

Общество с ограниченной ответственностью
ООО «Сибирско-Уральский энергетический сервис»
ООО «СУЭС»



УТВЕРЖДАЮ

Генеральный директор

ООО «СУЭС»

А.В. Худяков

25 04 20 18 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в
ООО «Сибирско-Уральский энергетический сервис»

Тюмень
2018 г.

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных (далее по тексту - Положение) Общества с ограниченной ответственностью ООО «Сибирско-Уральский энергетический сервис» (далее по тексту - Оператор) определяет закрепление механизмов обеспечения защиты прав работников, контрагентов и кандидатов (далее по тексту - Субъект) Оператора при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Кодексом об административных правонарушениях РФ, Гражданским кодексом РФ, Уголовным кодексом РФ, а также с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом «О персональных данных» № 152-ФЗ от 27.07.2006 г.

1.3. Персональные данные относятся к категории конфиденциальной информации.

1.4. Действие настоящего Положения распространяется на всех субъектов персональных данных Оператора.

2. Понятие и состав персональных данных

2.1. Для целей настоящего Положения применяются следующие термины и определения:

Субъект персональных данных - физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Субъекты персональных данных Оператора подразделяются:

Контрагент - физическое лицо, обратившиеся к Оператору с целью выполнения работ, оказания услуг, купли – продажи имущества, либо состоящие в иных гражданско-правовых отношениях с Оператором.

Работник – физическое лицо, состоящее в трудовых отношениях с Оператором.

Кандидат – физическое лицо, предполагаемое к трудоустройству к Оператору на определенную должность/профессию.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу – субъекту персональных данных.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действие, направленные на раскрытие персональных данных определенному лицу или определённым кругу лиц.

Обезличивание персональных данных – действие, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действие, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с Федеральным законодательством не распространяется требование соблюдения конфиденциальности.

2.2. Под информацией о Субъекте понимаются сведения о фактах, событиях и обстоятельствах жизни, необходимые Оператору в связи с трудовыми/гражданско-правовыми отношениями и используемые им в целях защиты прав Субъекта.

2.3. Персональными данными являются сведения, относящиеся к конкретному Субъекту и используемые Оператором, в частности, в целях выполнения требований:

- выполнения работ, оказания услуг, купли – продажи имущества, заключения договоров гражданско-правового характера;
- трудового законодательства при приеме на работу и заключении трудового договора, в процессе трудовых отношений, при предоставлении гарантий и компенсаций и др.;
- налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога;
- пенсионного законодательства при формировании и предоставлении персонализированных данных о каждом получателе доходов, учитываемых при

начислении страховых взносов на обязательное пенсионное страхование и обеспечение;
- заполнения первичной статистической документации.

2.4. В состав персональных данных входят:

- анкетные и биографические данные (в т.ч. фамилия, имя, отчество, фотография, изображение, полученное при помощи видеофиксации, дата рождения, место рождения, пол, гражданство);

- паспортные данные (данные иного документа удостоверяющего личность);
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о занимаемой должности;
- сведения о составе семьи;
- сведения из трудовой книжки;
- сведения о воинском учете;
- сведения о заработной плате, других доходах;
- сведения о социальных льготах;
- сведения о состоянии здоровья;
- наличие судимостей;
- адрес места жительства;
- сведения о фактах, событиях и обстоятельствах жизни Субъекта, позволяющие идентифицировать его личность;
- контактный телефон;
- адрес электронной почты;
- место работы или учебы, состояние здоровья членов семьи и родственников;
- содержание трудового договора;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о присвоении индивидуального налогового номера;
- содержание налоговой декларации.

2.5. Источниками персональных данных являются:

- паспорт гражданина РФ;
- военный билет;
- анкета соискателя;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о присвоении индивидуального налогового номера;
- унифицированная форма Т-2 утвержденная постановлением Госкомстата Российской Федерации от 05.01.2004г. №1;
- автобиография;
- свидетельство о заключении/расторжении брака, свидетельство о рождении детей;
- медицинское заключение о состоянии здоровья;
- информационные материалы и трудовые книжки;
- приказы по личному составу (подлинники и копии);
- основания к приказам по личному составу;
- материалы по повышению квалификации и переподготовке, аттестации, служебных расследованиях;
- трудовой договор, дополнительные соглашения к нему;
- налоговые декларации;
- гражданско-правовые договоры, заключаемые Оператором;
- документы, полученные от Субъекта в ходе заключения реализации гражданско-правового договора;
- отчеты, подаваемые в органы статистики и другие органы, в соответствии с законодательством РФ.

2.6. Сведения, перечисленные в пп.2.4 настоящего Положения, являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставится. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, установленного номенклатурой дел Оператора, если иное не определено законом.

3. Сбор, обработка и хранение персональных данных

3.1 Порядок получения персональных данных.

3.1.1. Все персональные данные следует получать у самого Субъекта. Если персональные данные возможно получить только у третьей стороны, то Субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Субъект должен располагать информацией о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Субъекта дать письменное согласие на их получение.

3.1.2. Оператор обязан:

- осуществлять обработку персональных данных Субъекта исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении, повышении в должности/профессии, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

- при определении объема и содержания обрабатываемых персональных данных Субъекта руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ и иными федеральными законами.

