**Алгоритм по работе с персональными данными**

**1. Утвердить в организации положение о защите персональных данных, политику оператора в отношении обработки персональных данных** (ст. 86 ТК РФ, ст. 18.1 Федерального закона № 152-ФЗ)

Обеспечить неограниченный доступ к политике в отношении обработки персональных данных. Если есть интернет-сайт, разместить на всех его страницах политику в отношении обработки персональных данных (или иной аналогичный акт) так, чтобы посетители сайта имели доступ к ней (ч. 2 ст. 18.1 Закона о персональных данных).

Ознакомить с локальным актом работников под роспись (ч. 1 ст. 18.1 Федерального закона № 152-ФЗ). Если работник принимается на работу, и в организации уже есть такой локальный акт, то он знакомится с ним до подписания трудового договора в силу ч. 3 ст. 68 (п. 8 ст. 86 ТК РФ).

**2. Назначить лицо, ответственное за обработку персональных данных**

Лицо, ответственное за обработку персональных данных, будет следить за сохранностью персональных данных как на бумажных носителях, так и в электронном виде (ст. 18.1, 22.1 Федерального закона № 152-ФЗ).

Назначение ответственного лица оформить приказом.

Отразить данную обязанность в должностной инструкции работника.

**3. Закрепить права доступа к персональным данным в приказе**

Издать приказ, в котором отразить, кто (должности, Ф.И.О.), к каким персональным данным и с какой целью (какие функции выполняет с использованием персональных данных работников) имеет доступ; отразить данные о работниках, имеющих доступ к персональным данным как на бумажных носителях, так и в электронном виде.

**4. Получить обязательство о неразглашении персональных данных** (п. 7 ст. 86 ТК РФ)

Работодатель должен оформить с работниками, которые в силу своих должностных обязанностей имеют доступ к персональным данным других работников, обязательство об их неразглашении.

Необходимо предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено (ст. 88 ТК РФ).

**5. Выбрать способ хранения персональных данных, издать приказы** о помещениях для хранения и обработки

Для хранения используются:

* сейфы;
* металлические запираемые шкафы;
* деревянные запираемые шкафы;
* специально оборудованные помещения.

Обеспечить, чтобы к документам не было свободного доступа. Порядок хранения документов закрепляется в положении о защите персональных данных.

**Обратите внимание:** инспекция труда допускает хранение копий документов работников (паспорта, трудовой книжки, документа, подтверждающего регистрацию в системе индивидуального учета, или СНИЛС, ИНН, свидетельств о рождении детей, о браке, документов об образовании, военного билета, справки о наличии (отсутствии) судимости и т.д.) в личных делах только с их письменного согласия. При отсутствии письменного согласия работников копии документов должны быть возвращены работникам или уничтожены (Доклад с руководством по соблюдению обязательных требований, дающих разъяснение, какое поведение является правомерным, а также разъяснение новых требований нормативных правовых актов за II квартал 2017 г. (утв. Рострудом).

Однако проверяющие Роскомнадзора могут признать хранение копий таких документов нарушением даже при наличии такого согласия, ссылаясь на то, что хранение копий превышает объем обрабатываемых персональных данных работника.

**6. Регулярно проверять знание работников,** имеющими отношение к работе с персональными данными, требований нормативно-методических документов по защите таких данных, проводить профилактическую работу с должностными лицами, имеющими доступ к персональным данным работников, по предупреждению разглашения таких сведений.

**7. Следить за сроками хранения документов. Организовать порядок уничтожения информации. Издать приказ об экспертной комиссии.**

При хранении документов, содержащих персональные данные работников, следует учитывать сроки хранения, установленные, в частности, в ст. 22.1 Федерального закона от 22.10.2004 N 125-ФЗ и Перечне типовых управленческих архивных документов (утв. Приказом Росархива от 20.12.2019 N 236). Порядок применения указанного Перечня установлен Инструкцией, утвержденной Приказом Росархива от 20.12.2019 N 237.

**8. Техническая часть – защита информационных систем (Приказ ФСТЭК России от 18.02.2013 N 21, Постановление Правительства РФ от 01.11.2012 № 1119)**

Определить тип угрозы и подобрать один из четырех уровней защиты персональных данных (пп. 7–16 Требований к защите персональных данных, утв. Постановлением Правительства РФ от 01.11.2012 N 1119). Состав и содержание мер по обеспечению безопасности персональных данных для каждого уровня защиты определены Приказом ФСТЭК России от 18.02.2013 № 21.

**9. Получить согласие работника на обработку, передачу его персональных данных**

* при подборе персонала – на обработку, получение
* при оформлении приема на работу - на обработку
* при передаче информации третьим лицам (страховым организациям, аутсорсинговым организациям и др.)
* согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения

**10. Уведомить Роскомнадзор об обработке персональных данных**

* оператор до начала обработки личной информации обязан уведомить уполномоченный орган о своем намерении обрабатывать персональные данные согласно ч. 1 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ

Не уведомляем Роскомнадзор только в случае:

* если обрабатываются только данные в государственных информационных системах персональных данных, созданных в целях защиты безопасности государства и общественного порядка
* если осуществляет деятельность по обработке персональных данных исключительно без средств автоматизации
* если данные обрабатываются в случаях, предусмотренных законодательством о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства

**В случае изменения сведений в направленном уведомлении, а также в случае прекращения обработки персональных данных - уведомить Роскомнадзор** в течение 10 рабочих дней с даты возникновения таких изменений или с даты прекращения обработки (ст. 22 Федерального закона № 152-ФЗ).

**11. Проводить внутренний контроль (аудит) соответствия обработки персональных данных законодательству и локальным актам** (ст 18.1 Федерального закона № 152-ФЗ)

**12. Проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательством о персональных данных, соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей в соответствии с требованиями Роскомнадзора** **(требования пока не установлены)** (ст. 18.1 Федерального закона № 152-ФЗ)

**13. В случае доступа постороннего лица к персональным данным сообщить в Роскомнадзор** (ст. 21 Федерального закона № 152-ФЗ)

В течение 24 часов с момента происшествия:

* об инциденте
* его предполагаемой причине и вреде, причиненном субъектам данных
* мерах по устранению последствий инцидента
* представителе компании, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с происшествием

В течение 72 часов с момента инцидента провести внутреннее расследование и сообщить в Роскомнадзор о его результатах, а также о виновниках (при наличии).

**14. Взаимодействовать с госсистемой обнаружения компьютерных атак (ГосСОПКА), в том числе направлять сообщения об утечке данных (механизм взаимодействия пока не установлен)** (ст. 19 Федерального закона № 152-ФЗ)

**15. Сообщать работнику о его персональных данных в течение 10 рабочих дней с даты получения запроса (срок может быть продлен не более чем на 5 рабочих дней, если направить работнику мотивированное уведомление с указанием причин продления срока)** (ст. 20 Федерального закона № 152-ФЗ)

**16. Отвечать на запросы Роскомнадзора в течение 10 рабочих дней с даты получения запроса (срок может быть продлен не более чем на 5 рабочих дней, если направить мотивированное уведомление с указанием причин продления срока)** (ст. 20 Федерального закона № 152-ФЗ)

**17. Блокировать (обеспечить блокирование) персональных данных** **на период проверки:**

* в случае выявления неправомерной обработки персональных данных
* в случае выявления неточных персональных данных
* в случае отсутствия возможности уничтожения персональных данных в течение установленного срока (уничтожение в этом случае необходимо произвести не позднее чем 6 месяцев, если иной срок не установлен законами)