Yandex Cloud × kept

Чеклист для клиентов Yandex Cloud по защите персональных данных

Yandex Cloud обрабатывает **персональные данные (ПДн)** в интересах клиента (компании) в случае использования клиентом облачной платформы.

В рамках российского законодательства Yandex Cloud — это оператор, который осуществляет обработку ПДн по поручению другой компании-оператора (для разделения ролей и ответственности мы будем называть Yandex Cloud «обработчиком»).

Yandex Cloud обладает Аттестатом соответствия, подтверждающим обеспечение первого уровня защищённости персональных данных, обрабатываемых с использованием облачной платформы.

Оператор, равно как и обработчик ПДн, **обязаны выполнять** определённые организационные и технические меры, направленные на защиту обрабатываемых данных.

Мы подготовили **чек-лист** для самопроверки выполнения требований российского законодательства в сфере обработки и защиты ПДн для наших клиентов.

Чек-лист для самопроверки

№	Требование	Что надо сделать?
	1. Инвентаризация процессов обработки ПДн	
1.1	п. 2 ч. 1 ст. 18.1 152-ФЗ	Собрать, описать и задокументировать информацию обо всех процессах обработки ПДн в компании в перечне (реестре) процессов обработки ПДн

1.2	п. 2 ч. 1 ст. 18.1 152-ФЗ	Поддерживать в актуальном состоянии информацию в перечне (реестре) процессов обработки ПДн в компании при появлении новых процессов и (или) изменении существующих процессов. **Перечень поможет:** • встроиться в процессы компании, связанные с запуском новых продуктов, новых информационных систем, согласованием договоров, которые предполагают передачу/получение ПДн; • довести до работников информацию о тех случаях, когда им необходимо ставить в известность ответственного за организацию обработки ПДн; • реализовать периодический пересмотр информации в перечне (реестре) процессов обработки ПДн
1.3	ч. 1 ст. 22 152-ФЗ	Проверить Реестр операторов, осуществляющих обработку ПДн, на наличие информации об обработке ПДн и при необходимости обновить её или подать уведомление

✅ 2. Документация

2.1	п. 2 и 3 ч. 1 ст. 18.1 152-ФЗ	Проверить имеющуюся документацию в области обработки и защиты ПДн. При проверке нужно установить, отражены ли в документации: • все категории и перечень обрабатываемых ПДн; • правовые основания обработки ПДн; • все категории субъектов ПДн; • способы и сроки обработки ПДн; • порядок и правила обработки и защиты различных категорий ПДн; • процедуры, направленные на предотвращение, выявление нарушений в сфере защиты ПДн; • отсутствие условий, ограничивающих права субъекта ПДн; • отсутствие положений, возлагающих на оператора дополнительные обязанности и полномочия, не регламентированные 1152-ФЗ. Доработать/разработать (при необходимости) отсутствующую документацию в области обработки и защиты ПДн. Проверить наличие или отсутствие нужной документации можно по нашему перечню документации в области приватности (см. перечень после данного чек-листа)
2.2	п. 1 ч. 1 ст.18. 1 152-ФЗ	Назначить приказом лицо, ответственное за организацию обработки ПДн
2.3	ч. 2 ст. 18.1 152-ФЗ	Опубликовать или иным образом обеспечить неограниченный доступ к Политике обработки ПДн
2.4	ч. 10 ст. 10.1 152-ФЗ	Опубликовать информацию об условиях обработки и о наличии запретов на обработку неограниченным кругом лиц ПДн, разрешённых субъектом ПДн для распространения