3.1.3. Оператор не имеет права:

- запрашивать информацию о политических, религиозных и иных убеждениях и частной жизни Субъекта;

- запрашивать персональные данные Субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом;

- при принятии решений, затрагивающих интересы Субъекта, основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.1.4. Защита персональных данных Субъекта от неправомерного их использования или утраты должна быть обеспечена Оператором за счет его средств в порядке, установленном федеральным законом.

3.2. Порядок обработки, передачи, хранения и использования персональных данных Субъекта.

3.2.1. Под обработкой персональных данных Субъекта понимается получение, хранение, комбинирование, передача или любое другое использование персональных

данных.

3.2.2. Обработка персональных данных Субъекта осуществляется с согласия Субъекта, исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, оформления трудовых отношений, расчета и выдачи заработной платы или других доходов, налоговых и пенсионных отчислений, содействия в трудоустройстве, обучении, повышении в должности/профессии, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Оператора. Согласие на обработку персональных данных может быть получено при приеме на работу, заключении гражданско-правового договора по форме предусмотренной Положением (образец Согласия на обработку персональных данных в Приложении №1, 2 к настоящему Положению).

3.2.3. Полный доступ: к обработке, передаче и хранению персональных данных Субъекта имеют следующие должностные лица Оператора:

- генеральный директор;
- главный бухгалтер;
- начальник службы управления персоналом;
- начальник службы экономической безопасности;
- заместитель начальника службы экономической безопасности;
- начальник юридического отдела.

Ограниченный доступ к обработке персональных данных Субъекта, исходя из функциональных обязанностей должностных лиц, имеют следующие должностные лица:

Наименование должности	Персональные данные и перечень документов, к которым может быть допущен. А также цели, для которых данное должностное лицо имеет право обрабатывать данные сведения.
Секретарь-делопроизводитель	-паспортные данные Субъекта – для заказа билетов при отправлении в командировку и бронировании гостиницы;
	- адрес места жительства - для отправки корреспонденции.
Специалисты службы управления персоналом, отдела кадров	-паспортные данные Субъекта, сведения о семейном положении, детях, иждивенцах, сведения о трудовом и общем стаже, ИНН, СНИЛС, информация с военного билета, сведения о медицинских ограничениях, сведения о квалификации, образовании, опыте работы и имеющимся профессиональным навыкам, анкетные данные, сведения о заработной плате – для ведение кадрового делопроизводства.

Работники сектора по начислению заработной платы бухгалтерии	- сведения о семейном положении, детях, иждивенцах, копия трудовой книжки, справка с учебного заведения на детей обучающихся по очной форме обучения, копии свидетельств о браке, рождении детей – для произведения необходимых вычетов из заработной платы, установленных законодательством.
	-ИНН, номер страхового свидетельства государственного пенсионного страхования, паспортные данные, адрес места прописки, данные трудовой книжки, военного билета, приказы о приеме – для оформления бухгалтерской, налоговой отчетности.
	- сведения о трудовом и общем стаже – для оформления листков нетрудоспособности.
	- сведения о заработной плате, других доходах – для начисления заработной платы, подготовки реестров, платежных поручений в банк
Работники службы охраны труда и промышленной безопасности, отдела охраны труда	- номер страхового свидетельства государственного пенсионного страхования, адрес места прописки – для оформления специальной оценки условий труда, направления на периодический медицинский осмотр.
	- медицинские ограничения (группа инвалидности, условия, прописанные в карте реабилитации) – для соблюдения установленных условий работы.
Руководитель структурного подразделения	- сведения о семейном положении, возрасте детей – для предоставления гарантий, установленных законодательно, в частности для решения вопроса о возможности привлечения к работе сверхурочно, в выходные и праздничные дни, в ночное время, отправления в командировки.
	- сведения о профессии, квалификации, образовании, опыте работы и имеющимся профессиональным навыкам – для принятия решений о переводах, возложении дополнительных обязанностей.
	- медицинские ограничения (группа инвалидности, условия, прописанные в карте реабилитации) – для соблюдения установленных условий работы, решения вопроса о возможных переводах.
	-сведения о заработной плате, других доходах – для планирования штатной расстановки кадров, передачи расчетных листков работникам.
Работники юридического отдела	- паспортные данные работника – для оформления доверенностей.
	- данные о трудовой деятельности, документы об образовании – для оформления документов на разрешенные виды деятельности.
	При рассмотрении судебных споров – любая необходимая информация, которая требуется для разрешения спора.
Ведущий экономист, экономист, экономист по труду и заработной плате	- сведения о заработной плате, других доходах – для ведения статистической отчетности, штатного замещения.

Техники участков	-анкетные данные, документы о приеме на работу, сведения о семейном положении, детях, иждивенцах – для подготовки отчетов, ознакомления работников с документами
Заместитель генерального директора по экономике и финансам	- сведения о заработной плате, других доходах – для ведения фонда оплаты труда.

Работниками вышеуказанных подразделений должна обеспечиваться конфиденциальность персональных данных, за исключением случаев, предусмотренных законом.

3.2.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.2.5. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда, затруднения реализации прав и свобод Субъекта. Ограничение прав Субъекта на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено.

3.2.6. Контроль за осуществлением порядка обработки, передачи, хранения и использованием персональных данных Субъекта, возлагается на руководителей структурных подразделений Оператора, имеющих доступ к персональным данным, и специалиста по экономической безопасности Оператора.

3.2.7. Контроль за неразглашением персональных данных осуществляется начальниками службы экономической безопасности и службы управления персоналом Оператора.

