Данные утекли, но я НЕ виноват

Артем Дмитриев
Управляющий партнер, Comply

t.me/comply_ru

comply.ru

Ужесточение контекста

15.10.2025

Завершение моратория на внеплановые проверки РКН

01.01.2025

Уголовная ответственность за утечку по ст. 272.1 УК

11.12.2024

Штрафы **3 – 15 млн ₽** за 1ю и **25 – 500 млн ₽** за 2ю утечку

30.05.2025

Расследование РКН кроме внеплановых проверок

30.05.2025

Privacy-**ОСАГО** от утечек

2026

Упрощение подачи **коллективных исков**

2026

Увеличение штрафа в т.ч. за **1-ю утечку** до **25 млн ₽**

2027

Увеличение **сроков давности** привлечения к ответственности

2027

2024 2025 2026 2027

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

Comply.

Что такое утечка?

ч. **11** ст. 13.11 **КоАП** / ч. **3.1** ст. 21 **152-ФЗ**

ч. **12-18** ст. 13.11 **КоАП**

1 **передача** ПД (предоставление, распространение, доступ) 2 **неправомерная** / случайная 3 повлекшая **нарушение прав** субъектов ПД

- Неправомерное копирование ПД
- Копия БД в Интернете
- Получены угрозы раскрытия ПД

Даже одного субъекта ПД

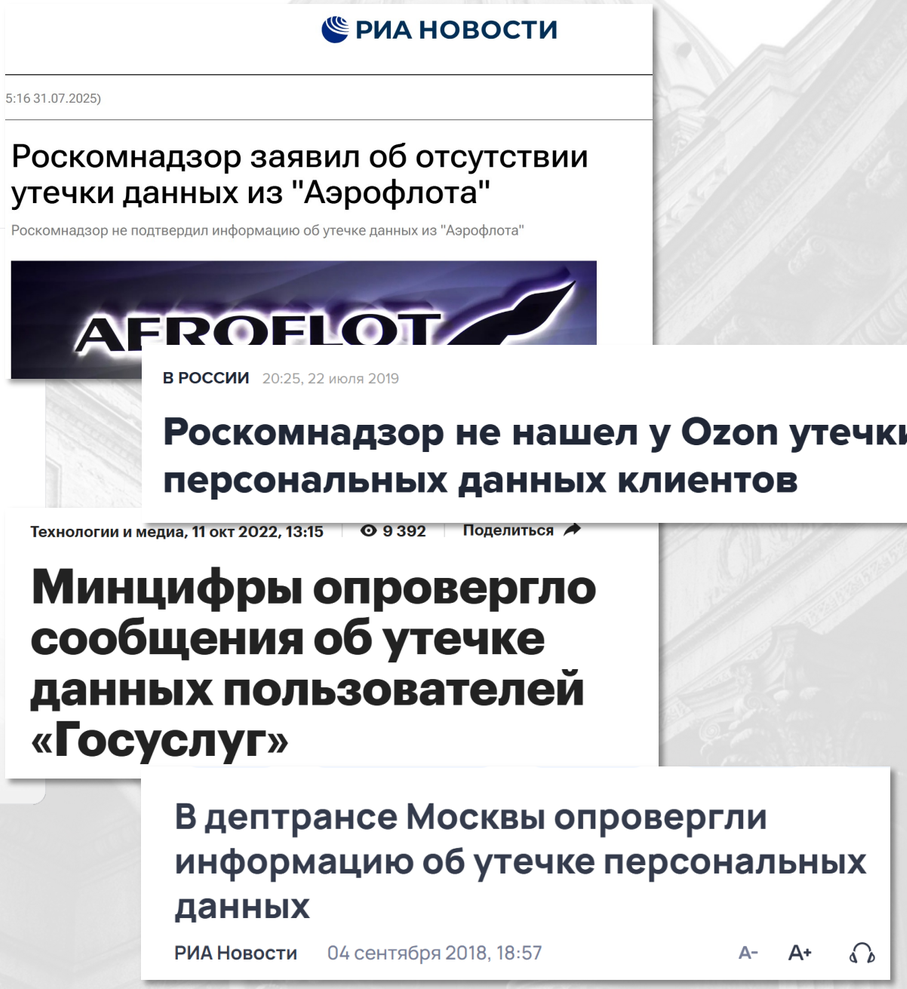
- НСД инсайдера к БД без копирования
- Случайное уничтожение БД инсайдером
- Подозрительная активность пользователя

Нарушены ли права субъекта, если утекли обезличенные и/или зашифрованные ПД?

