Выжившие в 2026-м: итоги весенних профвизитов РКН

Intro

Мария Пономарева

Старший юрист
Comply

Анастасия Верещагина

Старший юрист
Comply

Agenda

- Карта мероприятий РКН 10’
- Кто под прицелом 10’
- Таймлайн профвизита 10’
- Формат и итоги 15’
- Подготовка 20’
- Q&A 20’

Comply.

Карта мероприятий РКН

Тип мероприятия РКН	Чем регулируется	План мероприятий	Сообщения в СМИ и 3х лиц	Требование прокурора / ПП	Истечение срока устранения	Сведения об угрозе	Утечка ПД	Индикаторы риска
Выездная проверка	Ст. 73 248-ФЗ П. 51-52.1 ПП № 1046	⚠️		✅	⏸️	⏸️	⏸️	⏸️
Документарная проверка	Ст. 72 248-ФЗ П. 46-50 ПП № 1046	⚠️		✅	⏸️	⏸️	⏸️	⏸️
Административное расследование	Ст. 28.7 КоАП						✅	
Обязательный профилактический визит	Ст. 52.1 248-ФЗ П. 30-36 ПП № 1046	✅						
Инспекционный визит	Ст. 70 248-ФЗ П. 43-45.1 ПП № 1046			✅	⏸️	⏸️	⏸️	⏸️
Наблюдение	Ст. 74 248-ФЗ П. 59 ПП № 1046	✅	✅					
Объявление предостережения	Ст. 70 248-ФЗ П. 43-45.1 ПП № 1046					✅		

Карта мероприятий РКН

Тип мероприятия РКН	Чем регулируется	План мероприятий	Сообщения в СМИ и 3х лиц	Требование прокурора / ПП	Истечение срока устранения	Сведения об угрозе	Утечка ПД	Индикаторы риска
Выездная проверка	Ст. 73 248-ФЗ П. 51-52.1 ПП № 1046	⚠		✅	⏸	⏸	⏸	⏸

Группа тяжести

А

- Передача в неадекватные страны
- Спец. категории и биометрия
- Обработка ПД более 100 тыс. субъектов ***new***
- Обработка ПД на основании согласия, если его получение не обусловлено ФЗ ***new***
- Сбор ПД с помощью иностранного ПО и сервисов ***new***
- Передача обезличенных ПД 3-м лицам

Б

- Обработка ПД несовершеннолетних лиц ***new***
- Обработка более 10 тыс. субъектов ***new***
- Сбор ПД с использованием зарубежных БД
- Трансграничная передача на публичных основаниях (ч. 15 ст. 12 152-ФЗ)
- Обезличивание и (или) обработка обезличенных ПД без передачи 3-м лицам ***new***

* В редакции ПП № 1286 от 27.08.2025 (вступило в силу 05.09.2025)

Группа вероятности

Предписание, требование, предупреждение за последние 2 года или наказание (штраф) за 3 года по составам ст. 13.11 КоАП:

- Повторная незаконная обработка ПД (ч. 1.1)
- Повторная обработка ПД без согласия / нарушение требований к согласию (ч. 2.1)
- Повторное невыполнение в срок требования субъекта об уточнении, блокировании или уничтожении ПД (ч. 5.1)
- Нелокализация и повторная нелокализация БД (ч. 8 и 9)
- Утечка и повторная утечка ПД (ч. 12-18)

Карта мероприятий РКН

Тип мероприятия РКН	Чем регулируется	План мероприятий
Выездная проверка	Ст. 73 248-ФЗ П. 51-52.1 ПП № 1046	⚠️
Документарная проверка	Ст. 72 248-ФЗ П. 46-50 ПП № 1046	⚠️
Административное расследование	Ст. 28.7 КоАП	
Обязательный профилактический визит	Ст. 52.1 248-ФЗ П. 30-36 ПП № 1046	✅
Инспекционный визит	Ст. 70 248-ФЗ П. 43-45.1 ПП № 1046	
Наблюдение	Ст. 74 248-ФЗ П. 59 ПП № 1046	✅
Объявление предостережения	Ст. 70 248-ФЗ П. 43-45.1 ПП № 1046	

С **5.09.2025** действует текущий формат профвизитов в ПП № 1046

~ 1760 операторов в плане обязательного профилактического визита на 2026 год.