3.2.8. Передача персональных данных Субъекта возможна только с согласия, за исключением случаев:

- когда это необходимо в целях предупреждения угрозы жизни и здоровья;
- по запросу органов дознания, следствия, прокуратуры и суда в связи с проведением расследования или судебным разбирательством, в пределах своей компетенции и в соответствии с действующим законодательством Российской Федерации;
- в иных случаях, прямо предусмотренных Федеральным законодательством.

3.2.9. При передаче персональных данных Субъекта Оператор должен соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия Субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья, а также в случаях, установленных федеральным законом;
- не запрашивать информацию о состоянии здоровья Субъекта, за исключением тех

сведений, которые относятся к вопросу о возможности выполнения трудовой функции;

- не сообщать персональные данные Субъекта в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные Субъекта о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными Субъекта в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным Субъекта только специально уполномоченным лицам, определенным приказом Оператора или настоящим Положением, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

3.2.10. Работник, имеющий доступ к персональным данным, должен соблюдать следующие требования:

- во время приема посетителей не допускается выполнять функции, связанные с обработкой, хранением, передачей и использованием персональных данных;

- не допускается отвечать на вопросы, связанные с передачей персональных данных, по телефону. Ответы на письменные запросы других учреждений и организаций даются в письменной форме на бланке Оператора и в том объеме, который позволяет не разглашать излишний объем персональных данных. По телефону передавать запрошенную третьими лицами информацию только с письменного согласия Субъекта (образец Согласия на передачу данных третьей стороне в Приложении №3 к настоящему Положению);

- при выдаче справки с места работы необходимо удостовериться в личности Субъекта, которому эта справка выдается. Не разрешается выдавать ее родственникам или другим лицам (за исключением случаев предоставления нотариально заверенной доверенности Субъекта);

- не разрешается при выходе из помещения оставлять какие-либо документы на рабочем столе или оставлять шкафы незапертыми. Документы, содержащие персональные данные Субъекта (п.2.4.настоящего Положения), хранятся в соответствии с требованиями законодательства и внутренних локальных актов;

- на рабочем столе работника может находиться только тот объем документов, с которым в настоящий момент он работает;

- принимать необходимые меры безопасности и обеспечить защиту информации, содержащей персональные данные, от несанкционированного доступа со стороны третьих лиц, в том числе не оставлять без присмотра носители такой информации, осуществлять их

хранение в сейфе либо в ином специально приспособленном для хранения документов месте;

- в конце рабочего дня все документы, дела, листы бумаги и блокноты с рабочими записями, инструктивные и справочные материалы, содержащие персональные данные, должны быть убраны таким образом, чтобы исключить доступ со стороны третьих лиц. Черновики и редакции документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются путем измельчения;

- при уборке помещений, в которых производится обработка, хранение, передача, использование персональных данных, обязательно присутствие работника соответствующего подразделения;

- сообщать непосредственному руководителю, а в его отсутствие лицу, исполняющему его обязанности, об утрате или недостатке документов, содержащих персональные данные Субъекта, ключей от сейфов и шкафов, печатей, а также о причинах и условиях возможной утечки таких сведений.

3.2.11. При обработке персональных данных на материальных носителях не допускается фиксация на одном материальном носителе тех данных, цели обработки которых заведомо не совместимы.

3.2.12. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если не имеется возможности осуществлять их отдельно, должны быть приняты следующие меры:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) только копия;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

3.2.13. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление).

3.2.14. Персональные данные Субъекта хранятся на бумажных носителях и в электронном виде.

3.2.15. Хранение текущей документации и оконченной производством документации, содержащей персональные данные Субъекта, осуществляется в подразделениях Оператора, а также в помещениях, предназначенных для хранения отработанной документации.

3.2.16. Документы, содержащие персональные данные Субъекта, могут выдаваться на рабочие места: руководителю, начальнику службы экономической безопасности, заместителю начальника службы экономической безопасности Оператора, для осуществления возложенных на них обязанностей.

Передача документов, содержащих персональные данные Субъекта, руководителю Оператора через секретаря-делопроизводителя допускается при наличии у него обязательства о неразглашении персональных данных.

Руководители структурных подразделений Оператора могут знакомиться с документами, содержащими персональные данные Субъекта, в помещении службы управления персоналом, под наблюдением работника службы управления персоналом. Субъект имеет право знакомиться только с документами, содержащими его персональные данные.

3.2.17. В случае изъятия документов, содержащих персональные данные Субъекта, производится запись с указанием основания для подобного действия и нового местонахождения документа. С документа, подлежащего изъятию, снимается копия, заверенная подписью работника службы управления персоналом, которая подшивается на место изъятых документов.

Замена документов, содержащих персональные данные Субъекта, запрещается. Новые исправленные документы помещаются вместе с ранее подшитыми.

3.2.18. При возврате документов, содержащих персональные данные Субъекта, тщательно проверяется сохранность документов, отсутствие повреждений, включение в материалы других документов или подмена документов. Просмотр документов производится работником службы управления персоналом, в присутствии должностного лица, получившего в пользование документы. В случае недостачи документа(ов) проводится служебное расследование.

3.2.19. Во исполнение настоящего Положения, Субъект обязан:

- предоставлять Оператору комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом РФ, при приеме на работу, заключении гражданско-правового договора и в процессе трудовой деятельности

в необходимых случаях;

- своевременно в срок, не превышающий 5 календарных дней, сообщать Оператору об изменении своих персональных данных.

