

ИНСТРУКЦИЯ ПО РАБОТЕ С ЛОКАЛЬНЫМИ АКТАМИ

Введение

В этой инструкции мы коротко опишем виды и назначение разработанных документов. Данное описание поможет правильно понимать их назначение. Разработанные акты являются типовыми и соответствуют требованиям законодательства. Каждый разработанный Локальный акт содержит реквизиты организации и её полные и краткие наименования в тексте документов. Внесение правок и изменений в акты может привести к искажению смысла формулировок и нарушению закона.

Из используемой терминологии можно отметить два основных термина — «оператор персональных данных» и «субъект персональных данных». Согласно законодательству РФ, оператор персональных данных — это любое физическое или юридическое лицо, которое обрабатывает персональные данные. При этом хранение и даже уничтожение данных считается обработкой. Субъектом персональных данных является гражданин, являющийся собственником персональных данных. Без его согласия обрабатывать его данные запрещено законодательством.

К данной инструкции прилагаются несколько образцов по заполнению заявлений.

Журнал учёта электронных носителей

Данный журнал предназначен для учёта электронных носителей, на которых содержатся персональные данные. Персональные данные требуют строгого учёта и обеспечения сохранности, поэтому во многих организациях копии всех персональных данных хранятся на сменных носителях, таких как съёмные жёсткие диски, USB-флешки, CD и DVD дисках.

Такие копии полезны в случае утери данных с компьютера (сервера). Утеря персональных данных может произойти по разным причинам, таким как:

- ✓ выход из строя оборудования без возможности восстановления,
- ✓ хищение оборудования или жёстких дисков с данными,
- ✓ умышленное уничтожение оборудования или данных и т.д.

В этом случае у организации будет возможность восстановить данные, которые были утеряны. Для этого данные периодически копируются на сменные носители и отправляются на хранение в сейф. При этом обязательно вести журнал учёта, чтобы знать что и куда копируется, когда копируется, где хранится и кто отвечает за хранение. Сведения из журнала помогут в случае утери данных быстро найти нужные носители с последними сохранёнными данными.

В пакете документов мы предлагаем образец журнала, который поможет вам правильно вести учёт носителей информации с персональными данными.

См. образец:

Учётный номер	Дата постановления на учёт	Вид электронного носителя, место его хранения (размещения)	Ответственный за использование и хранение		
			ФИО	подпись	дата
0125478	01.09.2019	USB-флеш Transcend сейф в каб.№5.	ФИО	подпись	01.09.2019
546876531845	01.10.2019	DVD диск Vtrbatim сейф в каб.№5.	ФИО	подпись	01.10.2019

Учётный номер — в этой ячейке мы записываем учётный номер, который присваиваем носителю. Как правило у всех электронных носителей есть свой заводской серийный номер или идентификатор — его и можно указать, чтоб не выдумывать. К тому ж такой номер будет уникальный и никогда не потеряется. Если у носителя нет своего номера — его можно присвоить самостоятельно.

Дата постановления на учёт — это дата, когда носитель поставили на учёт (на баланс, если так понятней).

Вид электронного носителя, место его хранения (размещения) — тут понятно, например диск DVD, сейф в каб.№5.

Ответственный за использование и хранение — ФИО, подпись, дата. За хранение должен отвечать тот, кто не имеет доступа к персональным данным. Это делается в целях безопасности. Нередки случаи, когда сотрудники умышленно уничтожают данные или вносят изменения. Нельзя допустить чтобы доступ к данным и сохраняемым копиям был в руках одного сотрудника. В случае надобности он может уничтожить все имеющиеся копии.

Журнал по учету мероприятий по контролю

В данном журнале требуется отражать возникающие аварийные ситуации, связанные с персональными данными, такими как:

- Дата, время аварийной ситуации
- Описание аварийной ситуации
- Принятые меры
- Дата, время ликвидации аварийной ситуации
- Последствия аварийной ситуации
- Ф.И.О. и подпись ответственного лица

Журнал учёта обращений граждан по обработке ПДн

Данный журнал ведётся для учёта обращений граждан по вопросам обработки персональных данных. В журнале отражаются следующие данные:

