УТВЕРЖДЕНО

приказом СРО СОЮЗа

«Содружество строителей»

от 23 мая 2019 г. № 6.1-ПД

ПОЛОЖЕНИЕ
о порядке обработки персональных данных в СРО СОЮЗе «Содружество строителей»

СРО-СС-ПД-2.1.-2019-01

Содержание

Список условных сокращений

ИСПДн	–	Информационная система персональных данных
ПДн	–	Персональные данные
Положение	–	Положение о порядке обработки персональных данных
Организация	–	Саморегулируемая организация СОЮЗ «Содружество Строителей»
РФ	–	Российская Федерация
Субъект	–	Субъект персональных данных
ФСБ России	–	Федеральная служба безопасности России
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России

1. Общие положения

1.1 Положение о порядке обработки персональных данных (далее – Положение) в информационных системах саморегулируемой организации СОЮЗ «Содружество строителей» (далее – Организация), расположенного по следующему адресу:

443110, РФ, г. Самара, ул. Лесная, д. 23.

определяет порядок сбора, хранения, обработки, передачи и любого другого использования ПДн с использованием средств автоматизации и без использования таких средств в соответствии с законодательством РФ.

Положение разработано в соответствии с:

– Конституцией РФ;

– Трудовым кодексом РФ;

– Гражданским кодексом РФ;

– Федеральным законом от 27 июля 2006 г. № 152 «О персональных данных»;

– Федеральным законом от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации»;

– Постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом ФСТЭК от 15 декабря 2008 г. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом ФСТЭК от 14 февраля 2008 г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом ФСБ от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности» и иными нормативно-правовыми актами РФ в области обеспечения информационной безопасности.

1.2 В Организации не обрабатываются биометрические категории ПДн.

Организация не осуществляет трансграничную передачу ПДн.

1.3 Приказом генерального директора Организации назначается лицо, ответственное за организацию обработки ПДн. Организация определяет должностной регламент лица, ответственного за организацию обработки ПДн, в служебные обязанности которого, в частности, входит:

– осуществление внутреннего контроля за соблюдением Организацией и его работниками законодательства РФ о ПДн, в том числе требований к защите ПДн;

– доведение до сведения работников Организации положения законодательства РФ о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

– организация приема и обработки обращений и запросов субъектов ПДн или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.

1.4 Настоящее Положение является обязательным для исполнения всеми работниками, имеющими доступ к ПДн.

2. Общий порядок обработки

2.1 Субъект ПДн (далее – Субъект) – это:

– субъекты персональных данных, не являющиеся работниками Организации;

– работники Организации.

2.2 Обработка ПДн осуществляется в целях реализации прав и обязанностей Организации для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской федерации функций, полномочий и обязанностей в отношении субъектов ПДн в рамках:

– трудового законодательства при приеме на работу и заключении трудового договора, в процессе трудовых отношений, при предоставлении гарантий и компенсаций;

– законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также страховых взносов на добровольное и обязательное медицинское, пенсионное и социальное страхования;

– пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов;

– Устава Организации.

2.3 Обработка ПДн в иных целях, не предусмотренных законодательством РФ, не допускается.

2.4 При обработке ПДн обязаны соблюдаться следующие требования:

– обработка ПДн осуществляется с соблюдением Конституции РФ, законов и иных нормативных правовых актов РФ и Самарской области;

– ПДн не могут быть использованы в целях причинения имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан РФ;

– запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы;

– Работники или их законные представители должны быть ознакомлены под расписку с документами Организации, устанавливающими порядок обработки ПДн субъектов, а также их права и обязанности в этой области.

3. Получение персональных данных

3.1 Персональные данные следует получать непосредственно от субъекта ПДн. Субъект самостоятельно принимает решение о предоставлении своих ПДн и даёт письменное согласие на их обработку. В случае отказа предоставить ПДн Организация обязана разъяснить субъекту ПДн юридические последствия отказа предоставить свои ПДн.

В случае недееспособности или несовершеннолетия субъекта ПДн все ПДн субъекта следует получать от его законного представителя. Законный представитель самостоятельно принимает решение о предоставлении ПДн субъекта и даёт письменное согласие на их обработку Организации.

3.2 Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае недееспособности или несовершеннолетия субъекта согласие может быть отозвано законным представителем субъекта ПДн.

3.3 В случаях, когда Организация может получить необходимые ПДн субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. В уведомлении Организация обязана сообщить о целях, способах и источниках получения ПДн, а также о характере подлежащих получению ПДн и возможных последствиях отказа субъекта дать письменное согласие на их получение. Согласие оформляется в письменной форме в двух экземплярах, один из которых предоставляется субъекту, второй хранится в Организации.