Уведомить ли РКН?

Да! Если нет, то…

- Штраф до 3 млн ₽
- Внеплановая проверка / расследование
- Отягчающее обстоятельство при назначении штрафа
- Не перенести бремя уведомления на подрядчика



Эти критерии НЕ работают, если не уверены, что утечка ваша, или это практически недоказуемо
(нет уникальных атрибутов данных, уверены, что у «третьей стороны» нет доказательства принадлежности ПД)

Какова реакция РКН?

	ЗАПРОС	ПРОВЕРКА	РАССЛЕДОВАНИЕ
Уведомление	n/a	24 часа	24 часа
Исполнение	10 раб. дней	по договоренности, как правило – 1-2 дня для каждого запроса	3 календарных дня для каждого запроса
Санкция	5 тыс. ₽	5 тыс. ₽ и продление проверки	дисквалификация ФЛ, приостановление деятельности ЮЛ
Срок	n/a	10 раб. дней	30 календарных дней

Какова реакция РКН?

НИЧЕГО… 😇

Не было инцидента вовсе

Утекли данные, но **не** ПД!

Удалили все выявленные публикации скомпрометированных ПД

Утечка может и была, но **другой оператор** этих ПД

ИЛИ

СУРОВ В ПРОТОКОЛЕ

«… Оператором подтвержден **факт** неправомерного доступа … В действиях Оператора усматривается **состав** …»

ИНОГДА ЛОЯЛЕН В СУДЕ

«… просил назначить компании **минимальное** наказание …»

«… не возражала против наказания в **минимальном** размере …»

«Оператором **приняты меры**, закрыт доступ из вне …»

Позиция инспектора РКН в суде имеет критичное значение.

А что суд?

- В АС пока нет практики рассмотрения таких дел
- Установлены смягчающие обстоятельства только для 2-й утечки
- Без штрафа – каждая 8-я компания, как минимум

ИНГОССТРАХ

S7 Airlines

МТС БАНК

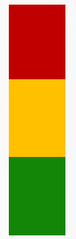
Контроли и ритуалы ДО утечки

	Артефакт	Скоринг
• Регулярный контроль процессов обработки ПД • **Актуализация ЛНА, RoPA, сведений в реестре** • Контроль внедрения новых процессов, ИТ-систем	• Ежегодные планы актуализации ЛНА • Список триггеров актуализации ROPA и сведений в реестре РКН • RACI-матрица с обязанностями по актуализации • Отчеты об устранении отклонений	
• Контроль контрагентов • Внедрение системы защиты ПД • **Минимизация обрабатываемых ПД** • Контроль доступа к данным • Проверка знаний работников	• Одобрение DPO состава собираемых ПД / DPIA • Privacy-playbook по уничтожению ПД • Акты / журналы регулярного уничтожения ПД • Описи дел в архив и акты архивации • Связь данных в КХД и сервисах через синтетический ИД	
• **Минимизация рисков альтернативными методами** • Внедрение рабочих процедур по реагированию на инциденты	• Киберстраховка • Адаптация ДИ и иных документов работников для управления уголовно-правовыми рисками • Договоры с контрагентами включают нормы об эксцессе исполнителя и его последствиях	

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

Comply.

