**Реестр операторов персональных данных роскомнадзора**

Реестр операторов персональных данных находится в свободном доступе на сайте Роскомнадзора (далее - РКН). Еще в 2015 году изменения в Закон № 152-ФЗ обязали организации, осуществляющие обработку личных данных регистрироваться в данном реестре. Однако не многие спешат это делать. Сегодня мы определим, когда и на каком основании вашу организацию может проверить Роскомнадзор. Какими правами и обязанностями наделены проверяющие и на что вам следует обратить особое внимание при подготовке к таким проверкам.

**Кто такой оператор персональных данных**

С первого взгляда к операторам персональных данных (далее - ОПД) можно отнести всех, кто работает с личной информацией граждан. То есть формально абсолютно все организации, как государственные, так и частные. Ведь любая компания нанимает сотрудников или заключает договора с потребителями работ или услуг. При этом они волей-неволей получают данные работников или клиентов.

Но это подход скорее формальный. И исходит из определения, приведенного в Законе № 152-ФЗ. Так, согласно статье 3 указанного законодательного акта к ОПД относят государственные и муниципальные структуры, физические и юридические лица осуществляющие сбор сведений. А также определяющие самостоятельно цели, состав и операции с такими сведениями.

**Требования к оператору персональных данных**

Во многом требования к ОПД сводятся к требованиям по защите получаемой информации. Так важнейшей задачей ОПД является обеспечение конфиденциальности доверенной ему информации. Однако, если такие сведения не привязаны к конкретному субъекту (гражданину), то есть являются обезличенными, то ст. 7 Закона №152-ФЗ позволяет передавать и распространять их без ограничений.

Так к примеру, статистическая отчетность по возрасту сотрудников компании без привязки к личности может быть общедоступна. В противном случае,когда информация о сотруднике распространяется (передается) с его ФИО, то на такие действия уже требуется получение разрешения от субъекта персданных.

А вот в случае ЧП и угрозе жизни сотрудника работодатель не просто должен, но и обязан предоставить запрашиваемую информацию, для спасения человека. Обычно к таким случаям относят несчастные случаи на производстве и когда бригаде скорой помощи, к примеру срочно необходимо знать группу крови пострадавшего.

**Необходимая документация в работе оператора персональных данных**

Принципы конфиденциальности должны быть прописаны в обязательном для работодателя локально-нормативном акте называемом “Положение о защите персональных данных”. С данным положением все поступающие на работу новые сотрудники должны быть ознакомлены под роспись в специальном журнале или листке ознакомления.

Еще на этапе проведения собеседования компания должна заручиться разрешением кандидата на обработку его личной информации. Для этого кандидат на вакантную должности или поступающий на работу заполняет специальное заявление (согласие). Корректно оформленные документы помогут избежать лишних вопросов от проверяющих и как следствие, штрафных санкций.

Несоблюдение работодателями правил обработки и хранения вверенной личной информации позволяет работнику отозвать свое согласие. После чего ОПД обязан их уничтожить.

**Уведомление Роскомнадзора об обработке персональных данных работников**

Требования “Закона о персональных данных” предельно просты. Все организации должны быть включены в реестр операторов осуществляющих обработку персональных данных. Однако, как из любого правила есть исключения.

В случае проверки компании еще предстоит доказать, то приведенные в законе исключения могут быть распространены на компанию. А что-то доказать проверяющим бывает ой как сложно. Поэтому не включение компании в реестр является одним из самых распространенных нарушений.

Процедура включения в такой список не так сложна, поэтому безопаснее подать уведомление и избежать ненужных вопросов. К тому же это делается один раз на весь период существования организации. Опасаться лишних проверок после включения в реестр не стоит. На практике такое встречается крайне редко.

**Когда нужно уведомлять Роскомнадзор**

Уведомление Роскомнадзора должно осуществляться еще до начала ОПД. Так как обработка персданных начинается уже с момента подбора кандидатов, то включение в реестр обработки персональных данных должно осуществляться до этого. То есть в первые дни после регистрации юридического лица.