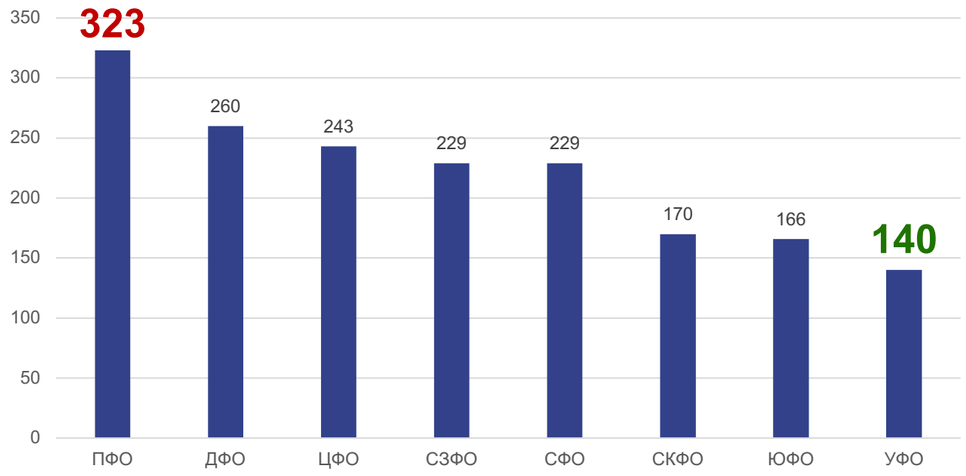
Отказаться нельзя, иначе – основание для проверки (п. 9 ч. 1 ст. 57 248-ФЗ).

Наименование компании	Запланированная дата визита
АО «ОТП Банк»	6 апреля
ООО МФК «Вэббанкир»	6 апреля
ПАО «Банк Уралсиб»	6 апреля
ООО «Деливери клаб»	6 апреля
АО «Райффайзенбанк»	6 апреля
ООО «Ситимед»	18 мая
ООО «Инстамарт Сервис»	18 мая

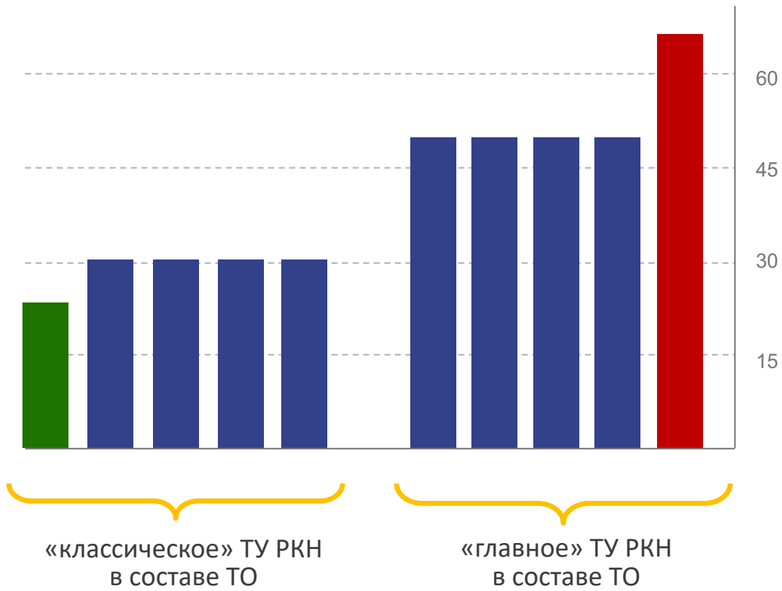
Кто под прицелом

На одно ТУ РКН в составе каждого ТО приходится в среднем 30 профвизитов, кроме «главного» ТУ – на них приходится в среднем 50 профвизитов.