3.2.20. Субъект имеет право:

- на полную информацию о своих персональных данных и обработке этих данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Субъекта, за исключением случаев, предусмотренных законодательством РФ;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных трудовым законодательством;
- при отказе Оператора исключить или исправить персональные данные Субъекта, заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия;
- требовать об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные Субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в суде любые неправомерные действия или бездействие Оператора при обработке и защите его персональных данных.

4. Доступ к персональным данным

4.1 Работники, допущенные к сведениям, содержащим персональные данные, несут персональную ответственность за соблюдение ими установленного у Оператора режима конфиденциальности этих данных. Прежде чем получить доступ к персональным данным, они должны изучить требования настоящего Положения и другие нормативные документы, определяющие защиту конфиденциальной информации у Оператора, и подписать соответствующее личное письменное обязательство. (Образец Обязательство о неразглашении персональных данных» в Приложении №4 к настоящему Положению),

4.2. Внутренний доступ.

4.2.1. Право доступа к персональным данным Субъекта, имеют лица, указанные в п.3.2.3. настоящего Положения. Другие Работники Оператора имеют доступ к персональным данным только с письменного согласия Субъекта.

4.2.2. По письменному заявлению Субъекта Оператор обязан не позднее трех рабочих дней со дня подачи этого заявления выдать копии документов, связанных с работой (копии

приказа о приеме, переводе, увольнении; выписки из трудовой книжки; справки о начислении заработной платы, других доходах, периоде работы у Оператора и другое). Копии документов, связанных с работой, должны быть заверены надлежащим образом и представляться Субъекту безвозмездно.

4.3. Внешний доступ.

4.3.1. К числу лиц, допущенных к персональным данным Субъекта имеют организации (и соответственно должностные лица, данных организаций) осуществляющие контрольные и надзорные функции, а также другие лица, установленные федеральными законами, в частности:

- налоговые инспекции;
- инспекции труда (инспектора труда правового департамента и департамента охраны труда);
- органы, осуществляющие миграционный учет иностранных граждан;
- органы ФСС РФ;
- органы Пенсионного фонда РФ;
- правоохранительные органы;
- страховые агентства;
- прокуратура РФ;
- подразделения муниципальных и государственных органов управления;
- кредитные учреждения.

4.4. Органы и должностные лица, указанные в п. 4.3.1. настоящего Положения имеют доступ к информации только в сфере своей компетенции, в порядке, установленном законодательством РФ.

4.5. Организации, в которые Субъект может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным только в случае письменного разрешения Субъекта.

4.6. Сведения о Субъекте могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления Субъекта о согласии на предоставление информации о нем.

4.7. Персональные данные Субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения. В случае развода и отсутствия соглашения сторон об уплате алиментов справка о заработной плате Субъекта может быть предоставлена в суд без его согласия, на основании письменного запроса и определения суда.

4.8. Согласие на обработку персональных данных может быть отозвано Субъектом. В случае отзыва Субъектом согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия Субъекта при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона. (Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных"). (Образец заявления на отзыв согласия на обработку персональных данных в Приложении 5 к настоящему Положению).

5. Общедоступные источники персональных данных

5.1. Включение персональных данных в общедоступные источники персональных данных возможно при наличии письменного согласия Субъекта.

5.2. В целях информационного обеспечения Оператором могут создаваться общедоступные источники персональных данных Субъекта (в том числе справочники, адресные книги, информационные стенды для потребителей услуг, оказываемых Оператором, информация в официальных источниках опубликования). В общедоступные источники персональных данных с письменного согласия Субъекта могут включаться его фамилия, имя отчество, год и место рождения, адрес, иные персональные данные, предоставляемые Субъектом.

5.3. При обезличивании персональных данных согласие Субъекта на включение персональных данных в общедоступные источники персональных данных не требуется.

5.4. Сведения о Субъекте могут быть исключены из общедоступных источников персональных данных по требованию самого Субъекта, либо по решению суда или иных уполномоченных государственных органов.

6. Защита персональных данных

6.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

6.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия,

экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

6.3. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Оператора.

6.4. Внутренняя защита.

6.4.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных.

6.4.2. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации.

6.4.3. Для защиты персональных данных Субъекта Оператор принимает следующие меры:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

- строгое избирательное и обоснованное распределение документов и информации между работниками. Порядок работы с документами, содержащими персональные данные Субъекта регламентирован должностными инструкциями, настоящим Положением, иными локальными нормативными актами Оператора.

- рациональное размещение рабочих мест, при котором исключалось бы бесконтрольное использование защищаемой информации;

- знание работником требований нормативно - методических документов по защите информации и сохранении тайны. Для этого со всеми работниками, допущенными к персональным данным проводится при допуске и периодически соответствующий устный инструктаж и обучение;

- наличие необходимых условий, исключающих несанкционированный доступ в помещения для работы с конфиденциальными документами и базами данных;

- организация порядка уничтожения информации. Документы уничтожаются решением специально созданной комиссией при необходимости. Способ уничтожения определяется данной комиссией;

- своевременное выявление нарушения требований разрешительной системы доступа

работниками подразделения;

-воспитательная и разъяснительная работа с работниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами. Данная обязанность возложена на руководителей структурных подразделений, в подчинении которых находятся работники, допущенные к персональным данным;

-не допускается выдача личных дел Субъекта на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только работникам, согласно п.3.2.11 настоящего Положения.

