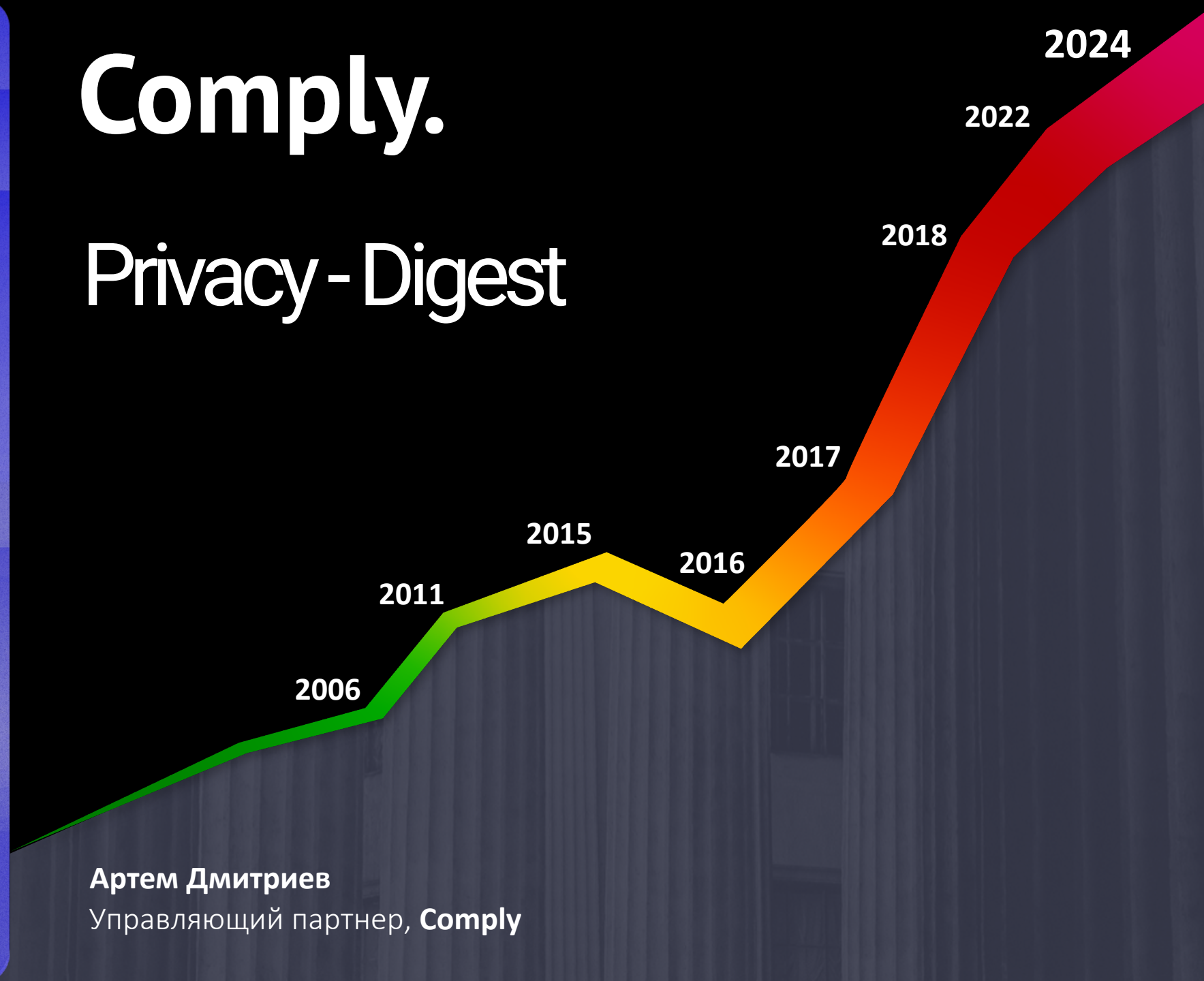
H F Labs

Comply.