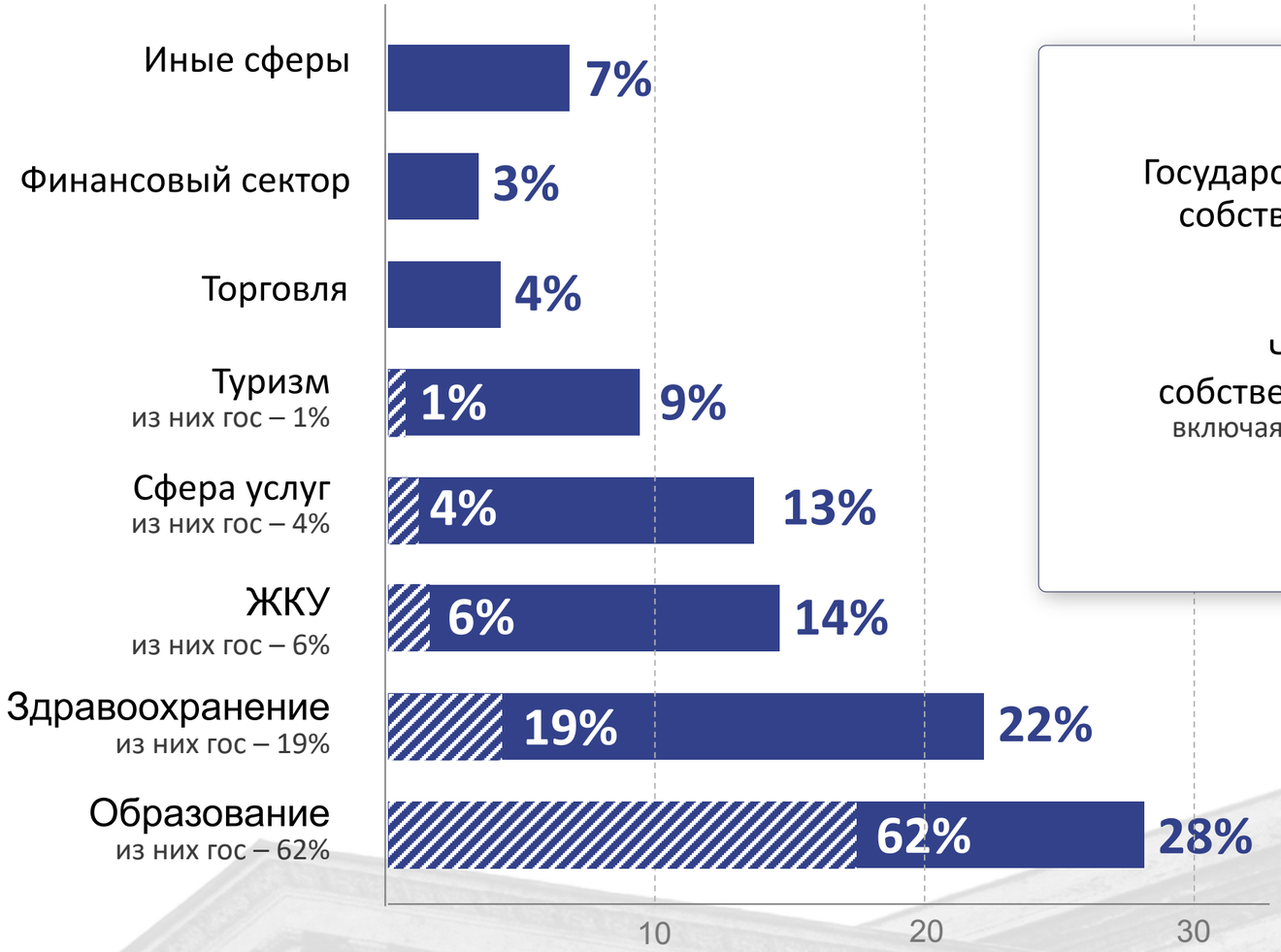
Меньше всего профвизитов приходится на ТУ РКН по Волгоградской обл. и Республике Калмыкия – 26. Максимальное у ТУ РКН по ЦФО – 65.