Однако, на практике организации достаточно поздно спохватываются о такой необходимости. Многие компании работают многие годы без уведомления и не подают его из-за боязни получить штраф за его отсутствие в момент подачи. Опасаться этого не стоит. В процессе подачи документов вас не оштрафуют за “опоздание”. А вот если у Вам нагрянет Роскомнадзор с проверкой, то здесь уже держитесь.

В том случае, если уведомление подается с опозданием не стоит в качестве даты начала ОПД указывать текущую дату. Правильнее будет указать фактическую, с которой начался процесс обработки.

**Как избежать уведомления Роскомнадзора**

Если Вы все же хотите избежать включения Вашей компании в реестр ПД Роскомнадзора, стоит внимательно изучить п. 2 ст. 22 Закона № 152-ФЗ. Данный пункт содержит исчерпывающий список тех, кто может избежать включения в реестр:

ОПД осуществляется исключительно в соответствии с трудовым законодательством. Обратите внимание, что если Вы получили от работника информацию не предусмотренную ТК РФ, например, номер мобильного телефона или ИНН, то под этот пункт Вы не попадаете.

Сведения используются только для целей исполнения договора между сторонами.

Личная информация членов религиозных и общественных организаций, не выходящая за рамки такой организации.

Гражданин сам сделал личную информацию общедоступной.

Сведения содержат только ФИО их владельца.

ПД применяются для выдачи одноразового пропуска.

Если ОПД производится в автоматизированных государственных информационных системах.

ПД обрабатывают без использования компьютерной техники.

Для соблюдения транспортной безопасности.

Как видите список достаточно ограничен и относится к узкому кругу компаний. Поэтому большинство юридических лиц под него все же не попадают

**Как заполнить и подать уведомление в Роскомнадзор**

Прежде всего отметим, что вся подробная информация о подаче уведомления содержится на сайте Роскомнадзора (https://pd.rkn.gov.ru). Уведомление заполняется и подается через сайт Роскомнадзора. Данная форма достаточно обширна и включает множество сведений о компании. Электронная форма это еще не все, что требуется от ОПД. Обычной почтой необходимо в адрес РКН направить документы согласно перечню. Список мы приведем ниже.

В форме уведомления кроме стандартных ИНН и ОГРН также потребуется сформулировать цели ОПД. Также указывается правовое обоснование обработки личной информации. Оно должно быть заполнено в соответствии с уставом компании. Так же в этом пункте указываются номера лицензий на осуществление деятельности, если таковые имеются.

Далее описываются меры предпринимаемые для защиты личной информации, применяемые средства обработки и шифрования.

Датой начала обработки ПД, как мы уже говорили выше, лучше указать фактическую дату начала, а не текущую. Также оператору обработки персональных данных предоставляется возможность ограничить время пребывания в реестре. То есть если обработка предполагается на какой-то определенный период, после которого данные будут уничтожены, это также можно указать. Окончание периода может быть определено как конкретной датой, так и наступлением какого-либо события.

Также потребуется указание какие именно сведения будут использоваться (ФИО, семейное положение, образование, адрес и т.д.). После необходимо описать, кто будет являться субъектом персданных и перечень действий с информацией. Описываются методы их обработки и способы передачи. Заключительной частью являются данные ответственного за ОПД в компании.

Далее заполненная форма предлагается к проверке и распечатывается. А ее электронный вариант отправляется в Роскомнадзор. Распечатанный экземпляр подписывается руководителем, проставляется печать и вместе с пакетом документов отправляется по почте в территориальный орган Роскомнадзора.

Портал государственных услуг, также предоставляет возможность заполнения такого уведомления, однако это менее удобно.

**Список документов для регистрации в реестре персональных данных Роскомнадзора**

Для включения в реестр потребуется собрать достаточно обширный круг документации. Конечно же потребуется:

Положение о защите персональных данных.

Форма согласия на их обработку.

Описание используемых систем обработки ПД и лиц допущенных для их обработки.

Перечень ОПД.

Перечень помещений, где ведется обработка.

Уведомление и др.

Прочитайте полезные статьи по теме:

Персональные данные работников: особенности обработки

**Срок регистрации оператора персональных данных**

После отправки уведомления на сайте Роскомнадзора работодатель получает его номер и код. После этого на специальной странице сайта представители компании могут отслеживать статус документа. А также узнать, когда предоставленные сведения попадут в реестр. Вся информация на сайте является общедоступной.

