HTTP/1.1 **200 OK**

За пределами формального privacy-комплаенса



Артем Дмитриев
Управляющий партнер
comply.ru | t.me/comply_ru



Две характеристики функции и процедур

ЗРЕЛОСТЬ

Устойчиво ли устроена работа функции?

- Роли
- Встроенность в бизнес
- Ресурсы
- Контроль
- Улучшение
- Артефакты

ЭФФЕКТИВНОСТЬ

Достигаем ли **результата** с соразмерными затратами?

- Трудозатраты
- Сроки
- Стандартизация
- Результат
- Автоматизация
- Контекст

Выявляет ли это обычный комплаенс аудит процессов обработки ПД?

НЕТ если это не наш аудит

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

Comply.

Примеры незрелости / неэффективности

Кейс	**Риск** (пример)
Новый процесс	DPO узнаёт после запуска продукта / передачи ПД вендору
Посмотрел и забыл	Нет контроля после запуска процесса / устранения нарушения
Уход DPO	Знания и privacy-процедуры уходят вместе с ним, после – чистый лист
Запрос / инцидент	DPO бегает за владельцами систем и собирает информацию по чатам
Постоянный аврал	Всегда догоняющий и не поспевающий за изменениями бизнеса или зак-ва



Причина кроется не в знании 152-ФЗ и практик РКН, а устройстве процессов

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

Comply.