Privacy - Digest



CDI CONF 2024

Артем Дмитриев
Управляющий партнер, **Comply**

Более 150 инициатив за 2024

Риск-скоринг РКН
Аутсорсинговые услуги
Front-end и Back-end комплаенс
Правила экстерриториального применения 152-ФЗ
Риски non-compliance
Новые позиции РКН
Сегрегация операторов
Информирование
Управление согласиями работников
Требования по уничтожению
Введение категории «спецоператор обработки ПД»
Best practices
Отмена моратория на проверки по утечкам
Защита от утечек информации
Штормит согласия
Использование биометрии в СКУД
Уведомление ФСБ об инцидентах
Состав специальных категорий ПД
Требования по уничтожению ПД
Внимание к утечкам
Уведомление о трансграничной передаче
Обезличивание и дата-национализация
Госозеро данных
Включение в реестр операторов
Импортозамещение в IT
Интенсификация мониторинга РКН
Цифровой кодекс
Уголовная ответственность
Нацпроект «Экономика данных»
Ужесточение ответственности
Уведомление об утечке
Рост privacy культуры
Компенсации за утечки данных
Законопроект об оборотных штрафах

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

Comply.

Интенсификация мониторинга РКН

3+ тыс./год
мероприятий контроля

Пропускная способность сервиса РКН
500 тыс./год

Проверить privacy-виктимность

	КРИТИЧНОСТЬ			
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
Политика обработки	Нет ссылки на каждой странице сайта, 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
Информирование, 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

Штормит согласия

- Отход от согласий
- Единое окно для управления согласиями на Госуслугах
- Критика мультиоператорских согласий
- Доказывание согласия (логи и идентификация)
- Законопроект о сборе согласий отдельно от других документов

- Замещение «токсичных» согласий
- Инвентаризация и учет согласий
- Логирование

Comply.

Сегрегация операторов

- Спецоператоры будут обрабатывать ПД непривилегированных операторов
- Передать обработку значительного объема ПД, т.е. **более 100 тысяч записей**

- Отслеживать принятие подзаконки
- Оценить критерии для спецоператора:
  - компания в РФ
  - не менее 5 работников с высшим образованием в области ИБ
  - страховка на случай утечки от 100 млн руб.
  - локализация БД в РФ
  - лицензии ФСТЭК и ФСБ на работу с СКЗИ
  - подтвердить ИБ-комплаенс

Национализация

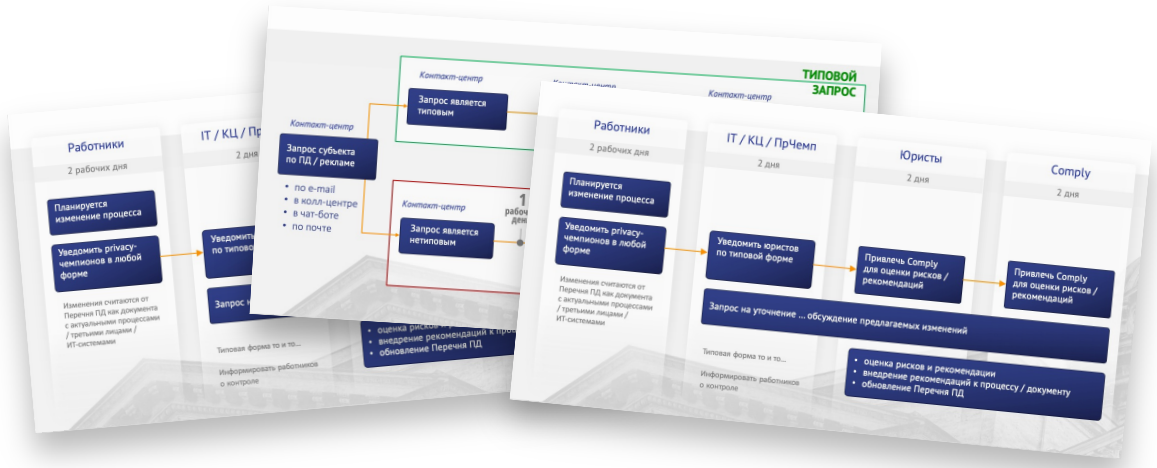
- С 1.9.2025 операторы **обязаны обезличивать и передават**ь ПД в ГИС по требованию Минцифры
- **Методику обезличивания** определит Правительство
- Спустя год после передачи доступ к наборам данных будет открыт для бизнеса

- Проверить, могут ли ваши данные представлять интерес для Минцифры
- Отслеживать принятие подзаконки:
  - о методах обезличивания,
  - порядке передачи,
  - порядке предоставления доступа и т.д.
  - ответственности

Ужесточение ответственности

- Нет согласий на **рекламу** — 1 млн, нет **письменных** согласий — 0,7 млн
- Кратно увеличился размер **компенсации субъектам** за нарушения
- Законопроект об **оборотных штрафах**, из недавнего: компенсации, добровольный аудит и страховка