Нормативный срок регистрации уведомления составляет 15 дней.

Хотя уведомление и подается всего лишь раз, но при изменении данных компании необходимо производить корректировку. Изменение сведений должно быть внесено в систему не позднее 10 дней после изменения. А с учетом того, что данных вносимых в уведомление достаточно много, поэтому стоит внимательно отнестись к их корректировке.

**Принципы защиты персональных данных сотрудника**

Глава 14 Трудового кодекса РФ и Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных) позволяют определить основные принципы защиты личных сведений работника.

**Принцип 1.** Конфиденциальность получаемых персданных, ограничение доступа к ним иных лиц.

Работники не должны отказываться от своих прав на сохранение и защиту тайны. Лица, получающие такие данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен ПД работников в порядке, установленном федеральными законами.

Например, Налоговым кодексом РФ, Федеральным законом от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» и др.

**Принцип 2.** Достоверность и полнота персональной информации. Запрет включения в конфиденциальной информации недостоверных фактов и информации, полученной не от работника или от иных лиц без его письменного согласия. Если это не предусмотрено федеральным законом.

Работник вправе требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ.

Вправе ли мы направить запрос в медучреждение о правомерности работы нашего сотрудника в период временной нетрудоспособности у другого работодателя? Дело в том, что наш сотрудник, будучи на больничном, был замечен работающим водителем на автомобиле другой организации.

Согласно п. 3 ст. 86 ТК РФ все сведения о работнике следует получать у него самого. Если информацию возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель обязан сообщить работнику о целях, предполагаемых источниках и способах получения личных данных. А также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

Так как указанные мероприятия работодателем проведены не были, следует их исполнить либо воздержаться от направления запросов в медучреждение. Иначе будут нарушены требования законодательства и прав работника.

*Обратите внимание!*

*Целевой характер означает, что ПД должны храниться не дольше, чем этого требует цель, для которой они накапливаются, и подлежат уничтожению, если в них миновала надобность*

**Персональные данные сотрудников в информационных системах**

**Принцип 3.** Целевой характер личной информации, законность целей и способов ее обработки и добросовестность.

Согласно ст. 86 ТК РФ обработку персданных работника можно проводить исключительно для того, чтобы:

обеспечить соблюдение законов и иных нормативных правовых актов,

содействовать работникам в трудоустройстве, обучении и продвижении по службе,

соблюдать личную безопасность работников,

контролировать количество и качество выполняемой работы и сохранность имущества.

**Права сотрудников в отношении их персональных данных**

**Принцип 4.** Свободный доступ работника к своим данным и право на полную информацию о них. А равно и запрет работодателю объединять созданные для несовместимых между собой целей базы ПД. Недопустимость создания информационных ресурсов персонального характера, закрытых или ограниченных в доступе для работника, кроме случаев, предусмотренных федеральным законом.

**Принцип 5**. Гарантированность субъективных прав работника, связанных с защитой его личной информации. Государственные органы, работодатели обязаны соблюдать эти права.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту конфиденциальных данных работника, в соответствии с нормой ст. 90 ТК РФ несут:

дисциплинарную ответственность,

административную ответственность (ст. 13.11 и 13.14 КоАП РФ),

гражданско-правовую ответственность (ст. 277 ТК РФ для руководителя организации, ст. 1100 ГК РФ),

уголовную ответственность (ст. 137 и 138 УК РФ).

Разглашение сведений, составляющих служебную тайну (ст. 243 ТК РФ) может быть в качестве одного из оснований наступления полной материальной ответственности работников. Наряду с дисциплинарной ответственностью по ТК РФ (подп. «в» п. 6 ч. 1 ст. 81, ст. 192 ТК РФ), имеющих в связи с должностными обязанностями доступ к персданным работников.

**Кто проводит проверку соблюдения норм Закона о персональных данных**

В соответствии контрольные и надзорные полномочия в сфере защиты ПД имеет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (РКН). Также согласно установленным полномочиям определенные проверочные функции в данной сфере осуществляет Государственная инспекция труда.