Контроли и ритуалы ПОСЛЕ утечки

	Артефакт	Скоринг
• Остановка утечки		
• 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	
• Создание рабочей группы и оценка инцидента		
• Уведомление регулятора об инциденте		
• Информирование субъектов	• Доказательства добровольной компенсации пострадавшим • Уведомление субъектов ПД (с логами рассылки, шаблонами) • Публичное размещение пресс-релиза (PR-коммюнике) • Усиление первой линии для обработки запросов субъектов (скрипты чат-бота, горячая линия и т.д.) • Журналирование обращений / жалоб субъектов • Утвержденная программа поддержки субъектов	
• Работа с контрагентами (если применимо)		
• 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	
• Устранение уязвимости		

Артем Дмитриев
Управляющий партнер

t.me/comply_ru
comply.ru

Чек-лист 1
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.

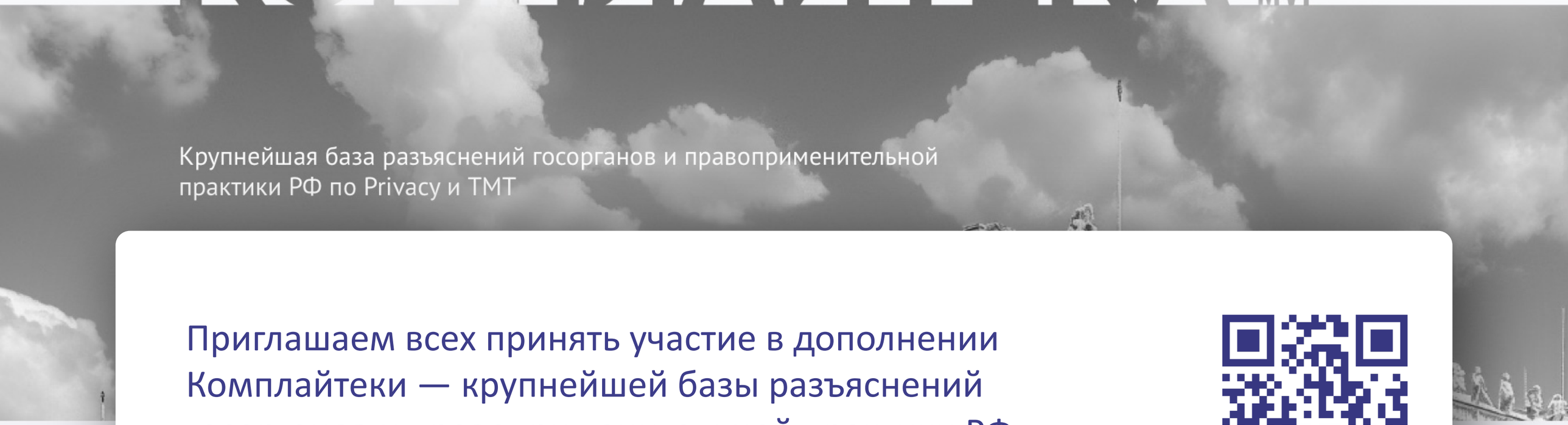
Ниже чек-лист с примерами доказательств первой группы, а здесь – второй.

Контроль	Артефакт и уровень соответствия	Зона ответственности
Регулярный контроль процессов обработки ПД	• План и акты внутренних проверок ПД • 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

Зона ответственности
• DPO
• ИБ
• DPO
• Legal
• DPO
• Legal

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

КОМПЛАЙТЕКА MVP



Крупнейшая база разъяснений госорганов и правоприменительной практики РФ по Privacy и TMT

Приглашаем всех принять участие в дополнении Комплайтеки — крупнейшей базы разъяснений госорганов и правоприменительной практики РФ по Privacy и TMT. Сделайте свою работу комфортнее!

Обширная база данных

Более 150 официальных разъяснений, систематизированных по 10+ правовым категориям. Позиции 7+ руководящих органов, включая РКН, Роструд, ФАС и Минцифры. Скоро – суды

Чаще всего позиции госорганов «пылятся» в архивах или теряются в чатах. Комплайтека создана, чтобы это изменить. Мы сделали первый шаг – внесите и вы свой вклад!