

План мероприятий, проводимых специалистами Оператора ПД в целях выполнения требований законодательства по работе с персональными данными его клиентов и работников

1. Создаем пакет печатных документов по обработке персональных данных, для целей ознакомления с ними работников и предоставления в случае проверки Роскомнадзора (далее - РКН), запросов со стороны клиентов, или работников (бывших работников) Оператора ПД.

Для этого распечатываем в 2х экземплярах следующие документы:

- Политика оператора в отношении обработки персональных данных (подписываем руководителем на 1 листе, размещаем эл версию на сайте, или на удаленный диск (например Яндекс облако, Гугл Диск и т.д.), эл. ссылку на место размещения Политики вписываем в нижеуказанные Положения);

- Положения о работе с персональными данными работников (подписываем руководителем на 1 листе и ознакомляем работников Оператора ПД с документом под подпись);

- Положение о работе с персональными данными клиентов и контрагент (подписываем руководителем на 1 листе и ознакомляем работников Оператора ПД с документом под подпись);

- Приказ об утверждении перечня обрабатываемых персональных данных и категорий субъектов, персональные данные которых обрабатываются (подписываем руководителем на 4 листе и регистрируем в соответствии с реестром приказов Оператора ПД);

- Приказ об утверждении места хранения персональных данных (подписываем руководителем на 1 листе, регистрируем в соответствии с реестром приказов Оператора ПД и ознакомляем работников оператора с документом под подпись. В приложение к приказу указываем подразделения, специалисты которого занимаются обработкой и хранением документов содержащих ПД (помощник руководителя, бухгалтерия, специалисты кадровой службы, иные работники), места нахождения данных подразделений, наименование информационных систем, используемых при обработке ПД (1С Бухгалтерия, 1С Кадры, АМОСРМ и т.д.));

- Приказ о создании комиссии по оценке возможного вреда субъектам персональных данных (подписываем руководителем на 1 листе, регистрируем в соответствии с реестром приказов Оператора ПД и ознакомляем работников оператора с документом под подпись. В текст приказа вписываем ФИО председателя комиссии (как правило это руководитель), заместителя председателя комиссии и 2х её членов. В приложениях на страницах 2,3 необходимо проставить реквизиты приказа, приложениями к которому они являются.);

- Приказ о создании комиссии по уничтожению персональных данных (подписываем руководителем на 1 листе, регистрируем в соответствии с реестром приказов Оператора ПД и ознакомляем работников оператора с документом под подпись. В текст приказа вписываем ФИО председателя комиссии (как правило это руководитель), заместителя председателя комиссии и 2х её членов, можно меньше).

- Политика обработки файлов «cookie» (подписываем руководителем на 1 листе и ознакомляем работников Оператора ПД с документом под подпись, на место выделенном желтым цветом в тексте документа вставляем активную ссылку на Политику конфиденциальности, которая должна быть утверждена и размещена на сайте Оператора ПД);

- на случай проведения проверки РКН необходимо распечатать бланки согласия субъекта на обработку персональных данных, согласия работника на обработку персональных данных, согласия на обработку персональных данных третьим лицом, согласия на распространение персональных данных и форму уведомления об отказе на запрос о предоставлении персональных данных клиента. Документы не заполняем и не подписываем, только распечатываем.

Создаем физическую папку с файликами, в которую помещаем вышеуказанные документы, на случай проверки РКН или обращения клиентов.

2. Получение персональных данных клиентов/контрагентов через сайт Оператора ПД.

На сайте Оператора ПД необходимо разместить сканы Политики оператора в отношении обработки персональных данных, Политики обработки файлов «cookie» и Политики конфиденциальности.

При посещении сайта Оператора ПД клиент/контрагент получает следующее предупреждение: *«На сайте осуществляется обработка пользовательских данных с использованием Cookie в соответствии с Политикой обработки файлов cookie. Вы можете запретить сохранение Cookie в настройках своего браузера».*

В случае если клиент/контрагент приступил к заполнению своих персональных данных в таблице обратной связи, расположенной на сайте Оператора ПД, сайт уведомляет его о начале обработки ПД, следующим всплывающим сообщением: *«Оставляя свои персональные данные в данном разделе сайта Вы даете свое информированное и однозначное согласие на использование своих персональных данных _____ (ИНН _____/ОГРНИП или ОГРН _____) и третьими лицами, которые могут быть привлечены для исполнения обязательств, в соответствии со статьями 9, 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».*

Согласие выдается в отношении Ваших персональных данных с использованием средств автоматизации, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных.