Проверку персональных данных проводит Роскомнадзор

Один из значимых документов для ОПД - Административный регламент исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Государственная функция по осуществлению госконтроля (надзора) за соответствием обработки персданных требованиям законодательства РФ в области личных данных (далее - Регламент). Утв. приказом Минкомсвязи России от 14.11.2011 № 312.

Данный регламент определяет сроки и последовательность действий (административных процедур) РКН и ее территориальных органов. Также порядок взаимодействия с государственными и муниципальными органами, юридическими или физическими лицами, организующими и (или) обрабатывающими личной информацией. Также определяющими цели и содержание при обрабатывании личной информации, в рамках проведения проверок при осуществлении надзора.

*Обратите внимание!*

*Проверки Роскомнадзора и ее территориальных органов проходят в соответствии с требованиями Федерального закона от 2612.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»*

*Обратите внимание!*

*План проверок Роскомнадзора размещается на официальном сайте (http://www.rsoc.ru/)*

**Виды проверок Роскомнадзора**

Проводимые проверки могут быть плановыми и внеплановыми.

Плановые проверки проводятся на основании ежегодного плана проведения плановых проверок.

Основанием для включения плановой проверки в план является начало осуществления оператором деятельности по ОПД, а также истечение трех лет со дня:

государственной регистрации оператора в качестве юридического лица, индивидуального предпринимателя;

окончания проведения последней плановой проверки оператора.

Внеплановые проверки проводятся по следующим основаниям.

Основания для проведения проверок операторов персональных данных

Основание 1. Истечение срока исполнения оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства РФ в области персональных данных.

Основание 2. Поступление в Роскомнадзор или ее территориальные органы обращений:

заявлений граждан,

юридических лиц,

индивидуальных предпринимателей,

информации от органов государственной власти,

органов местного самоуправления,

из средств массовой информации о возникновении угрозы причинения вреда жизни, здоровью граждан; причинении вреда жизни, здоровью граждан.

Основание 3. Приказ руководителя Роскомнадзора, изданный в соответствии с поручениями Президента РФ или Правительства РФ.

Основание 4. Нарушение прав и законных интересов граждан действиями (бездействием) операторов при обработке их личных данных.

Основание 5. Нарушение операторами требований законодательства РФ в области личных данных, а также несоответствие сведений, содержащихся в уведомлении об ОПД, фактической деятельности.

В ходе проведения проверки Роскомнадзор или ее территориальный орган рассматривают документы оператора. Также исследуют (обследуют) информационную систему персональных данных в части, касающейся личных сведений субъектов персональных данных, обрабатываемых в ней.

Прочитайте полезные статьи по теме:

Изменения законодательства о защите персональных данных. Что нужно знать работодателю

Международное право в области защиты персональных данных

Основополагающим документом, принятым на международном уровне в целях развития института частной жизни, является Всеобщая декларация прав человека. Она утверждена 10.12.1948 на Генеральной Ассамблее ООН.

В статье 12 Декларации указывается, что каждый человек имеет право на:

защиту закона от произвольного вмешательства в его личную и семейную жизнь,

произвольного посягательства на его честь и репутацию.

Статьи 8 и 10 Европейской конвенции о защите прав человека и основных свобод (1950 г.) закрепили право на уважение частной жизни, свободу получать и распространять информацию.

В Международном пакте о гражданских и политических правах (1966 г.) провозглашается запрет на вмешательство в личную и семейную жизнь. А также незаконное посягательство на честь и репутацию. Каждый имеет право на защиту от такого вмешательства и таких посягательств (ст. 17).

*Данные положения нашли отражение и развитие в:*

Руководстве ООН относительно компьютерных файлов персональных данных (1990 г.),

ряде конвенций и рекомендаций МОТ,

актах других международных организаций (например, в Основных положениях Организации по экономическому сотрудничеству и развитию (ОЭСР) о защите неприкосновенности частной жизни и международных обменов персональными данными (1980 г.)).

