softline
Мы всё сможем

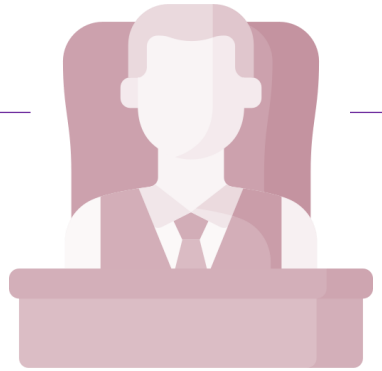
DPO напрокат или как снизить риски штрафов за нарушения порядка обработки персональных данных

Юлия Смолина
Руководитель центра компетенций по консалтингу ИБ

Ключевые лица

Трансформация.
Успешная. Цифровая. Защищенная.

ДИТ

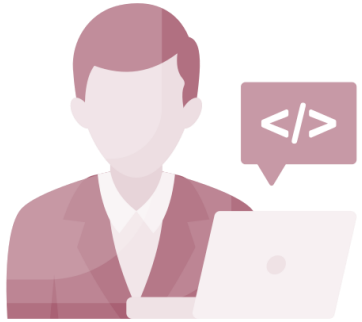


Директор

ДИБ

Юридический департамент

Отдел кадров

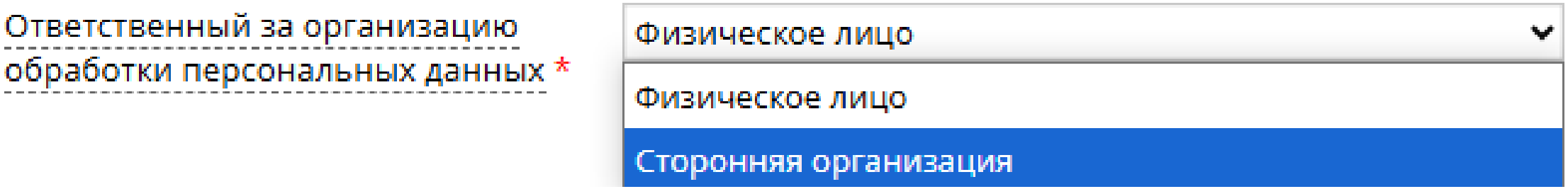


Инженер по ИБ

DPO

DPO – кто это и зачем?

DPO (Data Protection Officer) – эксперт, ответственный за организацию обработки персональных данных (ст. 22.1 152-ФЗ)



Компетенции DPO*

Теоретические основы

- знание законодательства в области приватности России и других стран

Профессиональные практические навыки (hard skils)

- применение знаний в сфере приватности, ИБ и ИТ на практике
- навыки выстраивания системы контроля приватности с учетом требований законодательства и внутренних процессов компании

Межпрофессиональное общение (soft skills)

- навыки общения с руководством компании и с другими подразделениями
- донесение рисков приватности менеджменту компании, учет бизнес-интересов компании
- внедрение защиты персональных данных через работу с сотрудниками
- обучение работников компании базовым навыкам в области обработки и защиты данных

ИИ-Расширение: Регулирование и комплаенс ИИ-систем

- понимание в части автоматизации на базе ИИ-систем
- представление о регулировании ИИ-систем
- понимание рисков в ИИ-системах

*по данным Общественного учреждения «Сообщество профессионалов в области приватности» (RPPA)

vDPO – кому актуально?

vDPO (Virtual Data Protection Officer) –
внешний специалист или компания, выполняющие функции ответственного за обработку персональных данных

Ответственного за обработку ПДн нет, функции распределены между юристами и ИТ, или не реализованы

Критичный бизнес-процесс завязан на обработку клиентских ПДн

Комплект документов разработан, но процессы не работают, что создает риск санкций со стороны регуляторов

Большое количество процессов обработки ПДн и передачи третьим лицам

Необходимо быть готовым к успешному прохождению проверок регуляторов

DPO-as-a-service или virtual DPO

Трансформация.
Успешная. Цифровая. Защищенная.

