

# Privacy-комплаенс РКН наблюдает

Comply.



# Framework

ФЗ №248, ПП № 1046, ПП №336

Профилактика

Контроль



Без взаимодействия



Выездное обследование

Наблюдение за соблюдением требований

Во взаимодействии

3,2+ тыс. / 22' → 500 тыс. / год

# Что это?

Профилактика

Контроль



Без взаимодействия

Во взаимодействии



Выездное обследование

Наблюдение за соблюдением требований

## Триггер наблюдения

- Нет согласования с прокуратурой
- При жалобах, информации в Интернете и др.
- Без уведомления оператора



## Проверка сайта

- Анализ данных: Интернет и Реестр операторов
- Система мониторинга нарушений на сайтах
- Запрос РКН – 10 (+5) рабочих дней



## Выявлено нарушение

- Требование об устранении, вкл. уничтожение ПД
- Протокол 13.11 КоАП
- Предостережение, рекомендации
- Стена позора



## Устранение нарушения

- Уведомление РКН и субъектов
- Повышение категории риска (план проверок)
- Внеплановые проверки при индикаторе риска

# Боязно ли?

При наблюдении РКН есть протоколы (**NEW**), **НО** нет рисков:

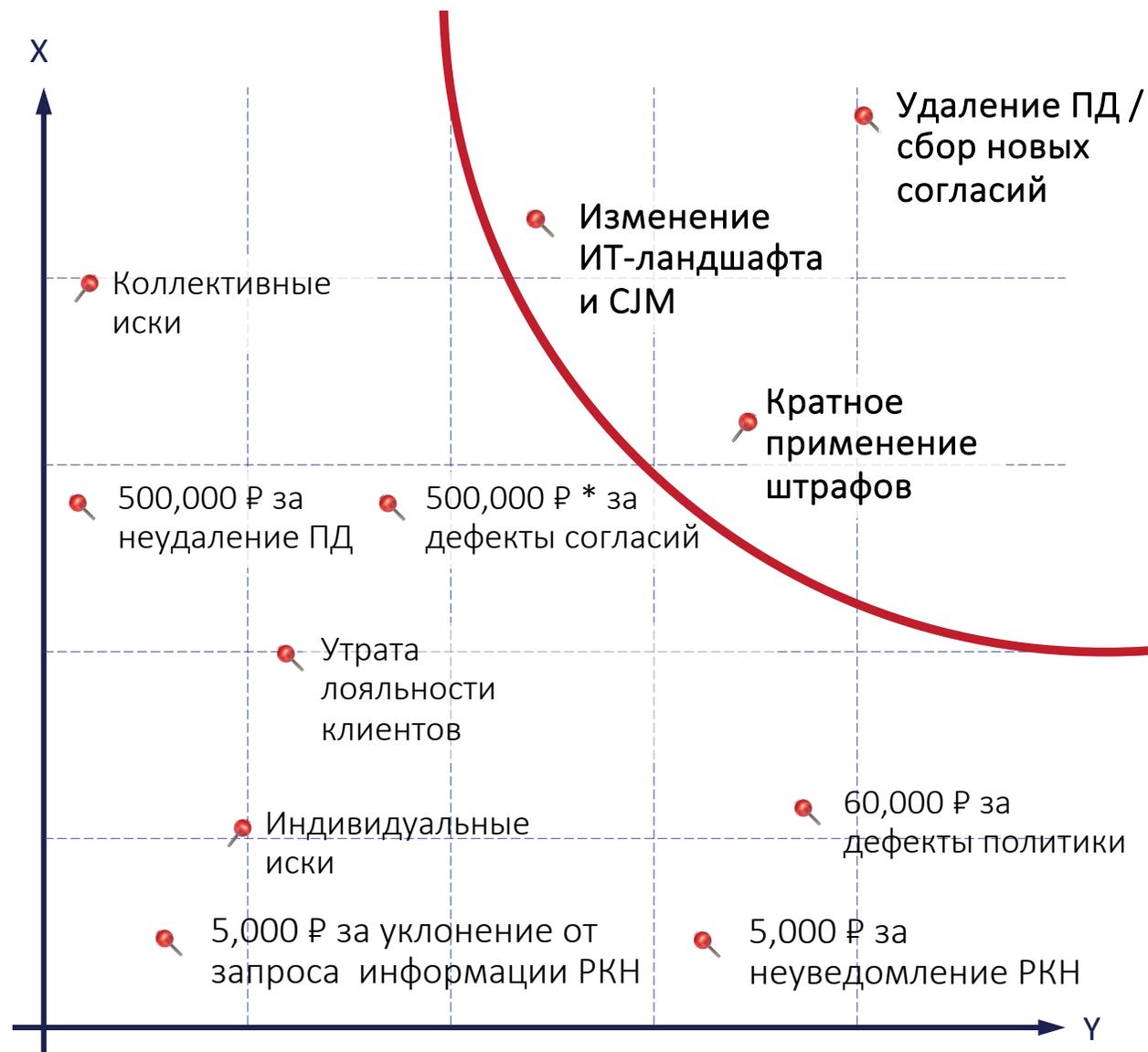
- нелокализации ПД
- предписания
- проверки / визита