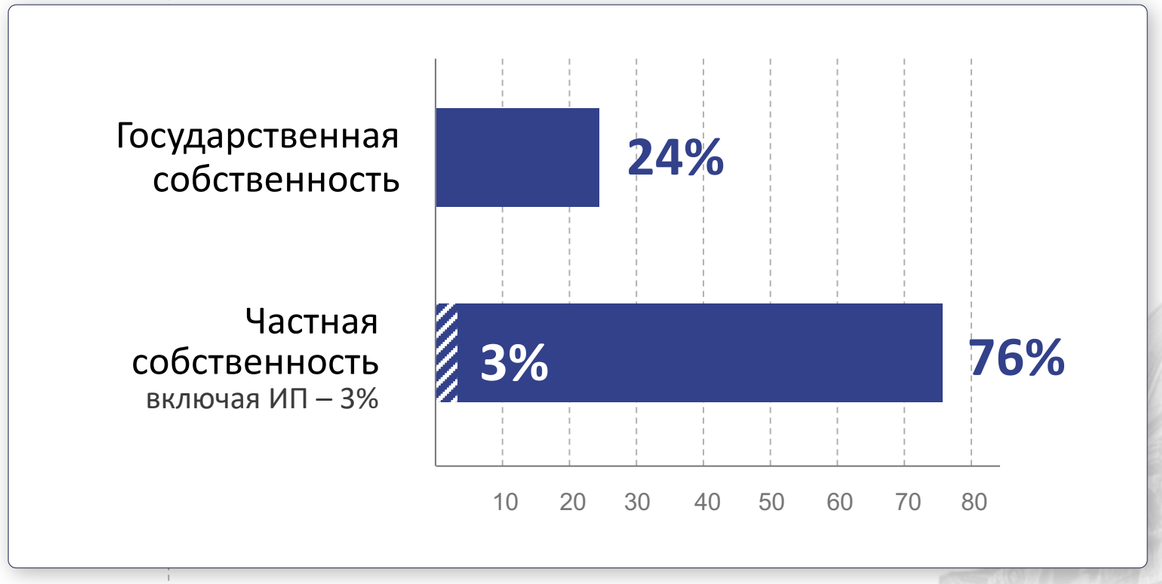


Всего запланировано 1760 профвизитов



Кто под прицелом





Comply.

Что проверяет РКН?

		Плановая проверка	Внеплановая проверка	Обязат-ый проф. визит	Админ. расследов-ие	Наблюдение (мониторинг)
Периметр	Любые требования	✅		✅		✅
	Только инцидент		✅		✅	
Действия РКН	Осмотр	✅	✅	✅	✅	
	Опрос	✅	✅		✅	
	Истребование документов	✅	✅	✅	✅	
	Письменные объяснения	✅	✅		✅	
	Инструментальное обследование	✅	✅			
	Экспертиза	✅	✅		✅	
	Изъятие и иное			✅	✅	✅
Итоги	Протокол	✅	✅		✅	✅
	Предписание	✅	✅	⚠️		
	Проведение иного мероприятия			✅		✅

Таймлайн профвизита

Уведомление о проверке и запрос

~ 24 часа

Ответ на запрос

Дата начала

10 рабочих дней

Акт проф.визита
+ предписание

Отчет РКН
об устранении

До 6 месяцев

Подготовка

- Запрос документов
- Интервью
- Проверка сайт и реестра РКН

Устранение выявленных нарушений до 6 месяцев. Если нет, то риск внеплановой проверки (п. 5 ч. 1 ст. 57, ст. 95 248-ФЗ)

>20

документов запрашивается

>5

справок готовится

Акт / предписание

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

Comply.

Что проверяет РКН?