С 28.01.1981 была открыта для подписания Конвенция Совета Европы! «О защите физических лиц в отношении автоматизированной обработки данных личного характера», вступившая в силу с 01.10.1985. Ратифицирована Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

**Документы, проверяемые при проверке Роскомнадзора**

В этом году наша организация внесена в план проверок, размещенный на официальных сайтах Роскомнадзора и Генеральной прокуратуры. Подскажите, пожалуйста, наличие и содержание каких документов нам нужно проверить при подготовке к ней?

Вам и другим переработчикам персональных данных следует обратить особое внимание на те документы, которые будут рассматриваться в ходе проведения проверки.

К таким документам в соответствии с п. 67.1 Регламента относятся:

уведомление об обработке персональных данных;

документы, необходимые для проверки фактов, содержащих признаки нарушения законодательства РФ в области персональных данных, изложенных в обращениях граждан и информации, поступившей в Роскомнадзор или ее территориальный орган;

документы, подтверждающие выполнение организацией предписаний об устранении ранее выявленных нарушений законодательства РФ в области персональных данных;

письменное согласие субъекта персональных данных на обработку его персональных данных;

документы, подтверждающие соблюдение требований законодательства РФ при обработке специальных категорий и биометрических персональных данных;

документы, подтверждающие уничтожение диспетчером персональных данных субъектов персональных данных по достижении цели обработки;

локальные нормативные акты, регламентирующие порядок и условия переработки личных данных.

**Права Роскомнадзора при проведении проверки персональных данных**

Работодателю нелишне будет знать, какими правами при проведении проверки обладают должностные лица Роскомнадзора.

Согласно п. 6 Регламента должностные лица Роскомнадзора или ее территориального органа при проведении проверок вправе в пределах своей компетенции:

1) выдавать обязательные для выполнения предписания об устранении выявленных нарушений в области персональных данных;

2) составлять протоколы об административном правонарушении или направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении дел об административных правонарушениях. А также о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

3) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных;

4) использовать технику и оборудование, принадлежащие Роскомнадзору или ее территориальному органу;

5) запрашивать и получать необходимые документы (сведения) для достижения целей проведения проверки;

6) получать доступ к информационным системам персональных данных в режиме просмотра и выборки необходимой информации;

7) направлять заявление в орган, лицензирующий деятельность организации, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством РФ порядке. При условии если условием лицензии на осуществление такой деятельности предусмотрен запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

8) принимать меры по приостановлению или прекращению обрабатывающих действий с ПД, проходящей с нарушениями требований законодательства РФ в области персональных данных;

9) требовать от компании уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных. Проверки могут проводиться в двух формах: документарной и выездной.

*Обратите внимание!*

*Проверки могут проводиться как в отношении операторов, включенных в Реестр организаций, так и в отношении, не включенных в Реестр, но осуществляющих такую обработку*

Форма проведения плановой и (или) внеплановой проверки определяется Роскомнадзором или ее территориальным органом самостоятельно.

**Как проводится документарная проверка?**

Документарная проверка проводится по месту нахождения РКН или ее территориального органа. Предмет документарной проверки:

сведения, содержащиеся в документах компании, устанавливающих его организационно-правовую форму, права и обязанности;

документы, используемые при осуществлении деятельности по обработке персональных данных. Связанные с исполнением обязательных требований, установленных нормативными правовыми актами в области персональных данных, предписаний Роскомнадзора или ее территориального органа.

*Обратите внимание!*

*В ходе документарной проверки в основном изучаются документы, находящиеся в распоряжении проверяющих*

Если же достоверность сведений вызывает сомнения, то проверяющие вправе направить запрос о предоставлении необходимых для проверки документов. Получив такой запрос, оператор персональных данных обязан представить необходимые документы в течение 10 рабочих дней со дня получения запроса.

При этом все необходимые документы представляются в виде копий, заверенных печатью (при ее наличии) и подписью руководителя или иного уполномоченного представителя компании.

В прошлом месяце РКН проверял наши документы в сфере обработки и защиты персональных данных. Проверяющие запрашивали у нас копии некоторых документов и просили заверить их у нотариуса. Правомерны ли такие действия?

Действия проверяющих в данном случае неправомерны.