X – материальность

Y – вероятность

📍 – риски от РКН / ФАС

📍 – риски от субъектов



\* Применимо, если оператор предоставил РКН доказательства нарушения

# Как проверить виктимность сайта?

Локализация  
и трансгран

Метрики и  
аналитика

Политика  
обработки

Основания  
обработки

Информирование,  
DSR



посетитель  
клиент  
контрагент  
работник  
соискатель

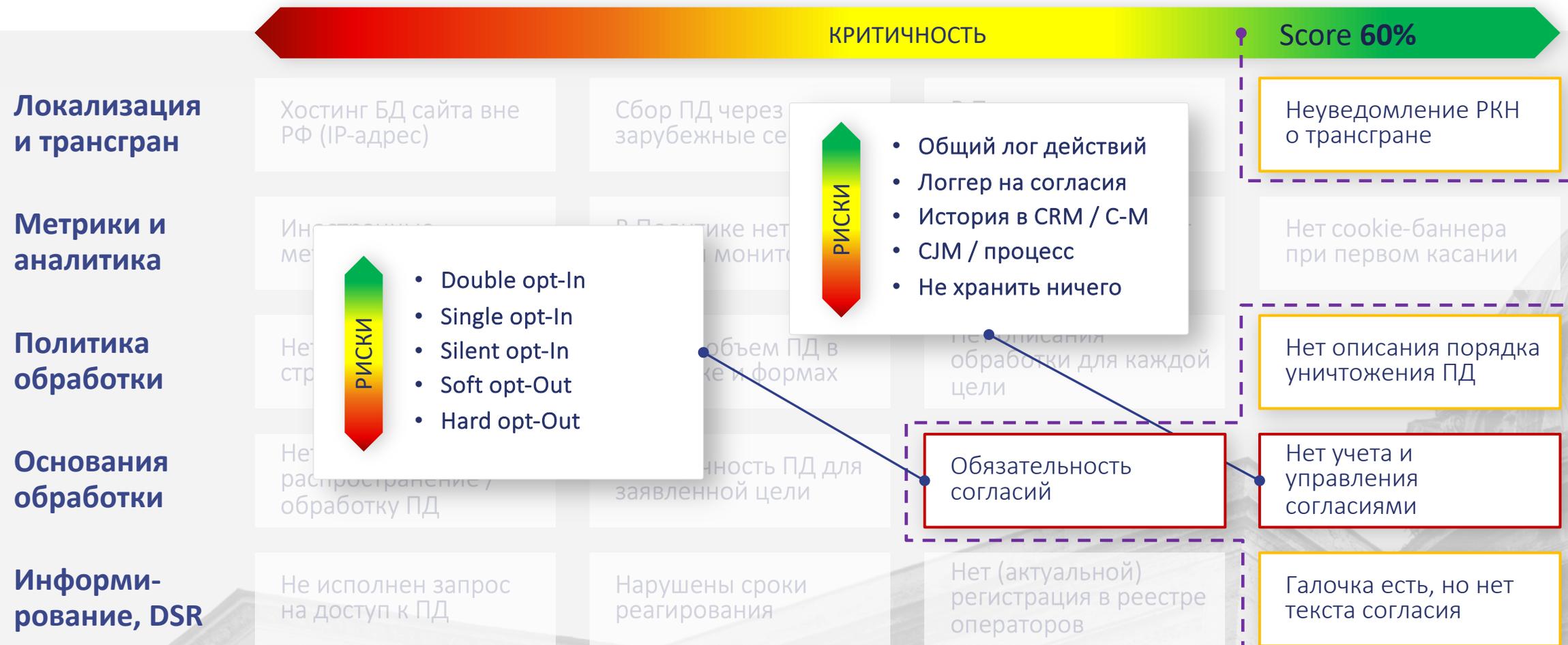


пройти опрос  
оставить заявку на звонок  
подписаться на рекламу  
оставить отзыв  
регистрация в ЛК  
запрос на доступ к ПД  
отозвать согласие  
податься на тендер  
публикация бизнес-кейса  
оставить контакты для связи  
заполнить резюме  
активировать чат-бот

# Библиотека уязвимостей (примеры)

	КРИТИЧНОСТЬ			
<b>Локализация и трансгран</b>	Хостинг БД сайта вне РФ (IP-адрес)	Сбор ПД через зарубежные сервисы	В Политике нет деталей трансгрانا	Неуведомление РКН о трансгране
<b>Метрики и аналитика</b>	Иностранные метрические сервисы	В Политике нет деталей мониторинга	Нет cookie-баннера при первом касании	В cookie-баннере нет согласия
<b>Политика обработки</b>	Нет ссылки на каждой странице сайта	Разный объем ПД в Политике и формах	Нет описания обработки для каждой цели	Нет описания порядка уничтожения ПД
<b>Основания обработки</b>	Нет согласия на распространение / обработку ПД	Избыточность ПД для заявленной цели	Обязательность согласий	Нет учета и управления согласиями
<b>Информирование, DSR</b>	Не исполнен запрос на доступ к ПД	Нарушены сроки реагирования	Нет (актуальной) регистрация в реестре операторов	Галочка есть, но нет текста согласия

# Библиотека уязвимостей (примеры)



# Comply.Privacy: Pentest

- **Методология** проверки сайтов включая весь CJM и DSR-процедуры на основе практики РКН
- **Понимание бизнеса**, маркетинга и принципов работы сайтов, практики РКН
- Отчет с **оценкой** рисков для бизнеса и практические **рекомендации** с учетом рынка
- Совместный с HF Labs продукт для consent-management – **Центр управления согласиями**



**Артём Дмитриев**  
Управляющий партнер, Comply

✉ [artem.dmitriev@comply.ru](mailto:artem.dmitriev@comply.ru)

☎ +7 (961) 806-2776

📌 [t.me/comply\\_ru](https://t.me/comply_ru)

🌐 [comply.ru](https://comply.ru)