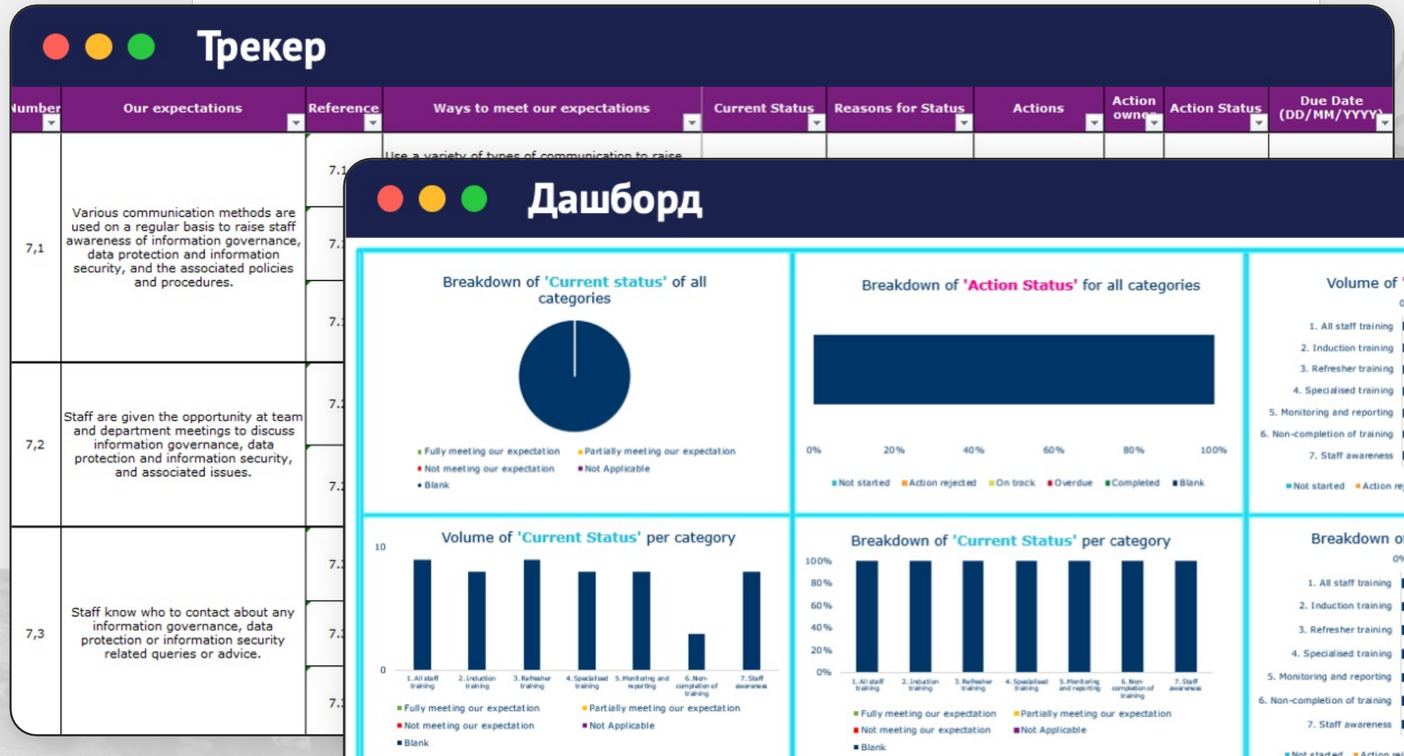
Международные ориентиры

ФРЕЙМВОРКИ

- NIST Privacy
- ISO/IEC 27701

ИНСТРУМЕНТАРИЙ

- ICO Audit Framework



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

Оценка по 5 критериям

Критерий	Примеры того, что проверяем
Формализация	• Типовые документы / образцы • ЛНА по процедуре, SOPs • Артефакты-доказательства
Проникновение	• Playbook’и для бизнеса • Селф-сервисы, чек-листы, опросники • Обучение и awareness
Управление	• RACI / DACI, аллокация ролей • Каналы запросов к DPO • Пути и точки эскалации
Оценка	• Периодические контроли и отчётность • Метрики и управление ими • KPI для бизнес-юнитов
Оптимизация	• Lessons learned • Риск-ориентированный подход • Алгоритмизация / автоматизация

Процедура

Vendor-менеджмент ▼

- ✓ **Vendor-менеджмент**
- Change-менеджмент
- Incident-менеджмент
- Обработка запросов субъектов
- Хранение и уничтожение ПД
- …

Подразделение

Вся компания ▼

- ✓ **Вся компания**
- HR
- Маркетинг
- ИТ
- Бухгалтерия
- Продажи

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

Comply.

Бенчмарк

Критерий	Примеры того, что проверяем	Vendor-менеджмент	Change-менеджмент
Формализация	Типовые документы / образцы	4/4	3/4
	ЛНА по процедуре, SOPs	3/4	3/4
	Артефакты-доказательства	3/4	2/4
Проникновение	Playbook’и для бизнеса	3/4	3/4
	Селф-сервисы, чек-листы, опросники	3/4	3/4
	Обучение и awareness	2/4	2/4
Управление	RACI / DACI, аллокация ролей	3/4	3/4
	Каналы запросов к DPO	2/4	2/4
	Пути и точки эскалации	2/4	2/4
Оценка	Периодические контроли и отчётность	2/4	2/4
	Метрики и управление ими	2/4	1/4
	KPI для бизнес-юнитов	1/4	1/4
Оптимизация	Lessons learned	2/4	2/4
	Риск-ориентированный подход	2/4	1/4
	Алгоритмизация / автоматизация	1/4	1/4
		56%	51%

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

Comply.

Бенчмарк

Критерий	Примеры того, что проверяем	Уровень внедрения
Формализация	• Типовые документы / образцы • ЛНА по процедуре, SOPs • Артефакты-доказательства	73%
Проникновение	• Playbook’и для бизнеса • Селф-сервисы, чек-листы, опросники • Обучение и awareness	63%
Управление	• RACI / DACI, аллокация ролей • Каналы запросов к DPO • Пути и точки эскалации	56%
Оценка	• Периодические контроли и отчётность • Метрики и управление ими • KPI для бизнес-юнитов	40%
Оптимизация	• Lessons learned • Риск-ориентированный подход • Алгоритмизация / автоматизация	36%

~64%

Описать и внедрить

Документы и роли есть: шаблон – разовая задача с видимым результатом

~38%

Проверять и улучшать

Метрики и улучшения редки: это постоянная работа – собирать данные и менять процесс

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

Comply.

Что дальше?