Регламентом прямо запрещено истребование оригиналов документов, а также их нотариального удостоверения (п. 70.7). Все необходимые документы представляются в виде копий, заверенных печатью (при ее наличии) и подписью руководителя или иного уполномоченного представителя (п. 70.6 Регламента).

Выявление нарушений в ходе проведения документарной проверки является одним из оснований для проведения выездной проверки

При проведении документарной проверки выявлены ошибки в представленных документах. Переработчику может быть направлено требование о представлении в течение 10 рабочих дней необходимых пояснений в письменной форме.

Если в результате проведенных мероприятий будут выявлены признаки нарушений обязательных требований, то должностные органы РКН вправе провести выездную проверку.

Также решение о проведении выездной проверки может быть принято в случаях, если предприятие не представило запрашиваемые документы в установленные законодательством сроки, т. е. в течение 10 рабочих дней.

**Как оформляются результаты проверки?**

Независимо от вида и формы по результатам проведения проверки составляется акт проверки. Требования к акту проверки содержатся в п. 78 Регламента. Пунктом 85 Регламента предусмотрено, что при выявлении нарушений вместе с актом выдается предписание об устранении нарушений.

Прочитайте полезные статьи по теме:

Защищаем персональные данные в информационных системах

Выносимые меры по результатам проверки оператора персональных данных

В случае выявления нарушений по результатам проверок возможны следующие меры:

Мера 1. Выдача предписания об устранении выявленного нарушения.

Мера 2. Направление протокола с материалами проверки в суд либо в прокуратуру в случае выявления административного правонарушения. Составление протокола об административном правонарушении.

Мера 3. Направление материалов проверки в органы прокуратуры, другие правоохранительные органы для рассмотрения вопроса о возбуждении уголовного дела. Если в ходе проверки выявлено уголовно наказуемое деяние.

Основные положения Регламента представлены в таблице.

**Правила проведения проверок Роскомнадзора**



Проверку оператора персональных данных проводит Гострудинспекция

В рамках полномочий, предоставленных ГИТ положениями ТК РФ, в ходе проведения проверки государственный инспектор труда вправе проверить исполнение требований гл. 14 ТК РФ.

Основным нарушением, которое может выявить проверяющий в этой области, является отсутствие в организации локального нормативного акта, регулирующего порядок обработки персональных данных работников и (или) то, что работники не осведомлены о его существовании и не ознакомлены под роспись с его положениями.

В ТК РФ прямо не указано, что работодатель должен иметь локальный нормативный акт, регулирующий порядок переработки ПД работников. Может ли трудовой инспектор проверить наличие этого документа?

Несмотря на то, что в ТК РФ напрямую отсутствует обязанность работодателя иметь такой локальный акт в гл. 14 можно найти неоднократные упоминания о наличии такого документа.

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке личной информации работника обязаны соблюдать требование п. 8 ст. 86 ТК РФ. Обязательно знакомить работников и их представителей под роспись с документами работодателя, устанавливающими порядок ОПД работников, а также об их правах и обязанностях в этой области.

Согласно ст. 87 ТК РФ порядок хранения и использования персданных работников устанавливается работодателем с соблюдением требований ТК РФ и иных федеральных законов.

При передаче ПД работника работодатель должен соблюдать также требование осуществления передачи личных сведений работника в пределах одной организации (ст. 88 ТК РФ). С локальным нормативным актом, с которым работник должен быть ознакомлен под роспись.

Кроме того, согласно ст. 18.1 Закона о персональных данных оператор, являющийся юридическим лицом, должен издать документы, определяющие:

политику в отношении обработки конфиденциальной информации,

локальные акты по вопросам обработки ПД,

локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

Организация обработки персональных данных работодателем должна регламентироваться соответствующим ЛНА, наличие которого может проверить трудовой инспектор.

Название такого локального акта законодательством не определено. Работодатель вправе обозначить его сам. Как правило, такой документ называют Положением о порядке обработки персональных данных, Инструкцией о защите персональных данных и др. Работников нужно ознакомить с этим локальным нормативным актом под роспись в соответствии с требованиями ч. 3 ст. 68 ТК РФ до подписания трудового договора (либо при вступлении локального нормативного акта в действие).