

Персональные данные: Общий чек-лист для самопроверки

Ставьте галочки ниже, чтобы проверить, насколько Ваши процессы соответствуют законодательству о персональных данных.

О чек-листе

Этот чек-лист не заменяет полноценный аудит, а служит лишь вспомогательным инструментом. Чек-лист содержит набор основных требований, чаще всего применимых к операторам персональных данных, но не является исчерпывающим.

Часть требований не следует напрямую из закона, но сформирована правоприменительной практикой. В зависимости от деятельности Вашей компании к ней могут не применяться отдельные требования или, наоборот, применяться дополнительные требования.

Документы

Во внутренних документах (политике / иных локальных актах) компании описаны:

- Цели обработки ПДн
- Для каждой цели обработки ПДн:
 - категории и перечень обрабатываемых ПДн
 - категории субъектов ПДн
 - способы обработки
 - сроки обработки и хранения
 - порядок уничтожения
- Порядок обработки запросов субъектов ПДн и Роскомнадзора
- Система реагирования при утечках ПДн
- Порядок проведения внутренних аудитов обработки ПДн
- Порядок оценки вреда субъектам ПДн
- Правила обработки ПДн без использования средств автоматизации
- Категории ПДн, обрабатываемых без использования средств автоматизации
- Для каждой категории ПДн, обрабатываемых без использования средств автоматизации:
 - места хранения материальных носителей с ПДн
 - перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ

Взаимодействие с регулятором

- Уведомление об обработке ПДн подано в Роскомнадзор (если не применяются исключения)

Периодически проверяйте актуальность сведений, указанных в уведомлении. При изменении таких сведений уведомите Роскомнадзор

Процессы обработки ПДн

Для каждого процесса:

- Объем собираемых ПДн минимизирован до действительно необходимого

Не собирайте излишние данные «про запас»
- Для первичной записи и обработки собираемых ПДн граждан РФ используются базы данных в РФ
- Есть правовые основания на обработку ПДн, например, согласия
- В одной информационной системе (ИСПДн) не обрабатываются ПДн с несовместимыми целями обработки
- Доступ к ИСПДн предоставлен только лицам, которым он необходим
- Срок хранения ПДн ограничен в пределах разрешенного по закону
- При обработке ПДн на материальных носителях (в бумажных документах) учтены дополнительные условия:
 - для различных категорий ПДн используются отдельные материальные носители
 - если цели обработки ПДн несовместимы, данные не фиксируются на одном материальном носителе
 - обеспечено раздельное хранение ПДн, обрабатываемых в различных целях

Если Вы планируете вводить новый или изменять текущий бизнес-процесс, Вам может пригодиться наш отдельный [чек-лист для бизнес-процесса](#)



Организация персонала (провайдеров услуг)

- Назначено лицо, ответственное за организацию обработки ПДн
- Работники ознакомлены с правилами обработки ПДн
- Создана система обработки запросов субъектов ПДн (например, назначены ответственные лица, установлены сроки реагирования)
- Создана система реагирования на утечки ПДн, включая взаимодействие с Роскомнадзором (например, назначены ответственные лица, установлены сроки реагирования)
- Лица, обрабатывающие ПДн без использования средств автоматизации, уведомлены о факте такой обработки ими ПДн, категориях обрабатываемых ПДн и особенностях, и правилах обработки
- Регулярно проводятся тренинги (обучение) персонала по вопросам обработки и защиты ПДн

Рекомендуем сохранять основные материалы тренингов

Передача третьим лицам

- Есть договоры с третьими лицами, которым компания передает ПДн
- Если компания передает ПДн в рамках поручения, договор с получателем ПДн содержит условия, необходимые по закону

Трансграничная передача ПДн

- До передачи ПДн иностранным получателям проведена их оценка
- Подано уведомление в Роскомнадзор о планируемой передаче ПДн за границу
- Со стороны Роскомнадзора отсутствуют ограничения и запреты на передачу ПДн за границу
- При наличии ограничений / запретов на передачу ПДн за границу иностранный получатель ПДн уничтожил переданные ПДн

Внутренний контроль и аудит

- Компания регулярно, не реже чем раз в год, проводит внутренние аудиты обработки ПДн
- Компания документирует результаты внутренних аудитов
- Компания периодически проводит и документирует оценку вреда, который может быть причинен субъектам ПДн

Сайты и приложения

- Опубликована политика обработки ПДн
- Соблюдены требования к распространению ПДн (если применимо)
- Есть cookies-баннер
- Для каждой формы сбора ПДн есть согласие или иное правовое основание

Ознакомьтесь с нашим [подробным чек-листом](#) для проверки соответствия сайта / приложения требованиям к обработке ПДн



Информационная безопасность

- Определены угрозы безопасности персональных данных при их обработке в ИСПДн
- Установлен уровень защищенности персональных данных при их обработке в ИСПДн
- Реализованы меры по обеспечению безопасности ПДн, в том числе, в зависимости от установленного уровня их защищенности
- Обеспечена безопасность материальных носителей ПДн (хранение в запирающихся комнатах, локерах, предоставление доступа ограниченному кругу лиц и т.д.)

Проверим обработку персональных данных на соответствие законам РФ и подготовим документы

Александр Монин
партнер

Alexander.Monin@mv.legal

Валерия Эйстрах
старший юрист

Valeriya.Eystrakh@mv.legal

Екатерина Сорокина
старший юрист

Ekaterina.Sorokina@mv.legal