+ фильтр

Найдено: 20 из 20

Критерий	Примеры того, что проверяем	Vendor-менеджмент	Change-менеджмент
Формализация	• Типовые документы / образцы • ЛНА по процедуре, SOPs • Артефакты-доказательства	Обновить шаблон поручения Закрепить хранение артефактов	Утвердить регламент изменений Каталог одобренных сценариев
Проникновение	• Playbook’и для бизнеса • Селф-сервисы, чек-листы, опросники • Обучение и awareness	Создать playbook по вендорам Система напоминаний, алертов	Дополнить playbook по AI Инструменты мотивации
Управление	• RACI / DACI, аллокация ролей • Каналы запросов к DPO • Пути и точки эскалации	Завести в тикетную систему Распределить роли по RACI	Связать запрос с картой процесса Закрепить точки эскалации
Оценка	• Периодические контроли и отчётность • Метрики и управление ими • KPI для бизнес-юнитов	План контроля за процедурой Ввести метрики запросов	Проверка актуальность RoPA Ввести KPI для команд
Оптимизация	• Lessons learned • Риск-ориентированный подход • Алгоритмизация / автоматизация	Разделить вендоров по риску Разбирать lessons learned	Библиотека знаний Автоматизированная проверка

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

Comply.

Что дальше?

+ фильтр | Масштаб: средняя B2B компания × | Риск-аппетит: умеренный × | Цель: меньше рутины × | Найдено: 4 из 20

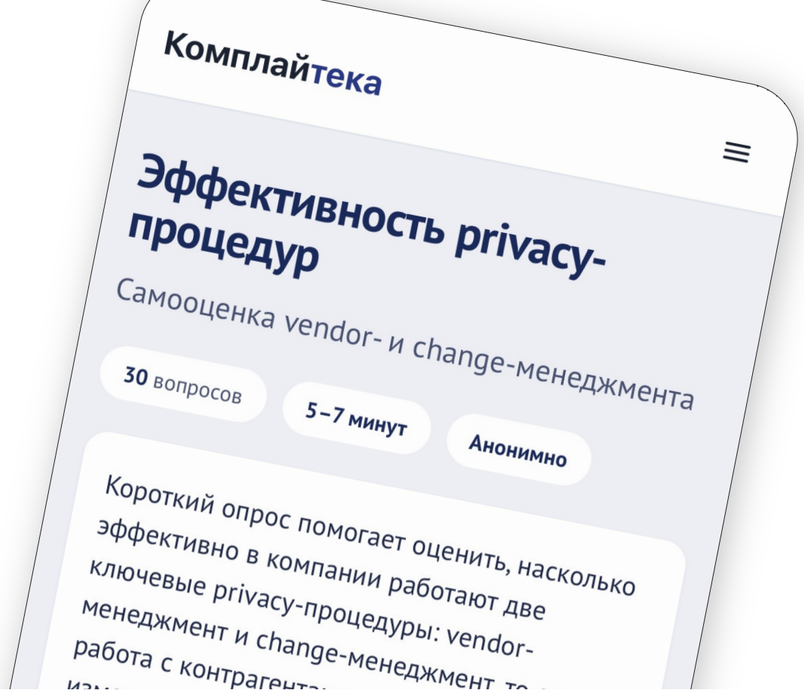
Критерий	Примеры того, что проверяем	Vendor-менеджмент	Change-менеджмент
Формализация	• Типовые документы / образцы • ЛНА по процедуре, SOPs • Артефакты-доказательства	Обновить шаблон поручения Закрепить хранение артефактов	Утвердить регламент изменений **Каталог одобренных сценариев**
Проникновение	• Playbook’и для бизнеса • Селф-сервисы, чек-листы, опросники • Обучение и awareness	Создать playbook по вендорам **Система алертов**	Дополнить playbook по AI Обучать команды изменениям
Управление	• RACI / DACI, аллокация ролей • Каналы запросов к DPO • Пути и точки эскалации	**Завести в тикетную систему** Распределить роли по RACI	**Связать запрос с картой процесса** Закрепить точки эскалации
Оценка	• Периодические контроли и отчётность • Метрики и управление ими • KPI для бизнес-юнитов	Планировать проверки вендоров Ввести метрики запросов	Проверять актуальность RoPA Ввести KPI для команд
Оптимизация	• Lessons learned • Риск-ориентированный подход • Алгоритмизация / автоматизация	Разделить вендоров по риску Разбирать lessons learned	Приоритизировать по риску Автоматизировать уведомления

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

Comply.

Сравни себя

Чек-лист самооценки privacy-процедур



Comply.



Артем Дмитриев
Управляющий партнер

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