Ознакомиться с политикой обработки персональных данных можно по ссылке: _____ . Продолжая взаимодействие со специалистом, Вы подтверждаете, что ознакомились с политикой и согласны с изложенными в ней положениями».

3. Размещаем следующие сообщения на платформах, через которые Оператор ПД получает персональные данные клиентов:

- сообщение чат бота в соцсети Телеграмм, или WhatsApp:

«Добрый день! Вы обратились в _____.

В ближайшее время с Вами свяжется персональный менеджер.

Продолжая диалог, вы даёте согласие на использование своих персональных данных _____, в соответствии с Политикой оператора в отношении обработки персональных данных » (здесь должна быть активная ссылка на Политику в формате pdf - _____).

- форма АМОСРМ для привлечения клиентов Оператора ПД (если вы её используете) должна содержать клавишу, при нажатии на которую, клиент попадает на Политику оператора в отношении обработки персональных данных в формате pdf .

4. Получение персональных данных специалистами Оператора ПД от клиентов, оставивших свои ПД на страницах оператора (в чат ботах) в соцсетях и в АМОСРМ.

3.1. Специалисты Оператора ПД при первом взаимодействии с клиентами, оставившими свои персональные данные (ФИО, телефон, адрес эл. почты и т.д.) в соцсетях или в системе АМОСРМ, направляю им текст уведомления об обработке персональных данных следующего содержания:

«Продолжая дальнейшее общение Вы даете свое информированное и однозначное согласие на использование своих персональных данных (ИНН /ОГРНИП или ОГРН) и третьими лицами, которые могут быть привлечены для исполнения обязательств, в соответствии со статьями 9, 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Согласие выдается в отношении Ваших персональных данных с использованием средств автоматизации, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных.

Ознакомиться с политикой обработки персональных данных можно по ссылке: . Продолжая взаимодействие со специалистом, Вы подтверждаете, что ознакомились с политикой и согласны с изложенными в ней положениями».

4.2. Перед совершением действий по получению от клиентов информации об их паспортных данных, СНИЛС, месте регистрации и т.д., специалист Оператора ПД должен направить им текст полного уведомления об обработке персональных данных следующего содержания:

«Продолжая дальнейшее общение Вы даете свое информированное и однозначное согласие на использование своих персональных данных (ИНН /ОГРНИП или ОГРН) и третьими лицами, которые могут быть привлечены для исполнения обязательств, в соответствии со статьями 9, 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Согласие выдается в отношении Ваших персональных данных с использованием средств автоматизации, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных.

Лицо, осуществляющее обработку персональных данных:

Перечень персональных данных, на обработку которых дается согласие:

Фамилия, имя, отчество, дата рождения, пол, номера телефонов (домашний, мобильный, рабочий), паспортные данные, адрес электронной почты, замещаемая должность, иные сведения, переданные оператору ПД.

Настоящее согласие действует бессрочно. При этом, Вы вправе отозвать данное согласие на обработку своих персональных данных, письменно уведомив об этом оператора.

В случае отзыва согласия на обработку своих персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев.

Ознакомиться с политикой обработки персональных данных можно по ссылке: [\[ссылка\]](#). Продолжая взаимодействие со специалистом, Вы подтверждаете, что ознакомились с политикой и согласны с изложенными в ней положениями.»

5. Получение согласия клиентов/контрагентов на обработку персональных данных в письменном виде.

При подписании Оператором ПД договоров с клиентами/контрагентами (физическими лицами, самозанятыми, или индивидуальными предпринимателями, либо представителями юридических лиц по доверенности), специалист должен вместе с бумажной версией договора подписать у них согласие на обработку персональных данных. Бумажные версии согласий и иных документов содержащих ПД хранятся в отдельной папке в офисе Оператора ПД.

Обработка персональной информации производится до окончания срока договора с клиентом/контрагентом.

Срок хранения документов на бумажных носителях – 3 года после истечения срока действия согласия или его отзыва клиентом.

6. Хранение и обработка персональных данных клиентов в электронном виде.

Полученные персональные данные от клиентов, оставивших их на сайте или страницах Оператора ПД (в чат ботах) в соцсетях и в АМОСРМ, заносятся специалистами Общества в систему АМОСРМ для использования ее в целях подбора оптимального варианта дальнейшей работы с клиентом. После использования данная информация сохраняется в облачном хранилище Яндекс облако, на сервере или на компьютере Оператора ПД, который будет определен как место хранения информации и документов, содержащих персональные данные. Данный компьютер представляется для ознакомления при проверке РКН, а в случае, если персональные данные хранятся в облачном хранилище Яндекс облако или системе или системе кадрового или бухгалтерского учета (1С Предприятие, 1С

Кадры и т.д.) Оператор ПД должен будет произвести выгрузку информации из данных мест хранения по требованию специалистов РКН.