3.4 Запрещается получать и обрабатывать ПДн субъекта о его политических, религиозных и иных убеждениях, частной жизни.

3.5 Запрещается получать и обрабатывать ПДн субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.6 В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ, Организация вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

3.7 Если ПДн получены не от субъекта ПДн, то до начала обработки таких ПДн Организация обязана предоставить субъекту ПДн следующую информацию:

– наименование либо фамилия, имя, отчество и адрес Организации или его представителя;

– цель обработки ПДн и ее правовое основание;

– предполагаемые пользователи ПДн;

– установленные Федеральным законодательством права субъекта ПДн;

– источник получения ПДн.

3.8 Организация освобождается от обязанности предоставить субъекту ПДн сведения, в случаях, если:

– субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим Организацией;

– ПДн получены Организацией на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн;

– ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника.

4. Доступ к персональным данным

4.1 Работники Организации, которые в силу выполняемых служебных обязанностей постоянно работают с ПДн, получают допуск к обработке ПДн с установленными правами доступа на срок выполнения ими соответствующих должностных обязанностей на основании Перечня лиц, участвующих в обработки ПДн в Организации, который утверждается генеральным директором Организации.

4.2 Перечень лиц, участвующих в обработке ПДн в Организации, должен поддерживаться в актуальном состоянии.

4.3 Доступ к ПДн может быть прекращен или ограничен в случае нарушения требований настоящего Положения, либо в случае перевода или увольнения работника.

4.4 В случае, если работник сторонней организации имеет доступ к ПДн Организации, необходимо чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПДн и обязанность сторонней организации и ее работников по соблюдению требований текущего законодательства в области защиты ПДн.

4.5 Организация утверждает Инструкцию пользователя информационной системы.

5. Передача персональных данных

5.1 При передаче ПДн субъекта ПДн Организация обязана соблюдать следующие требования:

– не сообщать ПДн третьей стороне без письменного согласия субъекта ПДн или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, а также в случаях, установленных федеральным законодательством.

– предупредить лиц, получающих ПДн, 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. Лица, получающие ПДн, обязаны соблюдать режим конфиденциальности;

– разрешать доступ к ПДн только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн, которые необходимы для выполнения ими конкретных функций;

– передавать ПДн представителям субъектов ПДн в порядке, установленном действующим законодательством, и ограничивать эту информацию данными, необходимыми для выполнения указанными представителями их функций;

– не сообщать ПДн субъекта ПДн в коммерческих целях без его письменного согласия;

– выдавать по заявлению субъекта ПДн (в случае необходимости - письменному), не позднее трех дней со дня подачи этого заявления, справки и копии документов, в случаях, предусмотренных законодательством (копии документов должны быть заверены надлежащим образом и выдаваться работнику бесплатно).

5.2 Учет передачи ПДн разрешается не производить при передаче их в случаях, установленных законом, а также при внутренних передачах, которые осуществляются в соответствии с настоящим Положением.

6. Порядок обработки персональных данных без использования средств автоматизации

6.1 Обработку ПДн субъектов ПДн без использования средств автоматизации осуществляют Работники Организации, занимающие должности согласно перечню лиц, участвующих в обработке ПДн в Организации.

6.2 ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее - материальные носители), в специальных разделах или на полях форм (бланков).

6.3 При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

6.4 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Организации, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых Организацией способов обработки ПДн;

– типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ПДн;

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

– типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

6.5 Уничтожение ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Порядок уничтожения ПДн определен в Положении о порядке уничтожения обрабатываемых ПДн.

6.6 Уничтожение информации на съемных носителях ПДн производится комиссией, утвержденной приказом генерального директора Организации, с оформлением Акта об уничтожении.

6.7 Документы на бумажных носителях, содержащие ПДн, должны храниться в закрытых помещениях с ограниченным правом доступа в закрытых шкафах.

7. Обязанности лиц, допущенных к обработке персональных данных

7.1 При работе со сведениями, содержащими ПДн, Работники Организации, осуществляющие обработку ПДн, обязаны:

– соблюдать требования настоящего Положения и внутренних нормативных документов Организации, определяющих процедуры обработки и защиты ПДн;

– хранить в тайне ставшие известными им сведения, содержащие ПДн, информировать непосредственно ответственного за организацию обработки ПДн о фактах нарушения порядка обращения с ПДн и о попытках несанкционированного доступа к ним;

– представлять ответственному за организацию обработки ПДн письменные объяснения о допущенных нарушениях установленного порядка работы, учета и хранения документов, а также о фактах разглашения сведений, содержащих ПДн.