- Сведения о запрашиваемом лице
- Краткое содержание обращения
- Цель запроса
- Отметка о предоставлении информации или отказе предоставления
- Дата предоставления или отказа в предоставлении информации
- Подпись ответственного лица
- Примечания

Акт об уничтожении носителей ПНд

Акт об уничтожении носителей персональных данных можно считать приложением Журнала учёта электронных носителей. Данный Акт необходим, когда нужно уничтожить носитель с персональными данными. Такая необходимость может возникнуть при замене устаревших носителей информации на новые или при создании обновлённой копии персональных данных. Чтобы не хранить бесконечное число устаревших данных их требуется уничтожать. Нельзя просто так выбросить флешку или диск с данными — он может попасть в руки злоумышленника. Носитель нужно уничтожить физически таким образом, чтобы восстановление данных с него было невозможным.

Например USB-флешку нужно поломать так чтобы повредить чип памяти. Если флешку просто поломать, то любой ИТ-специалист может произвести пайку. Даже сломанная флешка может сохранять данные. Флешку желательно разбить. То же самое с картами памяти SD и микро-SD.

Диски CD и DVD тоже нужно уничтожать физически — поломать, порезать ножницами. Можно просто нагреть зажигалкой в любом месте, пока он не деформируется так, что его невозможно будет использовать. Если одновременно уничтожаются несколько носителей, не нужно отдельно составлять на каждый носитель свой Акт. Достаточно все уничтожаемые носители отразить в таблице одного Акта.

См. образец:

№	Дата	Тип носителя	Рег. или инвент. № носителя ПНд	Способ уничтожения
1	00.00.0000	USB флеш USB-флеш Transcend 8 Gb	102145887454	Разбит (или поломан на несколько частей) без возможности восстановления данных
2	00.00.0000	DVD диск Vtrbatim 4 Gb	102145887454	Порезан ножницами на несколько частей без возможности восстановления данных

Акт оценки потенциального вреда субъектам персональных данных

Данный Акт относится к информационной безопасности персональных данных. Постановление Правительства РФ от 01.11.2012 №1119 требует от оператора определить тип актуальных угроз и сделать оценку возможного вреда субъектам персональных данных, в случае возникновения такой угрозы.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

- 1. Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.*
- 2. Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.*
- 3. Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.*

Определив уровень угрозы нужно обеспечить необходимый уровень защищенности персональных данных при их обработке в информационной системе и отразить это в соответствующем Акте. В разработанном образце отражён уровень вреда, который рассчитан на основе предоставленных Вами данных о типах существующих угроз.

Определение уровня защищенности персональных данных в ИСПДн

В данном локальном акте должен быть отражен уровень защищённости на основе Акта оценки потенциального вреда субъектам персональных данных. Для определения уровня защищенности персональных данных ИСПДн в Акте приводится Таблица 1. «Уровни защищенности персональных данных в ИСПДн». На основании данных из анкеты определяется требуемый уровень защищенности, который нужно обеспечить для защиты персональных данных — от УЗ1 до УЗ4.

Перечень АРМ участвующих в обработке ПДн

Данный документ представляет собой таблицу с данными об автоматизированных рабочих местах, на которых происходит обработка персональных данных. Таблица достаточно проста и не требует пояснений для специалиста, который обслуживает АРМ учреждения. В таблице не нужно перечислять все компьютеры, ноутбуки и серверы организации — достаточно указать только те, на которых обрабатываются персональные данные. Если на данном АРМ не хранятся персональные данные, это не значит что на этом АРМ не происходит обработка. Через такой компьютер может осуществляться доступ к другим АРМ, которые содержат данные. Или через такой компьютер могут отправлять/принимать персональные данные.

Итак, если компьютер каким-то образом принимает участие в обработке персональных данных или имеет возможность доступа по сети к АРМ на которых хранятся данные, то такой компьютер нужно отразить в этом Акте и обеспечить его безопасность.

Перечень ИСПДн

Данный локальный акт содержит таблицу с перечнем информационных систем персональных данных. Не следует путать ИСПДн и АРМ. АРМ — это компьютеры, ИСПДн — это информационные базы, содержащие персональные данные. К таким базам

могут относиться бухгалтерские программы, и всевозможные текстовые базы. В образцах заполнения есть вариант заполнения этой таблицы.