Срок хранения электронных документов – 3 года.

7. Передача ПД клиентов третьим лицам.

В случае, если Оператор ПД собирается использовать полученную от клиента персональную информацию для её передачи третьим лицам, оно должно получить от клиента отдельное письменное согласие на поручение обработки персональных данных третьим лицам.

8. Распространения ПД клиента среди неограниченного круга лиц.

В случае, если Оператор ПД собирается использовать полученную от клиента персональную информацию для размещения в качестве примеров успешных кейсов на своих страницах в соцсетях, или иным способом, он должен получить у клиента письменное согласие на обработку персональных данных, разрешенных клиентом для распространения неограниченному кругу лиц.

9. Уничтожение персональных данных клиентов/контрагентов.

Персональные данные клиентов, оставленные ими на сайте, страницах Оператора ПД (в чат ботах) в соцсетях, в АМОСРМ или в ходе общения со специалистами оператора, подлежат уничтожению по истечению 3х летнего срока.

Персональные данные клиентов/контрагентов (физ. лиц, самозанятых, ИП и т.п.), с которыми Оператор ПД заключал договоры, обрабатываются до окончания срока договора, после этого хранятся еще в течение 3 лет и уничтожаются по истечению данных сроков.

После истечения вышеуказанных сроков, комиссией по уничтожению персональных данных Оператора ПД составляется акт об уничтожении персональных данных, содержащий перечень бумажных и электронных документов подлежащих уничтожению в связи с достижением цели обработки персональных данных и истечением сроков их хранения.

На основании данного акта специалистами Оператора ПД производится уничтожение:

- персональные данные в электронном виде, путем стирания с информационных носителей/физического уничтожения носителей, на которых хранится информация;
- персональные данные содержащихся на бумажных носителях, путем измельчения в шредере/сжигания.

Уничтожение персональных данных без решения комиссии не допускается.

10. Отзыв согласия на обработку персональных данных клиентом.

В случае отзыва клиентом или контрагентом согласия на обработку его персональных данных Оператор ПД прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных (выполнения условий договора), уничтожает персональные данные в срок, не превышающий 3 лет после истечения срока действия согласия. Обработка данных прекращается в течение 10 дней, с момента получения Оператором ПД отзыва согласия на обработку ПД.

11. Обработка, хранение и уничтожение персональных данных соискателей работы, работников и бывших работников ИП

Персональные данные, полученные при работе с соискателями работы, работниками и бывшими работниками ИП, поступают к специалистам кадровой службы (специалистам компании, которой данная функция передана по договору оказания услуг) на бумажных носителях (резюме, анкеты, сканы паспортов, трудовых книжек, и т.д.) и хранятся в специально отведенных для этого сейфах или железных ящиках с ключом.

Персональные данные, работников образующиеся в период его трудовой деятельности заносятся, обрабатываются и хранятся в электронной системе кадрового учета (например 1С Кадры). При приеме на работу все работники ИП подписывают согласия на обработку персональных данных на бумажных носителях (документ 8 пакета документов).

Персональные данные по кадровому учету хранятся 75 лет, включая персональные данные, имеющих отношение к денежным начислениям, например, зарплатных ведомостей, выдаче премий и материальной помощи.

Для менее значимых документов, служебной документации, командировочных, локальных приказов, справок и выписок установлен 5-летний срок обработки и хранения.

После истечения данных сроков, собирается комиссия по уничтожению персональных данных и принимает решение об их уничтожении, составляет протокол, на основании которого персональные данные стираются с электронных носителей и уничтожаются путем измельчения бумажных носителей в шредере

12. Установление фактов неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных клиентов, контрагентов и работников ИП

В случае выявления фактов неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав клиентов, контрагентов и работников ИП, он передает в Роскомнадзор следующие уведомления с информацией о компьютерных инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав клиента/контрагента, работника и предполагаемом вреде, нанесенном их правам, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о лице, уполномоченном ИП на взаимодействие РКН, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Штраф за невыполнение или несвоевременное выполнение ИП обязанности по уведомлению РКН об установление факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, составляет:

- на граждан **от пятидесяти тысяч до ста тысяч рублей;**
- на должностных лиц - **от четырехсот тысяч до восьмисот тысяч рублей;**

- на юридических лиц - **от одного миллиона до трех миллионов рублей.**