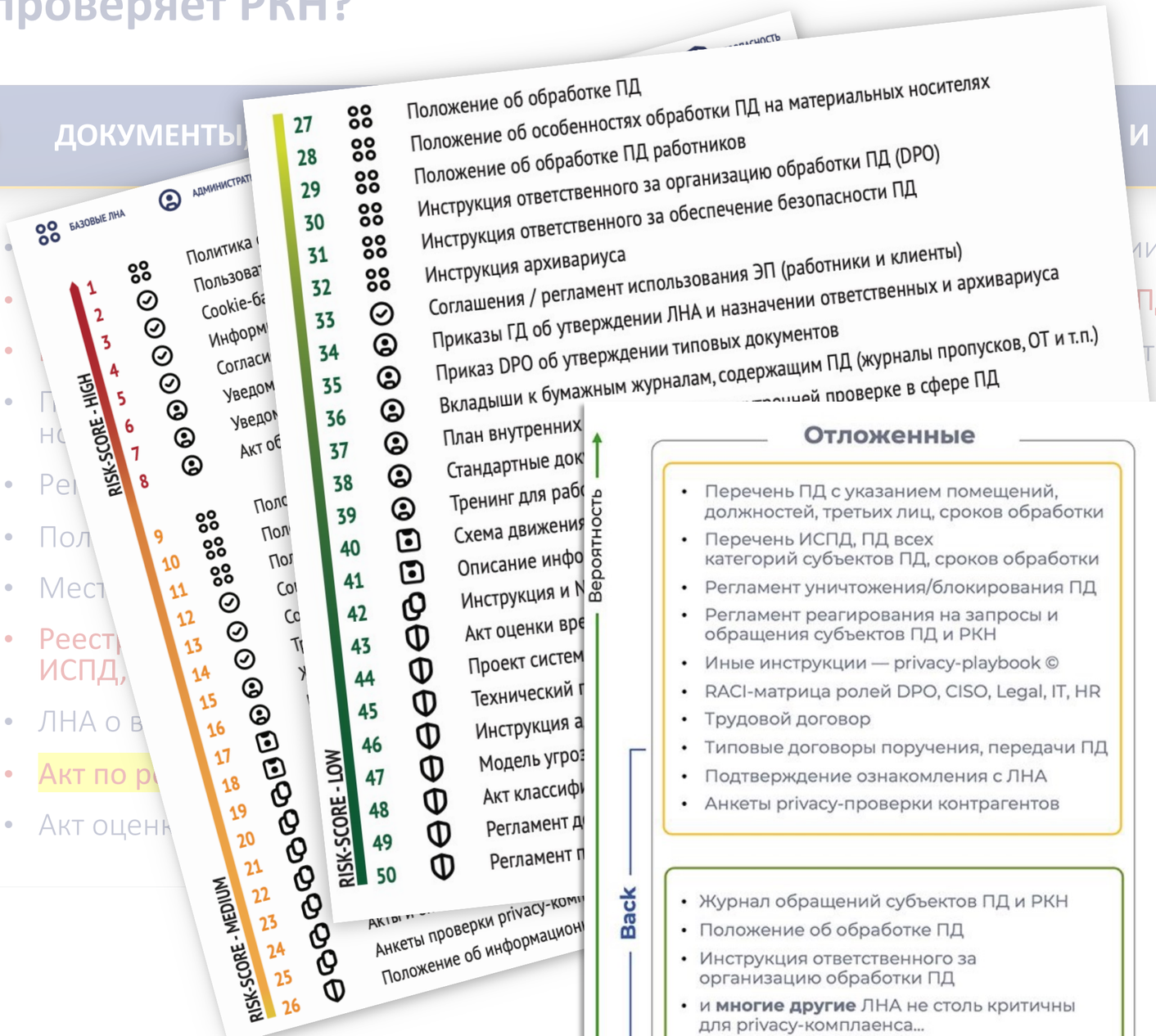
1 ДОКУМЕНТЫ, ПОДТВЕРЖДАЮЩИЕ ПРИНЯТИЕ МЕР, УКАЗАННЫХ В СТ. 18.1 И СТ. 19

- Приказ о назначении DPO
- Политика
- Положение об обработке ПД работников
- Положение об обработке ПД на материальных носителях
- Регламент уничтожения, акты уничтожения
- Положение об архиве
- Места хранения ПД
- Реестры процессов обработки ПД, третьих лиц, ИСПД, перечень мест хранения ПД
- ЛНА о внутреннем контроле (аудите)
- Акт по результатам внутренних проверок (аудита)
- Акт оценки вреда субъектам ПД
- Акт классификации УЗ ИСПД
- Модель угроз ИСПД
- Акт оценки эффективности мер безопасности в ИСПД
- Журнал учета машинных носителей ПД
- Регламент доступа к ПД, перечень лиц, имеющих доступ к ПД
- Политика ИБ
- ЛНА по недопущению и реагированию на инциденты
- Подтверждение ознакомления работников с ЛНА
- Отчеты об обучении работников, обучающие материалы

Что проверяет РКН?

1 ДОКУМЕНТЫ … И СТ. 19

- …ии УЗ ИСПД
- …ПД
- …тивности мер безопасности в
- Реестр … ИСПД,
- ЛНА о в…
- Акт по р…
- Акт оценк…



Вероятность

Отложенные

- Перечень ПД с указанием помещений, должностей, третьих лиц, сроков обработки
- Перечень ИСПД, ПД всех категорий субъектов ПД, сроков обработки
- Регламент уничтожения/блокирования ПД
- Регламент реагирования на запросы и обращения субъектов ПД и РКН
- Иные инструкции — privacy-playbook ©
- RACI-матрица ролей DPO, CISO, Legal, IT, HR
- Трудовой договор
- Типовые договоры поручения, передачи ПД
- Подтверждение ознакомления с ЛНА
- Анкеты privacy-проверки контрагентов