6.4.4. Для обеспечения безопасности персональных данных Субъекта при автоматизированной обработке предпринимаются следующие меры:

6.4.4.1. За организацию защиты персональных данных при автоматизированной обработке персональных данных у Оператора отвечает Администратор безопасности, назначенный приказом руководителя Оператора.

6.4.4.2. Каждый работник Оператора, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к персональным данным (пользователь), несет персональную ответственность за свои действия (бездействия) и обязан:

- хранить в тайне сведения о персональных данных, ставшие известными ему в соответствии с родом работы;
- при обработке персональных данных руководствоваться данным Положением;
- при выходе в течение рабочего дня из помещения объекта информатизации убирать документы и машинные носители информации, содержащие персональные данные в рабочий стол (шкаф или сейф), при возможности – закрывать и опечатывать его, а также закрывать само помещение объекта информатизации;
- использовать только штатные программные и технические средства, используемые у Оператора;
- выполнять мероприятия по антивирусной защите. Использовать антивирусное программное обеспечение. Проводить обязательную проверку получаемых из других сторонних организаций оптических компакт дисков и иных носителей антивирусными средствами перед копированием или запуском информации с них;
- производить выключение питания персонального компьютера после завершения своей работы при помощи стандартной процедуры ОС Windows «Завершение работы»;
- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами;
- знать и строго выполнять правила работы со средствами защиты информации,

установленными на его персональном компьютере;

- немедленно сообщать Администратору безопасности и ставить в известность руководителя подразделения в случае утери индивидуального устройства идентификации (при наличии) или при подозрении компрометации личного пароля, а так же при обнаружении:

- а) нарушений целостности пломб наклеек, нарушении или несоответствии номеров печатей) на системном блоке персонального компьютера или иных фактов совершения его отсутствие попыток несанкционированного доступа к персональному компьютеру;

- б) отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию персонального компьютера, выхода из строя или неустойчивого функционирования узлов персонального компьютера или периферийных устройств (дисководов, принтера и т.п.);

- в) некорректного функционирования установленных на персональном компьютере технических средств защиты;

- г) нештатных отводов кабелей и подключенных устройств.

6.4.4.3. Работникам Оператора категорически запрещается:

- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;

- оставлять включённым без присмотра персональный компьютер, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана);

- передавать кому-либо свое индивидуальное устройство идентификации (при наличии) или другие реквизиты разграничения доступа (кроме Администратора безопасности или руководителя своего подразделения);

- оставлять без личного присмотра на рабочем месте какое бы то ни было свое персональное устройство идентификации (при наличии), машинные носители и распечатки, содержащие сведения о персональных данных;

- использовать нештатные технические средства и системы;

- самостоятельно вносить изменения в состав, конфигурацию и размещение технических средств;

- использовать нештатные программные средства;

- проводить обработку конфиденциальной информации при неисправно работающих средствах защиты;

- вносить изменения в средства защиты информации, используемые на объекте информатизации;

- допускать к работам в базе персональных данных лиц, не имеющих допуска к этим

работам.

6.4.4.4. Персональные компьютеры, имеющие доступ к базам хранения персональных данных Субъекта, защищены паролями доступа.

6.4.4.4.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей и контроль осуществляет Администратор безопасности.

6.4.4.4.2. Различный уровень доступа пользователей к ресурсам информационной системы, обрабатывающей персональные данные, обеспечивается системой имен пользователей и паролей. Каждый пользователь имеет свое уникальное имя и известный только ему пароль.

6.4.4.4.3. Пароль – идентификатор субъекта доступа, который является его секретной информацией.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов, например: части имени пользователя, номера кабинета, дата рождения и другие памятные даты; последовательности подряд идущих символов клавиатуры (например: 1234567 или qwerty и т.п.); географических названий и другие данные, которые могут быть подобраны путем анализа информации о пользователе.

6.4.4.4.4. Недопустимо использовать в качестве пароля один и тот же повторяющийся символ, либо повторяющуюся комбинацию из нескольких символов (например: 111111 или w2w2w2 и т.п.). В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.). Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

6.4.4.4.5. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

6.4.4.4.6. Личный пароль пользователь не имеет права сообщать никому. При наличии в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых работников (исполнителей) в их отсутствие (с разрешения непосредственного руководителя), такие работники могут сообщить свои пароли и обязаны при первой невозможности сменить свои пароли на новые значения.

6.4.4.4.7. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 6 месяцев.

6.4.4.4.8. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу у Оператора и другие обстоятельства) администраторов средств защиты и других работников, которым по роду работы были предоставлены полномочия по управлению полной защитой.

6.4.4.4.9. Хранение работником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном сейфе, либо в ином месте, доступ к которому имеет только данный работник.

Запрещается:

- записывать пароль и хранить его в местах, где с ним могут ознакомиться посторонние лица;
- хранить пароли в записанном виде на отдельных листах бумаги;
- сообщать посторонним лицам свои пароли;
- повторно устанавливать ранее использованные пароли.

6.4.4.4.10. В случае возникновения возможности несанкционированного ознакомления с паролем, пользователь обязан немедленно изменить скомпрометированный пароль самостоятельно и сообщить об этом Администратору безопасности, либо обратиться к Администратору безопасности.

6.4.5. Определен порядок и организационное обеспечение процесса изменения списка пользователей и наделение (изменение) их полномочиями доступа к сведениям, содержащим персональные данные. Организационное и техническое обеспечение процессов добавления, удаления пользователя, изменение полномочий пользователя баз, содержащих персональные данные, и контроль действий пользователя при работе с назначенными полномочиями возлагается на Администратора безопасности.