2.5	ч. 7 ст. 21 152-ФЗ	Регламентировать порядок уничтожения ПДн, в котором зафиксировать необходимость подтверждения уничтожения ПДн посредством составления акта с определённым содержанием и ведения журнала регистрации событий в информационной системе
2.6	п. 1 ч. 2 ст. 19152-ФЗ	Определить угрозы безопасности ПДн при их обработке в в информационной системе персональных данных (ИСПДн), задокументировать их в Модели угроз безопасности ПДн при их обработке в ИСПДн. При моделировании угроз необходимо руководствоваться Методикой оценки угроз безопасности информации (утверждена приказом ФСТЭК 05.02.2021)
2.7	п. 2 и 5 ч. 2 ст. 19 152-ФЗ	Определить и внедрить меры по обеспечению безопасности ПДн
2.7.1	ПП РФ № 1119	• Определить уровни защищённости ПДн при их обработке в ИСПДн в соответствии с утверждёнными требованиями
2.7.2	Приказ ФСТЭК № 21; Приказ ФСБ № 378	• Определить и внедрить меры защиты ПДн в ИСПДн по требованиям ФСТЭК и ФСБ
2.8	п. 5 ч. 1 ст. 18.1 152-ФЗ	Провести оценку вреда, который может быть причинён субъектам ПДн в случае нарушения требований 152-ФЗ. При проведении оценки нужно ориентироваться на Приказ Роскомнадзора от 27.10.2022 № 178
2.9	п. 14 ПП РФ № 1119	Назначить приказом лицо, ответственное за обеспечение безопасности ПДн в ИСПДн (для 3-го и 2-го уровней защищённости ПДн при их обработке в ИСПДн), или отдельное структурное подразделение (для 1-го уровня защищённости ПДн)
2.10	подп. «в» п. 13 ПП РФ № 1119	Утвердить перечень работников, допущенных к обработке ПДн в ИСПДн
2.11	п. 13 ПП РФ № 687	Разработать и утвердить Перечень лиц (должностей), допущенных к местам хранения ПДн (материальным носителям), а также Перечень мест хранения ПДн (материальных носителей)
2.12	п. 3 и 4 ч. 1 ст. 18.1, ч. 3 ст. 6 152-ФЗ	Свериться с матрицей распределения ответственности за безопасность ПДн между компанией и сервисом Yandex Cloud — Приложение 2 «Разделение ответственности за защиту персональных данных» к Заключению о соответствии системы защиты персональных данных требованиям № 152-ФЗ «О персональных данных». При необходимости внести правки в договор

3. Проведение процессов обеспечения безопасности ПДн

3.1	ч. 1 и 2 ст. 10.1 152-ФЗ	Обеспечить наличие допустимых оснований для обработки ПДн, разрешённых субъектом ПДн для распространения (как правило, требуется отдельное согласие в соответствии с требованиями Приказа Роскомнадзора от 24.02.2021 № 18)
3.2		Ознакомить работников под подпись со следующими положениями:
3.2.1	п. 6 ч. 1 ст. 18.1 152-ФЗ	• требованиями 152-ФЗ, Политикой обработки ПДн компании и остальной документацией, регламентирующей обработку ПДн в компании
3.2.2	п. 6 ст. 86 ТК РФ	• документами, устанавливающими порядок обработки ПДн работников, а также с документами об их правах и обязанностях в этой области (при наличии отдельной документации)
3.2.3	п. 6 ПП РФ № 687	• правилами обработки ПДн без использования средств автоматизации (если работник осуществляет такую обработку)
3.3	п. 4 ч. 1 ст. 18.1 152-ФЗ	Поддерживать документацию, регламентирующую обработку и защиту ПДн, в актуальном состоянии
3.4	п. 4 ч. 1 ст. 18.1 152-ФЗ; п. 17 ПП РФ № 1119	Проводить периодический внутренний контроль собственными силами и (или) аудит с привлечением внешнего поставщика услуг за соблюдением требований к обработке и обеспечению безопасности ПДн, в том числе контроль не реже одного раза в три года за обеспечением уровня защищённости ПДн и соблюдением условий использования средств защиты информации, соблюдением требований законодательства России по обработке ПДн. Задокументировать результаты в отчёте