Имидиативные

- Политика обработки ПД, вкл. cookie-файлы
- Пользовательское соглашение / ToU / T&C
- Cookie-баннер
- Информирования об обработке ПД в формах сбора данных на сайте и МП
- Согласие на получение рекламы
- Согласия клиентов на обработку ПД
- Уведомления РКН об обработке ПД, об изменениях,
- Уведомления РКН о трансграничной передаче ПД
- Акт об уничтожении ПД и журнал логов

Back

Front

- Журнал обращений субъектов ПД и РКН
- Положение об обработке ПД
- Инструкция ответственного за организацию обработки ПД
- и **многие другие** ЛНА не столь критичны для privacy-комплаенса…

- Положение о кадровом резерве
- Положение о системе внутреннего контроля, видеонаблюдения, СКУД
- Положение об архиве
- Акты и описи о передаче в архив
- Согласия работников, кандидатов на ПД
- Согласия на распространение ПД

TOP-50
privacy-документов

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

Comply.

Что проверяет РКН?

Чек-лист базовых требований

2 САЙТ ОПЕРАТОРА

1. Политика предусматривает обработку ПД на сайте
2. Наличие Политики на сайте во всех формах сбора / в футере с доступом с любой страницы
3. Соблюдение требований о локализации (хостинг сайта, Google Analytics, reCAPTCHA, Google Forms и т.д.)
4. Обработка cookie-файлов, cookie-баннер
5. Формы сбора ПД, предзаполненные чек-боксы
6. Согласия, пользовательское соглашение
7. Согласие на обработку ПД отдельно от согласия на рекламу
8. Согласие на обработку ПД не зашито в состав других документов
9. Распространение ПД

Что проверяет РКН?

3 РЕЕСТР ОПЕРАТОРОВ РКН

1. Наличие компании в реестре РКН
2. Дата последних изменений и соответствие действующей форме уведомления
3. Актуальность сведений:
    - об операторе
    - о DPO
    - о целях и условиях обработки
    - о защите ПД
    - о трансграничной передаче
    - о местах расположения баз данных

Формат проведения

Дистанционно (в любом случае) ✓ + **Очно** (возможен визит) ?

- Проверка сайта
- Проверка реестра операторов
- Мобильное приложение "Инспектор"
- Электронная почта
  - Интервью
  - Предоставление документов
  - Ответы на запросы
- Проверка наличия документов
  - Фиксация документов на фото/видео
  - Просмотр бумажных документов (в т.ч. журналов)
  - Интервью
- Визуальный осмотр
  - Хранение / таблички / видеонаблюдение

Подготовка к профвизиту: варианты

- Сбор рабочей группы для профвизита
- Проведение краткого обучения для сотрудников по ключевым правилам перед визитом
- + RARE & MEDIUM

Роскошный максимум = вовлечение владельцев процессов

- Апдейт RoPA, в т.ч. перечня ИТ-систем и третьих лиц
- Проверка помещений для оффлайн-визита (чаще всего офис)
- + RARE

Медиана = чек того, что может повлиять на предметы контроля

- Проверка наличия и корректности базовых ЛНА по ст. 18.1 и 19 152-ФЗ
- Проверка ключевых фронт-энд ресурсов и устранение текущих гэпов

Базовый минимум = чек предметов контроля

Подготовка к профвизиту: rare

ЛНА по ст. 18.1 и 19 152-ФЗ

- **Наличие** документов по **перечню**
- **Утверждены документы**, которые относятся к ЛНА
- Документы соответствуют бизнес-процессам, **нет очевидных противоречий**
- DPO хорошо ориентируется в документах, **может дать все необходимые пояснения**

Фронт-энд ресурсы

- Проверка тачпойнтов по **чек-листу**
- **Исправление ДО профвизита** гэпов, которые можно приоритизировать и устранить, в т.ч. в реестре РКН
- Эскалация до ЛПР гэпов, по которым **ранее риски были приняты** (например, GA)
- По оставшимся гэпам сформировать план устранения (1) за срок профвизита или (2) при получении предписания

Проверить privacy-виктимность

- **Локализация и трансгран**
- **Метрики и аналитика**
- **Политика обработки**
- **Основания обработки**
- **Информи-рование, DSR**