План внутренних проверок состояния защиты ПДн

План внутренних проверок создан для того чтобы своевременно осуществлять проверки состояния защиты. План внутренней проверки содержит следующую информацию:

- Название проверяемого мероприятия
- Периодичность проведения проверки
- Исполнитель

План содержит заполненную таблицу. При необходимости её можно редактировать.

Инструкции

Данные инструкции разработаны для обеспечения безопасности обработки и хранения персональных данных. Для того чтобы избежать проблем с безопасностью персональных данных нужно придерживаться рекомендаций, которые даются в инструкциях.

Лист ознакомления с локальными актами

Данный документ представляет собой шаблон списка ознакомления сотрудников с правилами обработки персональных данных. В случае возникновения проблемы сотрудник, который был ознакомлен с правилами обработки персональных данных, не сможет уйти от ответственности. Лист ознакомления заставляет сотрудников с ответственностью подходить к выполнению возложенных обязанностей, так как содержит его собственноручную подпись.

Отзыв согласия по обработке персональных данных

Данный документ представляет собой бланк заявления на прекращение обработки персональных данных. Такое заявление гражданин может подать оператору, который обрабатывает его персональные данные, например, работодатель или иная организация.

Право отозвать разрешение на обработку своих персональных данных гражданам гарантирует Статья 9, п2, 152-ФЗ «О персональных данных». Таким образом, если гражданин захочет прекратить обработку своих персональных данных, он должен будет написать заявление отзыва согласия. Данный документ как раз является бланком заявления.

Разместите его на сайте так чтобы его можно было скачать. В случае возникшей необходимости, гражданам у которых возникнет желание отозвать своё согласие можно будет отправить ссылку на скачивание документа или просто указать страницу сайта на которой они смогут скачать данный бланк, распечатать, заполнить и подать оператору, который обрабатывает их данные.

Перечень должностей допущенных к ИСПДн

Данный документ представляет собой бланк для заполнения списка должностей в организации, которые имеют доступ к персональным данным. Этот список нужен для разграничения прав доступа. Например, если в организации появилась новая должность,

сотрудники которой будут иметь доступ к персональным данным, то её нужно будет отразить в данном перечне, а сотрудников в Перечне лиц допущенных к ИСПДн. Определяется этот перечень специальным приказом о перечне лиц и должностей допущенных к ИСПДн. Образец приказа есть в предлагаемом пакете документов.

Перечень лиц допущенных к ИСПДн

Данный документ представляет собой бланк для заполнения списка лиц организации, которые имеют доступ к персональным данным. Этот список нужен для того чтобы знать, кто из сотрудников имеет доступ к персональным данным. Например, если в организации появились новые сотрудники, которые будут иметь доступ к персональным данным, то их нужно будет отразить в данном перечне, а их должность в Перечне должностей, допущенных к ИСПДн, если она отсутствует в списке. Определяется этот перечень специальным приказом о перечне лиц и должностей, допущенных к ИСПДн. Образец приказа есть в предлагаемом пакете документов.

Положение о разграничении прав доступа

Данный документ представляет собой локальный акт, из названия которого ясно, что в нём прописаны правила разграничения прав доступа к персональным данным. В каждой организации есть свои виды обрабатываемых данных и свои лица, которые допущены к разным категориям данных. В этом положении отражены разграничения. Каждая организация должна сама распределить сотрудников к данным в зависимости от выполняемых ими функций.

Положение о сайте

Положение о сайте является одним из самых важных документов, несмотря на то что сайты не содержат персональных данных, хотя могут их собирать. Положение определяет назначение, принципы построения и структуру информационных материалов, размещаемых на сайте, а также регламентирует его работу. Положение закрепляет за сайтом статус официального, что для организации является очень важным моментом. В качестве примера можем привести случаи, когда уполномоченные органы проверяли сайты на соответствие требованиям закона. Одному из сайтов выписали штраф за несоответствие требованиям законодательства, при этом сайт полностью соответствовал требованиям. Оказалось, что проверили старый сайт, не являющийся на момент проверки официальным. Несмотря на то что органам представили официальный сайт, избежать штрафа не удалось, так как не было официального подтверждения какой именно действительно является официальным. Если бы у этой организации в положении о сайте был прописан адрес сайта, то и вопросов бы не возникло. Таких случаев множество. Так вот в Положении о сайте, которое является официальным документом с подписью руководителя и печатью организации, прописан URL сайта — его адрес в сети Интернет.