4. Взаимодействие с третьими лицами

4.1	ч. 3 ст. 6 152-ФЗ	Проанализировать процессы обработки, в рамках которых ПДн передаются третьим лицам, и определить перечень лиц, которым поручена обработка ПДн. Поддерживать перечень лиц, которым поручена обработка ПДн, в актуальном состоянии
4.2	ч. 4 и 5 ст. 6 152-ФЗ	Обеспечить сбор согласий субъектов ПДн, чьи ПДн поручаются к обработке третьим лицам, на передачу их ПДн третьим лицам
4.3	ч. 3 ст. 6 152-ФЗ	Скорректировать уже заключённые договоры поручения на обработку ПДн с третьими лицами (при необходимости). Заключить договор (например, оказания услуг) и к нему заключить поручение на обработку ПДн, если договор вообще отсутствует. При этом если у третьего лица есть опубликованная публичная оферта, удовлетворяющая требованиям ст. 437 ГК РФ, то достаточно будет заключить поручение на обработку ПДн

5. Трансграничная передача

5.1	ст. 12 152-ФЗ	Определить бизнес-процессы компании, в рамках которых планируется трансграничная передача ПДн (составить перечень таких процессов и перечень государств, в которые будет осуществляться трансграничная передача ПДн). Этот этап может быть включён в 1-й этап, когда проводится анализ деятельности компании при обработке ПДн
5.2	ст. 12 152-ФЗ	Регламентировать внутреннюю процедуру осуществления и контроля трансграничной передачи ПДн. Например, во внутренней документации, регламентирующей обработку и защиту ПДн (в Положении по обработке и защите ПДн)
5.3		Определить порядок получения следующей информации от иностранных лиц, которым планируется передавать ПДн: • сведения о мерах защиты ПДн, которые применяет иностранное лицо; • информацию о правовом регулировании иностранного государства, куда передаются ПДн; • сведения о представителях иностранных лиц. Зафиксировать порядок во внутренней документации, регламентирующей обработку и защиту ПДн
5.4	ч. 14 ст. 12 152-ФЗ	Внести в типовые формы договоров с иностранными получателями ПДн и в действующие договоры (если они есть) механизм уничтожения ПДн по запросу компании (в случае принятия РКН соответствующего решения)
5.5	п. 7 ч. 4 ст. 12 152-ФЗ	Провести оценку соблюдения конфиденциальности ПДн и обеспечения безопасности ПДн при их обработке иностранным лицом и задокументировать её (например, с помощью акта о проведении такой оценки)
5.6	ч. 3 ст. 12 152-ФЗ	Уведомить РКН о планируемой трансграничной передаче ПДн
5.6	ч. 5 ст. 18 152-ФЗ	Обеспечить при сборе ПДн запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации

6. Уведомление об инцидентах

6.1	ст. 21 152-ФЗ	Регламентировать процедуру выявления, реагирования и нейтрализации последствий инцидентов, связанных с ПДн (в том числе определить порядок уведомления РКН в отношении инцидентов, связанных с ПДн). Например, во внутренней документации, регламентирующей обработку и защиту ПДн (в Положении по обработке и защите ПДн)
6.2	ч. 3.1 ст. 21 152-ФЗ	Уведомлять РКН об инцидентах, связанных с ПДн. Предоставлять результаты расследования инцидентов, связанных с ПДн

Документация в области обработки и защиты ПДн

Мы подготовили базовый перечень документов, который поможет вам соблюдать требования в сфере обработки и защиты ПДн по российскому законодательству. Обращаем ваше внимание на то, что комплект документов может увеличиться или уменьшиться, например, в зависимости от ваших бизнес-процессов, наличия или отсутствия ИСПДн, наличия или отсутствия контрагентов, которым может поручаться обработка или могут передаваться ПДн.