USERS

- посетитель
- клиент
- контрагент
- работник
- соискатель

CJM

- пройти опрос
- оставить заявку на звонок
- подписаться на рекламу
- оставить отзыв
- регистрация в ЛК
- запрос на доступ к ПД
- отозвать согласие
- податься на тендер
- публикация бизнес-кейса
- оставить контакты для связи
- заполнить резюме
- активировать чат-бот

Проверить privacy-виктимность

Библиотека уязвимостей (частые примеры)

Локализация и трансгран	Хостинг БД сайта вне РФ (IP-адрес)	Сбор ПД через зарубежные сервисы (опросы, капча)	В Политике нет трансграничной передачи ПД	Неуведомление РКН о трансграничной передаче ПД
Метрики и аналитика	Иностранные метрические сервисы (GA, FB пиксели)	В Политике нет деталей мониторинга	Нет cookie-баннера при первом касании	В cookie-баннере нет согласия или условий
Политика обработки	Нет ссылки на каждой «поверхности», где собираются ПД	Разные объем и условия обработки ПД в Политике vs формах	Нет описания обработки для каждой цели, вкл. сроки	Нет описания порядка уничтожения ПД
Основания обработки	Избыточность ПД для заявленной цели	Нет учета и управления согласиями	Обязательность согласий на обработку ПД и рекламу	Нет согласия на распространение / ограничений
Информи-рование, DSR	Не исполнен запрос на доступ к ПД	Регистрация в реестре неактуальна и не соответствует сайтам	Нарушены сроки / порядок реагирования на запрос субъекта	Галочка есть, но нет текста согласия / информирования

КРИТИЧНОСТЬ

Подготовка к профвизиту: medium

Апдейт RoPA

- **Проведение бриф-аудита** для среза изменений
- **Апдейт реестра процессов**, учет изменений в Политике / реестре
- **Апдейт перечня третьих лиц** оффлайн и онлайн (при наличии)
- Апдейт перечня ИТ-систем, учет изменений в реестре с т.з. БД и ТГП

Осмотр помещений

- Проверить **таблички и документы**, проверить входную группу, вкл. журналы и информирование
- Зачистить помещения, перенести бумагу в запираемые шкафы, лишнее – уничтожить / в архив
- Убрать / зачистить стенды на время профвизита, проинструктировать работников в офисе
- Предупредить охрану БЦ о посещении инспектора

Подготовка к профвизиту: well done

Рабочая группа

- **Формирование рабочей группы** во главе с DPO
- Распределение задач по подготовке **с учетом RACI**
- Составление приоритетов на будущее **для повышения уровня комплаенса**
- **Коммуникация итогов профвизита** работникам

Краткое обучение

- Определение перечня ключевых владельцев бизнес-процессов и систем
- Направление чек-листов для подготовки
- Проведение краткого тренинга по правилам взаимодействия или тренинга по следам профвизита
- Использование профвизита как одного из мотивов повышенного внимания к прайваси в компании

Владельцы процессов и систем

Training kit по проверкам

HR

- Подбор персонала
- Управление персоналом
- Организация командировок
- Кабинет врача в офисе
- ДМС и соц. пакет
- Корпоративные порталы и мессенджеры

IT и ИБ

- Аренда вычислительных мощностей
- Корпоративные справочники
- Корпоративный wi-fi
- Администрирование систем
- Защита информации
- Мониторинг и реагирование на инциденты

Маркетинг

- Сайты и мобильные приложения для клиентов
- Реклама
- Акции и промо-механики
- Лендинги
- Агентства и партнеры

Служба безопасности

- Проверка кандидатов
- Пропускной режим
- Видеонаблюдение
- Проверка благонадежности контрагентов
- Конфликт интересов

Исходы профвизита

Акт о проведении обязательного профвизита

Без предписания и без рекомендаций

- Самостоятельно определяем по итогам подготовки и профвизита «слабые места»
- По горячим следам согласовываем ресурсы и план для устранения гэпов

Без предписания, с устными рекомендациями

- Согласовываем план, срок и ответственных для выполнения рекомендаций
- DPO проверяет внедрение рекомендаций

С предписанием

- Согласовываем план, срок и ответственных для исполнения предписания
- В установленный РКН срок направляем отчет об исполнении

*Чтобы получить акт без предписания, выявленные инспектором нарушения необходимо **полностью устранить** до окончания проф.визита*

Стресс-тест готовности к проверке

Вопросы?

info@comply.ru

t.me/comply_ru