Положение о сайте обязательный документ, хоть и не относится в полной мере к актам по персональным данным. На сайте он должен быть обязательно, так как является основным документом, регламентирующим работу сайта.

Положение об обработке персональных данных

Данное Положение относится к одним из ключевых документов отражающих политику организации в отношении обработки персональных данных. В документе перечислены основные понятия и состав персональных данных, способы сбора, обработки и защиты персональных данных. Документ должен быть обязательно размещён на сайте в соответствии с требованием ст 18.1 Федерального закона №152 "О персональных данных".

Приказы

Все приказы, представленные в данном пакете документов являются необходимыми, так как они являются внутренними НПА, регулирующими обработку персональных данных. Размещать на сайте обязательно.

Согласие на передачу данных третьей стороне

Данный документ представляет собой бланк заявления на разрешающий передавать данные субъекта третьей стороне. Если субъект такого согласия не давал, то передача данных запрещена законом.

В случае передачи, субъект должен указать какие данные он разрешает передавать и кому. Если данные передаются тем, кого нет в списке, то это является нарушением законодательства. К инструкции прилагается образец заполнения.

Согласие на получение персональных данных у третьей стороны

Данный документ представляет собой бланк заявления на разрешающий получать данные субъекта у третьей стороны. Если субъект такого согласия не давал, то получение данных запрещена законом.

Субъект должен указать какие данные он разрешает оператору получать и от кого. Если данные получены из источников, на получение из которых субъект не давал согласия, то это является нарушением законодательства. К инструкции прилагается образец заполнения.

Согласие субъекта на обработку его персональных данных

Как и в случае согласия на передачу и получение персональных данных, документ представляет собой бланк, который заполняет субъект персональных данных, давая таким образом разрешение оператору обработку своих персональных данных. Данное разрешение можно отозвать, и этим запретить обработку своих персональных данных. Отзыв можно сделать заполнив соответствующее заявление.

Соглашение о неразглашении

Данный локальный акт является соглашением о неразглашении персональных данных. Данное соглашение заключается между оператором обработки персональных данных и физическим лицом (сотрудником организации или сторонним специалистом, которому временно предоставляют доступ к персданным).

Форма уведомления

Данную форму получают только те организации, которых мы регистрировали в Роскомнадзоре. Если Вы не получили Уведомление, значит Вы уже зарегистрированы. Дважды зарегистрировать организацию в РКН невозможно.

Если Вы получили Уведомление, распечатайте его, поставьте на нём печать и подпись руководителя и отправьте бумажное письмо в Ваш территориальный отдел Роскомнадзора. Адрес куда отправить находится в шапке Уведомления. После этого ждите в течение месяца, пока пройдёт регистрация. Без этого бумажного подтверждения регистрация в РКН не пройдёт.

Проверить свою регистрацию можно на портале РКН в «Реестре операторов, осуществляющих обработку персональных данных» по своим реквизитам: названию, ИНН и регистрационному номеру, который выдаётся при регистрации. Реестр находится по адресу:

<https://rkn.gov.ru/personal-data/register/>

ОБРАЗЦЫ ЗАПОЛНЕНИЯ ЛОКАЛЬНЫХ АКТОВ

Заявление-согласие субъекта на передачу его персональных данных третьей стороне

Это документ согласия о том, что гражданин разрешает организации передавать его персональные данные в другие организации. При этом указывается организация куда будут передавать данные и имя ответственного кто будет оттуда принимать передаваемые персональные данные.

Я, _____,
(фамилия, имя, отчество)
паспорт серия _____ номер _____, выданный _____

_____ «___» _____ года, в
соответствии со статьей 86 Трудового Кодекса Российской
Федерации _____
(согласен / не согласен)

на передачу моих персональных данных, а именно:

- паспортные данные, ИНН;
- данные страхового свидетельства государственного пенсионного страхования;
- данные документов об образовании, квалификации или наличии специальных знаний;
- анкетные данные, (в том числе сведения о семейном положении, перемене фамилии, наличии детей и иждивенцев);
- документы о возрасте малолетних детей и месте их обучения;
- документы о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний);
- документы о состоянии здоровья (сведения об инвалидности, о беременности и т.п.);
- сведения, содержащиеся в приказах о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;
- документы о прохождении аттестации, повышения квалификации;
- иные документы, содержащие сведения, необходимые для расчета заработной платы, выплаты стимулирующих и компенсационных выплат.

