервера, вкл. компоненты горизонтального перемещения / повышения привилегий злоумышленника, сброс паролей и т.д.) • Архив собранных логов всех системных компонентов на всех уровнях за период инцидента с метками времени • Отчеты SIEM/SOC/NAC/WAF о срабатывании автоматических правил блокировки / изоляции	• **ИБ** • **ИТ**
Мониторинг и противодействие публикациям утекших данных	• Скриншоты / выписки найденных утечек на открытых площадках, отчет о результатах мониторинга утечек • Отправленные требования владельцу / админу ресурса о снятии данных с публикации • Подтверждение удаления / снятия данных с публикации	• **ИБ** • **Legal**
Создание рабочей группы и оценка инцидента	• Фиксация даты и времени обнаружения инцидента (служебная записка, email отчет и др.) • Отчет с оценкой нарушения прав субъектов ПД, причинами инцидента, атрибутами скомпрометированных ПД • Документирование создания рабочей группы • «Карта воздействия» сценариев злоупотребления данными • Доказательства сложности атаки и использования ранее неизвестных уязвимостей	• **Руководство** • **DPO** • **ИБ** • **Legal**

Контроль	Артефакт и уровень соответствия	Зона ответственности
Работа с контрагентами (если применимо)	• Уведомление контрагента об инциденте с требованием проверки (тикет, email и др.) • Акт о выявленных нарушениях договора (NDA, SLA по ИБ, поручение) с приложением доказательств • Расторжение договора и/или претензия о компенсации убытков / неустойке по договору • Заключение договора с резервным вендором • Направление вовлеченным поставщикам и партнерам писем о компрометации данных с целью принятия мер реагирования • Киберфорензик отчет по системе контрагента	• **DPO** • **Legal** • **ИБ** • **Бизнес-подразделения**
Уведомление регулятора*	• Зарегистрированные отправленные уведомления (24 / 72 часа) • Актуализация ранее поданного уведомления (новые сведения, объем ПД и др.)	• **Руководство** • **DPO** • **ИБ**
Информирование субъектов ПД (если применимо)	• Уведомление субъектов ПД (с логами рассылки, шаблонами и др.) • Публичное размещение пресс-релиза (PR-коммюнике) на официальном сайте • Усиление первой линии для обработки запросов субъектов (скрипты чат-бота, горячая линия и т.д.) • Журналирование обращений / жалоб субъектов • Утвержденная программа поддержки субъектов (партнерские программы, льготы, компенсации) • Доказательства добровольной компенсации пострадавшим из-за утечки	• **DPO** • **PR/Коммуникации** • **Legal**

* В случае нарушения прав субъектов ПД оператор подает уведомление регулятору о возникшей утечке. При этом необходимо учитывать особенности регулирования в зависимости от типа деятельности, например, кредитные организации дополнительно обязаны уведомить Банк России.

Контроль	**Артефакт** и уровень соответствия	**Зона** ответственности
Преследование нарушителя	• Отчет с версией инцидента (вкл. потенциально виновных) в утечке правомерно собранных ПД • Заявление в полицию: регистрация в КУСП (Книга учета сообщений о происшествиях) --- • Постановление о возбуждении уголовного дела • Распоряжение о применении дисциплинарного взыскания для внутреннего нарушителя	• **Legal** • **Руководство** (при поддержке ИБ)
Исправление	• Досье инцидента: хронология, действия, решения, коммуникации, RCA, исправления, профилактики • Утвержденная дорожная карта исправлений (RACI, сроки, ресурсы, приоритеты) --- • Отчет о выполнении дорожной карты исправлений • Отчеты пентестов на исправленных системах (внутренний и внешний) • Подтверждение повышения осведомленности привилегированных и простых пользователей (отчеты о тренингах, результаты тестирования и т.д.)	• **Координатор рабочей группы** (DPO/ИБ) • **Legal** • **Бизнес - подразделения**

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
max.ru/comply