

Споры о персональных данных: тайна, покрытая правом

Как выстроить работу с подрядчиками по обработке персональных данных

Ирина Шоткевич,

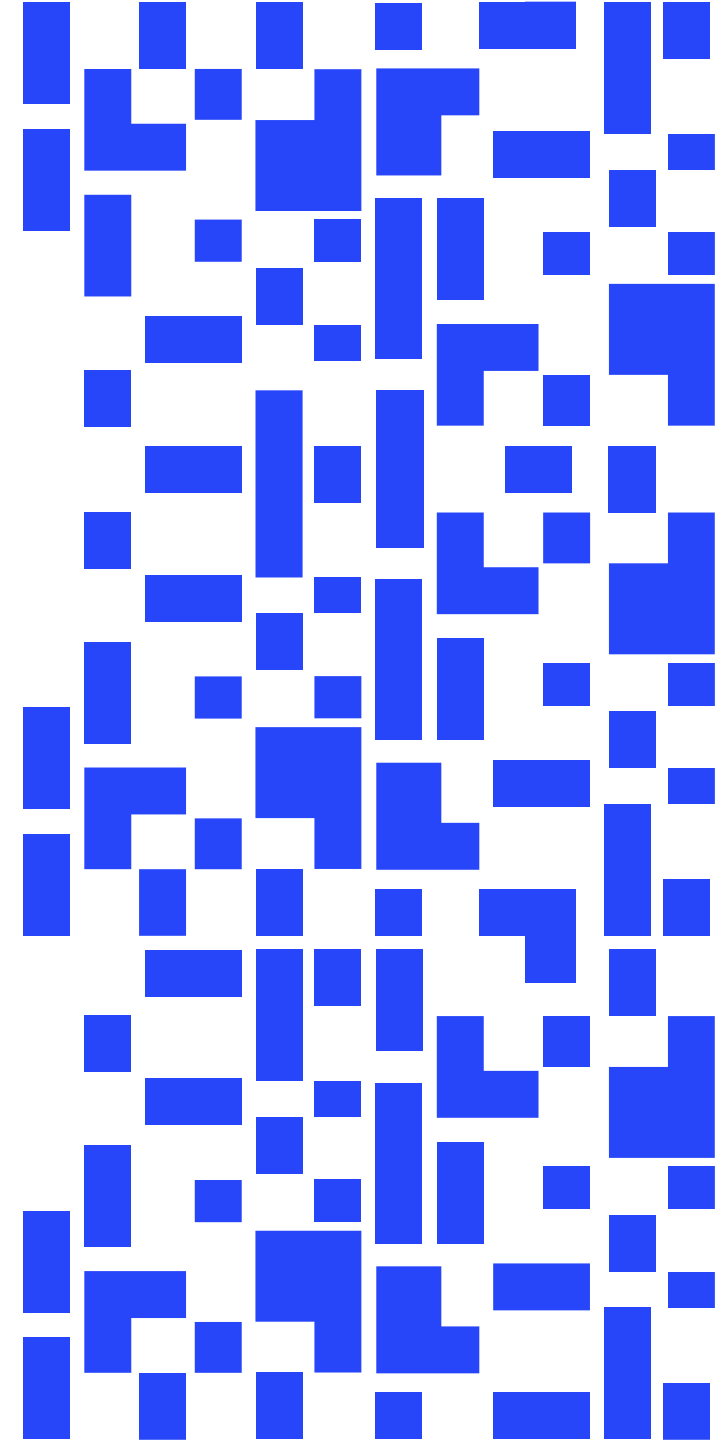
руководитель правовой поддержки направления информационных технологий и защиты персональных данных, ЮниРусь

Irina.Shotkevich@unirusgroup.ru

Ваш подрядчик – Ваша ответственность

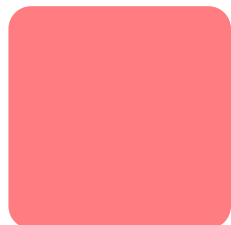
Почему это так актуально именно сейчас?

- Привлечение подрядчиков к обработке персональных данных – это обычная практика для бизнеса
- Оператор остается ответственным за переданные персональные данные
- Ответственность ужесточается
- Подрядчики стали внимательнее и не всегда готовы идти на уступки



**Цель – не переложить риск,
а управлять им**

1. Определите категорию риска контрагента



- > 10 000 записей о субъектах ПДн
- доступ к чувствительным данным (специальные категории, ПДн несовершеннолетних, уязвимых категорий граждан, биометрические ПДн)



- 1000 - 10 000 записей о субъектах ПДн
- обработка «обычных» персональных данных



- < 1 000 записей о субъектах ПДн
- обработка контактной информации в рамках делового взаимодействия
- доступ к обезличенным данным

2. Проверьте контрагентов средней и/или высокой категории риска

ОПРОСНИК

- Кто будет иметь доступ к персональным данным
- Где размещены дата-центры
- Какие применяются меры защиты персональных данных
- Есть ли субподрядчики
- Есть ли трансграничная передача персональных данных
- Собираете ли согласия от субъектов (если применимо)
- Как организовано уничтожение

- Используйте опросник с вопросами, которые имеют значение для вашего бизнеса или ситуации
- Для разных ситуаций подойдут разные опросники
например, отдельный опросник для иностранных контрагентов для оценки допустимости трансграничной передачи ПДн или отдельный опросник для контрагентов, предоставляющих функционал по обезличиванию ПДн
- Сохраняйте заполненные опросники как доказательство вашей добросовестности при выборе контрагента

2. Проверьте контрагентов средней и/или высокой категории риска

Что еще проверить
или запросить?



- Наличие в реестре операторов персональных данных – на сайте Роскомнадзора или в доступной системе по проверке контрагентов
- Наличие Политики в отношении обработки персональных данных
- Назначение ответственного за организацию обработки (копия приказа, контакты)
- Наличие внутренних регламентов, например, по реагированию на инциденты
- Модель угроз
- Отчет по результатам аудита (если проводился)
- Лицензии ФСТЭК /ФСБ (если применимо)
- Репутация: наличие информации о нарушения законодательства о ПДн или утечках ПДн со стороны подрядчика

Заключение договора



Договор в части ПДн – это не формальность, а ваша «страховка»

Что предусмотреть:

- Роли сторон: самостоятельные Операторы или Оператор и Обработчик по поручению
- Если поручение: все условия в соответствии с ч. 3 ст. 6 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных»
- Перечень технических и организационных мер защиты персональных данных
- Порядок привлечения субподрядчиков
- Право на проведение аудита или иной проверки подрядчика (желательно на регулярной основе)
- Порядок уведомления об инцидентах с ПДн (в случае утечки – не позднее 12 ч. с момента обнаружения)
- Распределение ответственности между сторонами
- Порядок возмещения убытков
- Порядок возврата и уничтожения ПДн при завершении работы



- ❑ Разработайте стандартный договор или дополнительное соглашение с условиями об обработке ПДн
- ❑ Подпишите его со всеми подрядчиками, которые относятся к категориям среднего и высокого риска

С чего начать?

План по выстраиванию отношений с подрядчиком по обработке ПДн

1. **Составьте реестр текущих подрядчиков,**
у которых есть доступ к персональным данным
2. **Приоритизируйте:** разделите подрядчиков по уровню риска
3. **Запустите процесс по заключению доп. соглашений**
с ключевыми / самыми рискованными подрядчиками
4. **Внедрите процедуру проверки**
для новых контрагентов