8. Защита персональных данных

8.1 Организация при обработке ПДн принимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

8.2 Обеспечение безопасности ПДн достигается, в частности:

– определением угроз безопасности ПДн при их обработке в ИСПДн;

– применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности ПДн;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

– учетом съемных носителей ПДн;

– обнаружением фактов несанкционированного доступа к ПДн и принятием мер;

– восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

– контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

9. Права субъектов на защиту своих персональных данных

9.1 В целях обеспечения защиты своих ПДн субъекты имеют право:

– получать полную информацию о своих ПДн и обработке этих данных (в том числе автоматизированной);

– осуществлять свободный бесплатный доступ к своим ПДн, включая право получать копии любой записи, содержащей ПДн, за исключением случаев, предусмотренных ФЗ от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

– требовать исключения или исправления неверных, или неполных ПДн, а также данных, обработанных с нарушением ФЗ от 27.07.2006 г. № 152-ФЗ «О персональных данных».

9.2 Сведения о наличии ПДн должны быть предоставлены субъекту ПДн работником, ответственным за организацию обработки ПДн, при получении Организацией письменного запроса субъекта ПДн или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его

законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя.

9.3 Работник, ответственный за организацию обработки ПДн, при получении запроса от субъекта, на предоставление информации, касающейся обработки его ПДн, в зависимости от содержания запроса должен предоставить субъекту ПДн запрашиваемую информацию, в том числе содержащую (в предоставленной информации не должны содержаться ПДн, относящиеся к другим субъектам):

- подтверждение факта обработки ПДн Организацией, а также цель такой обработки;
- способы обработки ПДн, применяемые Организацией;
- сведения о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ;
- перечень обрабатываемых ПДн и источник их получения;
- сроки обработки ПДн, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его ПДн.

9.4 При обращении в Организацию субъекта ПДн, его законного представителя или уполномоченного органа по защите прав субъектов ПДн с целью подтверждения наличия, ознакомления, уточнения, уничтожения или отзыв согласия на обработку ПДн следует руководствоваться Порядком действий при обращении, либо при получении запроса субъекта ПДн или его законного представителя, а также уполномоченного органа по защите прав субъектов ПДн.

10. Конфиденциальность персональных данных

10.1 Работники Организации и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено ФЗ от 27.07.2006 г. № 152-ФЗ «О персональных данных».

10.2 Конфиденциальность ПДн, обрабатываемых Организацией, обеспечивается путем реализации комплекса организационных и технических мер по обеспечению безопасности обработки ПДн.

В каждом заключенном договоре, контрагентом или выгодоприобретателем, по которому является субъект ПДн, должен быть предусмотрен раздел о конфиденциальности (об обеспечении конфиденциальности) полученных в рамках настоящего договора ПДн.

10.3 Организация может передавать ПДн субъектов на обработку третьим лицам, если это необходимо для достижения целей обработки ПДн при этом третьи лица обязаны обеспечить конфиденциальность ПДн и безопасности ПДн при их обработке.

11. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

11.1 Персональная ответственность – одно из главных требований функционирования системы защиты ПДн и обязательное условие обеспечения эффективности этой системы.

11.2 Руководитель, разрешающий доступ работника к конфиденциальному документу, содержащему ПДн, несёт персональную ответственность за данное разрешение.

11.3 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут дисциплинарную, материальную, административную, уголовную ответственность, предусмотренную действующим законодательством РФ.

11.4 Каждый работник несёт единоличную ответственность за сохранность и конфиденциальность полученных в процессе работы ПДн субъектов.

11.5 За неисполнение или ненадлежащее исполнение работником возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера руководство Организации вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

11.6 Должностные лица, в обязанность которых входит обработка ПДн работника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечёт наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

12. Контроль выполнения требований

12.1 Организация внутреннего контроля процесса обработки ПДн Организации осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

12.2 Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

– обеспечение соблюдения работниками Организации требований настоящего Положения и нормативно-правовых актов, регулирующих сферу ПДн;

– оценка компетентности персонала, задействованного в обработке ПДн;

– обеспечение работоспособности и эффективности технических средств информационной системы Организации и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн;

– выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений;

– принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств информационной системы Организации;

– разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий;

– осуществление контроля над исполнением рекомендаций и указаний по устранению нарушений.

12.3 Результаты контрольных мероприятий являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн, по модернизации технических средств информационной системы Организации и средств защиты ПДн, по обучению и повышению квалификации работников, задействованных в обработке ПДн.