6.4.6. Различный уровень доступа пользователей к информационным системам, обрабатывающим персональные данные, обеспечивается формированием уникального имени (учетной записи пользователя) на уровне операционной системы.

Учетная запись пользователя представляет собой набор данных, сообщающих операционной системе к каким папкам и файлам пользователь имеет доступ, какие он может делать изменения в работе компьютера, а также персональные настройки пользователя.

6.4.7. Процедура регистрации (создания учетной записи) или удаление учетной записи пользователя в операционной системе и предоставление (изменение) полномочий к базе

персональных данных иницируется служебной запиской непосредственного руководителя работника, для которого создается (изменяется, удаляется) учетная запись, либо руководителя, в подчинении которого находится специалист.

В служебной записке указывается:

- содержание запрашиваемых изменений: регистрация нового пользователя, удаление учетной записи пользователя, расширение или сужение полномочий зарегистрированного пользователя;

- должность, фамилия, имя и отчество работника;

- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю;

Служебная записка визируется начальником службы по экономической безопасности и направляется на исполнение Администратору безопасности.

Администратор безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (при первичном создании учетной записи) и заявленных прав доступа к базам персональных данных, включению его в соответствующие задачам группы пользователей и другие необходимые действия.

6.4.8. Оператор оставляет за собой право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

6.4.8.1. При работе с ресурсами сети Интернет недопустимо:

- использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, содержащему персональные данные;

- загружать и запускать исполняемые или иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.

6.4.9. Электронная почта Оператора является его собственностью и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

6.4.9.1. При работе с корпоративной системой электронной почты работникам

Оператора запрещается:

- использовать адрес корпоративной почты для оформления подписок без предварительного согласования с Администратором безопасности;

- публиковать свой адрес, либо адреса других работников Оператора на общедоступных Интернет ресурсах (форумы, конференции и т.п.);

- отправлять сообщения с вложенными файлами, общий объем которых превышает 14 Мегабайт;

- открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;

- осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;

- осуществлять массовую рассылку постовых сообщений рекламного характера без предварительного согласования с руководителем подразделения;

- рассылка через электронную почту материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;

- распространять информацию со сведениями о персональных данных, ставшей известной работнику Оператора по служебной необходимости либо иным путем;

- предоставлять кому-либо пароль доступа к своему почтовому ящику.

6.4.10. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение персональных данных у Оператора, применяется дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск, оптический диск и т.п.).

Резервное копирование и хранение баз персональных данных должно осуществляться на периодической основе – еженедельное резервное копирование с сохранением копий на файловом сервере и постоянным хранением не менее четырех последних версий резервных копий.

Съемные носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в негорючем шкафу или помещении, оборудованном системой пожаротушения.

6.4.11. В целях обеспечения антивирусной защиты при автоматизированной обработке персональных данных производится антивирусный контроль.

6.4.11.1. Периодический контроль состояния антивирусной защиты, а также контроль соблюдения установленного порядка антивирусной защиты осуществляется Администратором безопасности.

Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации несут работники, за которыми закреплены соответствующие персональные компьютеры.

6.4.11.2. При обнаружении компьютерного вируса или при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропажа файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан немедленно поставить в известность Администратора безопасности и прекратить работу

6.4.11.3. Периодическая проверка жестких магнитных дисков на отсутствие программных вирусов должна проводиться не реже одного раза в неделю. Обязательная проверка используемых в работе гибких магнитных дисков должна осуществляться перед началом работы с ними.

6.4.12. Защита персональных данных на бумажных носителях: все документы, содержащие персональные данные Субъекта, хранятся в кабинетах начальника службы управления персоналом, главного бухгалтера, помещениях службы управления персоналом, бухгалтерии Оператора, в специально отведенном для этого месте, с применением специального оборудования (металлические негорюемые шкафы, сейфы).

6.4.13. Ключи от специального оборудования в рабочее время хранятся у начальников вышеуказанных подразделений, без права передачи третьим лицам, на время их отсутствия ключи хранятся у лица, исполняющего обязанности руководителя подразделения.

6.5. Внешняя защита.

6.5.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение,

внесение вируса, подмена, фальсификация содержания реквизитов документа и др. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Оператора, посетители, Работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в службе управления персоналом.

6.5.2. Для защиты персональных данных Субъекта у Оператора действует приказ о соблюдении положений «Инструкции о пропускном и внутриобъектовом режиме ПАО «СУЭНКО», ООО «СУЭС».

6.6. Контроль за обеспечением режима при работе со сведениями, содержащими персональные данные Субъекта, осуществляется в целях изучения, анализа и оценки фактического состояния сохранности персональных данных, выявления недостатков и нарушений режима в работе с документами и сведениями, содержащими персональные данные Субъекта, установления их причин и выработки необходимых предложений.

Контроль за обеспечением режима при работе со сведениями, содержащими персональные данные Субъекта, осуществляют начальник службы экономической безопасности и начальник службы управления персоналом.

6.6.1. Для проверки обеспечения надежности работы с документами и сведениями, содержащими персональные данные Субъекта, у Оператора создается постоянно действующая экспертная Комиссия (приказом руководителя Оператора), комплектуется из опытных и квалифицированных работников, имеющих доступ к этой работе. Участие в проверке не должно приводить к необоснованному увеличению осведомленности проверяющих.