Внедрение процессов

- Разработка комплекта документов
- Назначение ответственных лиц
- Получение свидетельств

Обучение работников

- Адаптация обучающих материалов под контекст компании
- Проведение онлайн-обучения
- Инструктаж новых работников 1 раз в месяц
- Контроль знаний через полгода
- Повторное обучение

Мониторинг

- Проведение внутреннего аудита выполнения требований по защите ПДн
- Контроль выполнения политик и регламентов
- Реагирование на инциденты

Ответы на запросы

- Подготовка ответов на запросы субъектов ПДн/регуляторов/партнеров
- Регистрация запросов
- Организация уничтожения/изменения ПДн

Консультирование

- Регулярные онлайн-встречи для обсуждения всех текущих вопросов по теме обработки и защиты ПДн

Реагирование на изменения законодательства

- Подготовка новостных отчетов по теме обработки ПДн
- Оперативное планирование действий по доработке ОРД и корректировке процессов
- Актуализация ОРД

Мы всё сможем

softline

Преимущества

1. Постоянная поддержка:

- закрепление за каждым Заказчиком выделенного эксперта (+группа поддержки) – знание и опыт без необходимости обучения и адаптации сотрудника
- снятие со специалистов Заказчика рутинных операций

2. Снижение репутационных и финансовых рисков, связанных с нарушением требований законодательства

- готовность к проверкам и запросам регуляторов
- разделение ответственности
- подготовка артефактов для снижения оборотных штрафов

3. Опционально

- обоснование бюджета на средства защиты для Бизнеса через оценку рисков
- внесение данных в платформу автоматизации Securitm/Docshell/Кит Журнал для упрощения поддержки процессов и документации в актуальном состоянии
- правовая помощь в случае выявления нарушений законодательства о ПДн и компьютерных инцидентов

Кейс 1

Трансформация.
Успешная. Цифровая. Защищенная.

Портрет

1. 100 000+ субъектов ПДн
2. 1000+ ПК, 50+ серверов
3. Выручка компании за 2024 год – 1 млрд. руб.

Исходные данные

1. Компания разрабатывала документы по защите ПДн в 2020 году, актуализация отсутствовала.
2. Функции DPO распределены между юристами и ИТ-специалистами.
3. Защита ПДн не является приоритетной задачей.

Затраты на ИБ

1. 60 млн за 3 года

Смягчающие обстоятельства

1. Не применимы, т.к.:
   - несмотря на то, что ежегодные расходы на ИБ за 3 года составляют более 0,1 % от годового совокупного размера суммы выручки: 1 млрд * 0,1 %= 1 млн
   - не собраны документальные свидетельства выполнения требований

Последствия

1. Штраф за утечку – 15 млн
2. Оборотный штраф за повторную утечку – 30 млн (3%)
3. Штраф за несвоевременное уведомление РКН об утечки ПДн – 3 млн

Итоговая сумма: 48 млн + дополнительные репутационные потери и потери из-за простоя бизнеса

Кейс 2

Портрет

1. 100 000+ субъектов ПДн
2. 1000+ ПК, 50+ серверов
3. Выручка компании за 2024 год – 1 млрд. руб.

Исходные данные

1. В компании существует выделенный DPO.
2. Документы по защите ПДн поддерживаются в актуальном состоянии.
3. Есть заключение лицензиата ФСТЭК о выполнении мер по защите ПДн

Затраты на ИБ

1. 60 млн за 3 года

Смягчающие обстоятельства

1. Применимы, т.к.:
   - ежегодные расходы на ИБ за 3 года составляют более 0,1 % от годового совокупного размера суммы выручки: 1 млрд * 0,1 %= 1 млн
   - собраны документальные свидетельства выполнения требований
   - отягчающие обстоятельства отсутствуют

Последствия

1. Штраф за утечку – 10 млн
2. Оборотный штраф за повторную утечку с учетом смягчающих обстоятельств – 15 млн

Итоговая сумма: 25 млн + дополнительные репутационные потери и потери из-за простоя бизнеса

Что выгоднее?

Собственный DPO

180K*12=2,16M – оклад (gross)

180K – годовая премия

180K*0,3*12=648K – страховые взносы

Итого: 3M

DPO-as-a-service

от 1,8M с НДС в год

300K – возмещение НДС

Итого: 1,5M

Юлия Смолина

Руководитель центра компетенций по консалтингу ИБ

M +7 961 227 40 27

y.smolina@softline.com