- ✅ Политика в отношении обработки ПДн
- ✅ Положение об обработке и защите ПДн
- ✅ Регламент взаимодействия с регуляторами в области обработки и защиты ПДн
- ✅ Регламент реагирования на инциденты безопасности, связанные с ПДн
- ✅ Регламент реагирования на запросы субъектов ПДн
- ✅ Приказ о проведении организационных мероприятий в сфере обработки и защиты ПДн
- ✅ Приказ о назначении лица, ответственного за организацию обработки ПДн
- ✅ Инструкция для лица, ответственного за организацию обработки ПДн
- ✅ Приказ о назначении лиц, ответственных за обеспечение безопасности ПДн в ИСПДн (при наличии систем с уровнем защищённости 3 и выше)
- ✅ Инструкция для лица, ответственного за обеспечение безопасности ПДн в ИСПДн (при наличии систем с уровнем защищённости 3 и выше)
- ✅ Инструкция для работника по правилам обработки ПДн
- ✅ Перечень должностей и третьих лиц, допущенных к обработке ПДн
- ✅ Перечень ИСПДн
- ✅ Перечень мест хранения ПДн (материальных носителей)
- ✅ План мероприятий по защите ПДн

- ✅ Журналы учёта средств обработки ПДн, доступа к ПДн и другие необходимые журналы
- ✅ Протокол определения показателей опасности угроз для субъектов ПДн
- ✅ Акты определения уровня защищённости ПДн
- ✅ Модель угроз безопасности ПДн для ИСПДн
- ✅ Форма соглашения о передаче ПДн
- ✅ Форма поручения на обработку ПДн
- ✅ Формы согласий на обработку ПДн
- ✅ Перечень (реестр) процессов обработки ПДн

Курс по Compliance в облачной инфраструктуре

Совместно с партнёрами, Yandex Cloud разработал бесплатный курс, который будет полезен тем, кто отвечает за соответствие требованиям безопасности, руководителям продуктов и проектов, а также аудиторам безопасности.

Курс — это введение, которое позволит погрузиться и понять задачу соответствия требованиям стандартов, таких как 152-ФЗ, PCI DSS и ГОСТ 57580, в условиях публичного облака.

Курс поможет:

- разобраться с основами построения защитных систем;
- организовать процессы работы с данными;
- вникнуть в юридические аспекты обработки данных в облачной инфраструктуре;
- узнать, как учитывать требования регуляторов и аудиторов отраслевых стандартов.

Для начала обучения
пройдите по ссылке

Kept

Kept — это аудиторско-консалтинговая фирма, которая прежде была частью международной сети KPMG, но формально покинула её 8 июня 2022 года. Группа по оказанию услуг в области кибербезопасности Kept предоставляет в том числе следующие услуги:

- **Инвентаризация процессов обработки ПДн.**
- **Анализ применимости** законодательства в области обработки и защиты ПДн.
- **Анализ соответствия компании** требованиям применимого законодательства в области обработки и защиты ПДн (152-ФЗ, GDPR и иное законодательство), подготовка детального отчёта с описанием реализуемых мер и дорожной карты с указанием критичности рекомендаций с учётом рисков для компании.
- Помощь в **реализации организационных мер по** обработке и защите ПДн:
  — актуализация или разработка проектов документов по ПДн;
  — содействие в проведении анализов рисков, связанных с обработкой ПДн (DPIA/LIA/TIA);
  — проведение мероприятий по повышению осведомлённости по вопросам обработки и защиты ПДн.
- **Консультационная поддержка** по вопросам в области обработки и защиты ПДн (Privacy Hotline).

Yandex Cloud

Публичная облачная платформа Yandex Cloud предоставляет крупным компаниям, среднему бизнесу и частным разработчикам **более 50 взаимосвязанных сервисов**: масштабируемую инфраструктуру, сервисы хранения, обработки и анализа данных, инструменты машинного обучения, средства разработки и сервисы для командной работы.

В Yandex Cloud действуют меры по защите персональных данных, указанные в Постановлении Правительства РФ № 1119 и приказе ФСТЭК № 21 в соответствии с требованиями к 1-му уровню защищённости (УЗ-1).

Дополнительная информация доступна по ссылкам:

- Аттестат соответствия
- Соглашение об обработке данных
- Заключение о соответствии системы защиты ПДн требованиям ФЗ-152 «О персональных данных»