Для обработки в целях обеспечения расчета и начисления заработной платы, уплаты налогов и выполнения иных обязанностей в соответствии с действующим законодательством.

Следующим лицам ФФОМС Ф.И.О.; ФССП Ф.И.О. и так далее

(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их передачу.

«___» _____ 20__ г. (подпись) _____

**Заявление-согласие субъекта на получение
его персональных данных у третьей стороны**

Это документ согласия о том, что гражданин разрешает организации запрашивать его персональные данные в других организациях. При этом указывается организация, откуда будут получать данные и имя ответственного кто будет оттуда передавать запрашиваемые данные.

Я, _____,
(фамилия, имя, отчество)
паспорт серия _____ номер _____, выданный _____
_____ «___» _____ года, в
соответствии со статьей 86 Трудового Кодекса Российской
Федерации _____
(согласен / не согласен)

на получение моих персональных данных, а именно:

- паспортные данные, ИНН;
- данные страхового свидетельства государственного пенсионного страхования;
- данные документов об образовании, квалификации или наличии специальных знаний;
- анкетные данные, (в том числе сведения о семейном положении, перемене фамилии, наличии детей и иждивенцев);
- документы о возрасте малолетних детей и месте их обучения;
- документы о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний);
- документы о состоянии здоровья (сведения об инвалидности, о беременности и т.п.);
- сведения, содержащиеся в приказах о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;
- документы о прохождении аттестации, повышения квалификации;
- иные документы, содержащие сведения, необходимые для расчета заработной платы, выплаты стимулирующих и компенсационных выплат.

Для обработки в целях обеспечения расчета и начисления заработной платы, уплаты налогов и выполнения иных обязанностей в соответствии с действующим законодательством

у следующих лиц: ФФОМС Ф.И.О.; ФСИН Ф.И.О.; ФССП Ф.И.О. и так далее
(указать Ф.И.О. физического лица или наименование организации, которыми сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

« ___ » _____ 20__ г.

(подпись) _____

**Согласие субъекта
на обработку его персональных данных**

Примерные сведения, которые заполняем в
этот документ.

- 1) Цель обработки персональных данных: учет кадрового состава Организации, учет лиц, оказывающих услуги (выполняющих работы) по гражданско-правовым договорам с Организацией;
бухгалтерский учет и контроль за финансово-хозяйственной деятельностью Организации;
контроль исполнением финансовых обязательств по заключенным договорам;
выплата заработной платы, вознаграждений, лицам, оказывающим услуги (выполняющим работы) по гражданско-правовым договорам с Организацией;
контроль за исполнением программы реабилитации;
Реализации уставной деятельности.
- 2) Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных: ФИО, дата рождения, семейное положение, образование и т.д.
- 3) Перечень действий с персональными данными, на совершение которых дается согласие Сбор, обработка, хранение, уничтожение.
- 4) Используемые оператором способы обработки персональных данных: автоматизированный и неавтоматизированный
- 5) Срок, в течение которого действует данное согласие : на весь срок трудовых отношений (договора) или конкретной даты.
- 6) Способ отзыва данного согласия: по письменному заявлению со стороны субъекта.

« ___ » _____ 20 ____ г. Подпись субъекта персональных данных _____

ПЕРЕЧЕНЬ

ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

№ п/п	Наименование ИСПДн(ее составной части)	Наименование объекта (полное и сокращенное) отраслевая (ведомственная принадлежность адрес объекта)	Исходные данные классификации ИСПДн					Уровень защищённости (УЗ1-УЗ4)	Примечание
			Структура ИСПДн	Наличие подключения к ССОП и сетям МИО (Интернет)	Режим обработки Пдн	Разграничение доступа пользователей	Нахождение ИСПДн ее составных частей) в пределах России		
1	ПАРУС – Муниципальный учет	Администрация ХХХХ-вского	Локальная Информационная система	Используется сеть связи общего пользования	Многопользовательская	С разграничением прав доступа	В РФ	УЗ2	