6.6.2. Проверки обеспечения режима при работе с документами и сведениями, содержащими персональные данные Субъекта, проводятся по мере необходимости комиссиями на основании приказа руководителя Оператора.

6.6.3. Проверяющие имеют право знакомиться со всеми документами и другими материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы и консультации со специалистами и исполнителями, требовать представления письменных объяснений, справок, отчетов по всем вопросам, входящим в компетенцию комиссии.

6.6.4. По результатам проверок составляется акт (справка) с отражением в нем состояния режима при работе с документами и сведениями, содержащими персональные данные Субъекта, выявленных недостатков и нарушений, предложений по их устранению. С актом после утверждения его руководителем Оператора под роспись знакомится руководитель структурного подразделения.

6.6.5. Об устранении выявленных в результате проверки недостатков и нарушений в режиме при работе с документами и сведениями, и реализации предложений руководитель подразделения в установленные комиссией сроки сообщает начальнику службы экономической безопасности.

6.6.7. В случае установления факта утраты документов и дел, содержащими персональные данные Субъекта, либо разглашения содержащихся в них сведений немедленно ставятся в известность руководитель Оператора (или лицо, исполняющее его обязанности) и начальник службы экономической безопасности. На утраченные документы составляется акт. Соответствующие отметки вносятся в учетные документы. Акты на утраченные документы постоянного хранения после их утверждения руководителем Оператора и по истечении срока передаются в архив.

6.6.8. В случае выявления в ходе проведенного расследования факта разглашения работником информации, содержащей персональные данные Субъекта, доступ к которой указанный работник получил в связи с исполнением им трудовых обязанностей; утраты носителей информации; передачи третьим лицам, а также использования для занятия любой деятельностью, которая может нанести ущерб Субъекту, указанный работник несет ответственность в соответствии с настоящим Положением и действующим законодательством.

7. Права и обязанности Субъекта в области защиты его персональных данных

7.1. Если Субъект считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав Субъектов или в судебном порядке.

7.2. Субъект имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

7.3. В целях обеспечения защиты персональных данных, хранящихся у Оператора, субъект имеют право на:

- полную информацию о составе и содержимом их персональных данных, а также о способе обработки этих данных;

- свободный бесплатный доступ к своим персональным данным.

Субъект имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных Оператором;

- 2) правовые основания и цели обработки персональных данных;
- 3) способы обработки персональных данных;
- 4) сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором, или на основании Федерального закона № 152-ФЗ;
- 5) сроки обработки персональных данных, в том числе сроки их хранения;
- 6) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;
- 7) информацию о осуществленной или о предполагаемой трансграничной передаче данных;
- 8) иные сведения, предусмотренные Федеральным законом № 152-ФЗ или Федеральным законодательством.

7.4. Сведения должны быть предоставлены Субъекту Оператором в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

7.5. Сведения предоставляются Субъекту или его представителю Оператором при обращении либо при получении запроса субъекта или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, сведения о заключении договорных отношений с Оператором, либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись Субъекта или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.6. Субъект вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а так же принимать предусмотренные законом меры по защите своих прав.

7.7. В случае выявления неправомерной обработки персональных данных при обращении, либо по запросу Субъекта или его представителя, уполномоченного органа по защите прав Субъектов, Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому Субъекту, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом,

действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении Субъекта или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав Субъектов, Оператор обязан осуществить блокирование персональных данных, относящихся к этому Субъекту, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы Субъекта или третьих лиц.

7.8. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, предоставленных Субъектом или его представителем, либо уполномоченным органом по защите прав Субъектов, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня предоставления таких сведений и снять блокирование персональных данных.

7.9. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором (или лицом, действующим по поручению Оператора), Оператор, в срок, не превышающий трех рабочих дней с даты выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязательно уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить Субъекта или его представителя, а в случае, если обращение Субъекта или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

7.10. В случае достижения цели обработки персональных данных Оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом,

действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является Субъект, иным соглашением между Оператором и Субъектом, либо если Оператор не вправе осуществлять обработку персональных данных без согласия Субъекта на основаниях, предусмотренных Федеральным законом №152-ФЗ или Федеральным законодательством.

7.11. В случае отзыва Субъектом согласия на обработку его персональных данных Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и Субъектом, либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом №152-ФЗ или Федеральным законодательством.

7.12. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен Федеральным законодательством.

7.13. Для своевременной и полной реализации своих прав, Субъект обязан предоставить Оператору достоверные персональные данные.

7.14. Субъект обязан:

7.14.1. Для своевременной и полной реализации своих трудовых, пенсионных и иных прав поставить в известность Оператора об изменении персональных данных, обрабатываемых Оператором в связи с трудовыми отношениями, в том числе изменении фамилии, имени, отчества, паспортных данных, о получении образования, квалификации, получении инвалидности и иных медицинских заключений, препятствующих выполнению своих должностных обязанностей, и прочих данных с предоставлением подтверждающих документов.

8. Ответственность за разглашение персональных данных

8.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных Субъекта, привлекаются к дисциплинарной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

8.2. За разглашение информации, содержащей персональные данные, ставшей известной работнику в связи с исполнением им трудовых обязанностей, Оператор вправе расторгнуть трудовой договор на основании подпункта «в» пункта 6 части 1 статьи 81 Трудового кодекса РФ.

9. Порядок утверждения, ввода в действие и внесения изменений в Положение

9.1. Настоящее Положение и изменения к нему утверждается руководителем Оператора, вводится в действие приказом и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным Субъекта, действует до введения нового Положения по защите персональных данных.