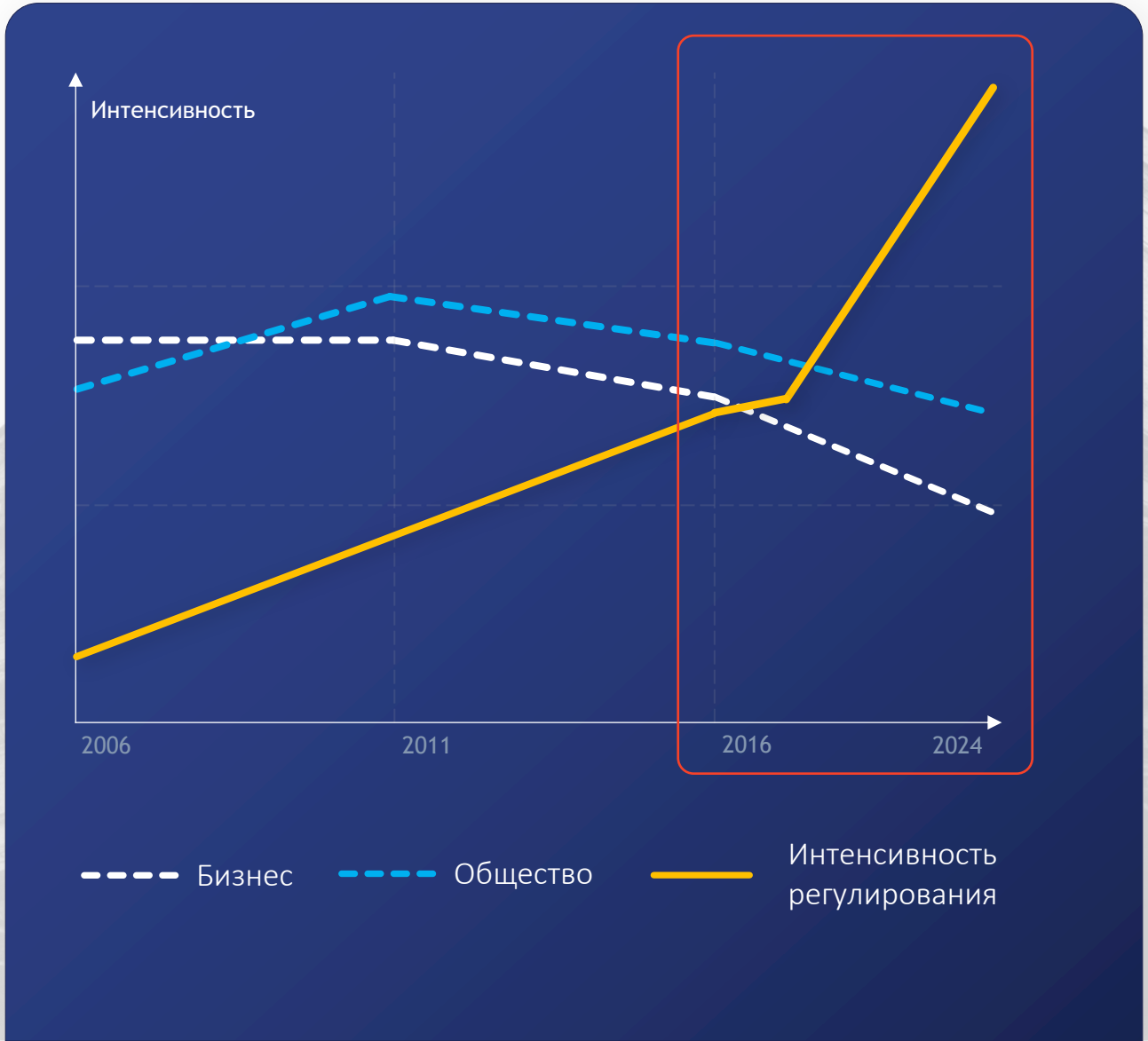
- Наличие доказательств регулярности privacy-процедур
- Privacy-Playbook



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

Comply.

Такое себе регулирование



Данные – **бизнес-актив**, а не комплаенс-нагрузка

Непропорциональность и волатильность **регулирования**

Фин. риски и риск **утраты** данных и возможности работы с ними

Долгосрочная комплаенс-стратегия по работе с данными

H F Labs

Comply.

Артем Дмитриев
Управляющий партнер, Comply

artem.dmitriev@comply.ru
+7 (961) 806-2776
t.me/comply_ru
comply.ru

CDI CONF 2024