**Алгоритм по работе с персональными данными**

**1. Определить необходимость уведомления Роскомнадзора об обработке персональных данных**

* оператор до начала обработки личной информации обязан [уведомить](consultantplus://offline/ref=97AAEBC8DC8965078D4A530538DCC1E171DB86BBE1AF74B90922EE1664546B0EBA160DED636AFF04m6e8N) уполномоченный орган о своем намерении обрабатывать персональные данные согласно ч. 1 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ
* если оператор обрабатывает персональные данные только в рамках трудовых отношений, то сообщать о такой обработке он не обязан

При обязанности уведомления – уведомить орган Роскомнадзора.

**2. Определить, какие документы организации содержат персональные данные**

Работу с персональными данными регламентирует Федеральный закон № 152-ФЗ, гл. 14 ТК РФ. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Поскольку к персональным данным относится информация, способная каким-либо образом идентифицировать человека, то и все документы, касающиеся работников, относятся к персональным данным.

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

**3. Утвердить в организации положение о защите персональных данных**

[С](consultantplus://offline/ref=48C9DFE89FE31A21120123E2E03602A30D2833F0A871F00201E5EC05B055F8945B2D0F34CEEEAC672EiFL)татья 86 ТК РФ обязывает работодателя принять локальный нормативный акт (далее­ – ­­ЛНА), который будет регулировать порядок хранения и использования персональных данных.

Согласно [п. 8 ст. 86](consultantplus://offline/ref=48C9DFE89FE31A21120123E2E03602A30D2833F0A871F00201E5EC05B055F8945B2D0F30CD2Ei6L) ТК РФ работники должны быть ознакомлены под роспись с таким положением. Если работник принимается на работу и в организации уже есть такое положение, то он знакомится с ним до подписания трудового договора в силу ч. 3 ст. 68 ТК РФ.

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

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

Назначение ответственного лица оформляется приказом. Данная обязанность отражается в должностной инструкции работника.

**5. 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 сотрудниках, имеющих доступ к персональным данным как на бумажных носителях, так и в электронном виде.

**6. Получить обязательство о неразглашении персональных данных** ([п. 7 ст. 86](consultantplus://offline/ref=525817F7B324D4C59A6D7CA77AAC6AC57252B46C3B63BCCAA82ECEBB77C7C5EF323BE90946dEtBN) 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).

**6. Выбрать способ хранения персональных данных**

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.

Чтобы персональные в электронном виде данные не мог увидеть и тем более скопировать кто-то, кроме ответственных лиц. Поэтому компьютеры на рабочих местах надо разместить так, чтобы посторонние лица, вошедшие в помещение, не смогли увидеть информацию на мониторах.

**7. Выбрать способ защиты персональных данных в базах данных**

Исходя из типа угрозы применяется один из четырех уровней защиты персональных данных ([пп. 8](consultantplus://offline/ref=52ABA83CA729EB17DFA22C09570F25E8FB44B7845862FB37D7E1D5C9A25915E79552AC5F437154F603xBN)–[16](consultantplus://offline/ref=52ABA83CA729EB17DFA22C09570F25E8FB44B7845862FB37D7E1D5C9A25915E79552AC5F437154F103xCN) Требований к защите персональных данных). Состав и содержание мер по обеспечению безопасности персональных данных для каждого уровня защиты определены [Приказом](consultantplus://offline/ref=52ABA83CA729EB17DFA22C09570F25E8FB43B6825F64FB37D7E1D5C9A25915E79552AC5F437154FC03xEN) ФСТЭК России от 18.02.2013 № 21.

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

* при подборе персонала
* при оформлении приема на работу
* при передаче информации третьим лицам (страховым организациям, аутсорсинговым организациям и др.)