9.2. Все Субъекты Оператора должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

9.3. Подпись Субъекта в листе ознакомления с Положением по защите персональных данных означает его согласие и обязательство исполнения.

**СОГЛАСИЕ ОТ ЛИЦА, ПРИНИМАЕМОГО НА РАБОТУ,
НА ПЕРЕДАЧУ ПЕРСОНАЛЬНЫХ ДАННЫХ**

«___» _____ 20__ г.

Я,

(фамилия, имя, отчество Субъекта)

паспорт серии _____ № _____

выдан (дата, кем) _____

проживающий(ая) по адресу: _____

-далее Субъект,

разрешаю Обществу с ограниченной ответственностью «ООО «Сибирско-Уральский энергетический сервис» (ООО «СУЭС»)), расположенному по адресу: г.Тюмень, ул. Чекистов, 26, далее Оператор,

обрабатывать, в том числе: принимать, а также хранить, систематизировать, уточнять (обновлять, изменять), комбинировать, блокировать, уничтожать, следующие мои персональные данные:

Персональные данные	Перечень действий
Фамилия, имя, отчество	1. Публичное обращение 2. Публичные поздравления с днем рождения, юбилеями, профессиональными праздниками 3. Отражение данной информации в кадровых документах 4. Внесение данных в 1С 5. Указание на сайте компании 6. Размещение данных на внутреннем электронном портале компании 7. Размещение данных на бумажном носителе (внутреннем справочнике) компании 8. Указание на двери кабинета 9. Оформления бухгалтерской, налоговой отчетности
Дата, месяц, год рождения	1. Публичные поздравления с днем рождения, юбилеями (только дата и месяц рождения) 2. Отражение данной информации в кадровых документах 3. Внесение данных в 1С 4. Оформления бухгалтерской, налоговой отчетности
Место рождения	1. Внесение данных в программу 1С
Наличие детей и их возраст	1. Отражение данной информации в кадровых документах 2. Предоставление льгот, установленных действующими нормами законодательства, например, при сокращении численности и других кадровых процедурах 3. Предоставление налоговых вычетов (при наличии детей в возрасте до 18 лет, обучающихся по очной форме до 24 лет)

	- Публичное вручение новогодних подарков (при наличии детей в возрасте до 14 лет) - Предоставление льгот и гарантий, предусмотренных локальными нормативными актами ООО «СУЭС» - Публичное награждение (при участии в детских конкурсах) - Внесение данных в 1С
Семейное положение	- Отражение данной информации в кадровых документах - Предоставление льгот, установленных действующими нормами законодательства, например, при сокращении численности и других кадровых процедурах - Предоставление льгот и гарантий, предусмотренных локальными нормативными актами ООО «СУЭС» - Внесение данных в 1С
Ближайшие родственники	- Отражение данной информации в кадровых документах - Возможная связь в чрезвычайных случаях - Предоставление льгот и гарантий согласно действующему законодательству (например, предоставление отпусков без сохранения заработной платы, дней отдыха по уходу за ребенком-инвалидов) и других - Предоставление льгот и гарантий, предусмотренных локальными нормативными актами ООО «СУЭС»
Предыдущие места работы \службы (с указанием периодов, места работы \службы, должностей)	- Отражение данной информации в кадровых документах - Расчет страхового стажа на оплату листов нетрудоспособности - Уведомление предыдущего работодателя о приеме на работу бывшего государственного или муниципального служащего.
Образование, квалификация, профессия, наличие удостоверений	- Отражение данной информации в кадровых документах - Учет преимущественного права в случае сокращения численности - Внесение данных в списки кадрового резерва - Предложение перевода, соответствующего его квалификации, в случаях установленных действующим трудовым законодательством - Внесение данных в 1С
Учебные заведения и периоды учебы	- Отражение данной информации в кадровых документах - Внесение данных в 1С
Знание иностранных языков (каких и степень знания)	- Отражение данной информации в кадровых документах - Внесение данных в списки кадрового резерва
Адрес, дата, месяц, год регистрации по месту жительства	- Отражение данной информации в кадровых документах - Оформление бухгалтерской, налоговой отчетности - Внесение данных в 1С - Оформление доверенностей
Фактический адрес места жительства	- Отправка официальных сообщений (корреспонденции от Оператора) - Отражение данной информации в кадровых документах - Случаи экстренной связи с лицами, проживающими совместно - Внесение данных в 1С
Контактный телефон	- Отражение данной информации в кадровых документах - Внесение данных в 1С
Сведения о состоянии здоровья, группа инвалидности, условия, прописанные в карте реабилитации	- Внесение данных в 1С - Оформления бухгалтерской, налоговой отчетности

Контактные телефоны ближайших родственников, друзей	1. Случаи экстренной связи с лицами, проживающими совместно 2. Внесение данных в 1С
Страховое свидетельство государственного пенсионного страхования	1. Отражение данной информации в кадровых документах 2. Внесение данных в 1С 3. Оформления бухгалтерской, налоговой отчетности
Свидетельство о присвоении индивидуального налогового номера	1. Отражение данной информации в кадровых документах 2. Внесение данных в 1С 3. Оформления бухгалтерской, налоговой отчетности
Данные о воинской службе	1. Отражение данной информации в кадровых документах 2. Внесение данных в 1С 3. Ведение воинского учета на предприятии
Паспортные данные или данные другого документа удостоверяющего личность	1. Отражение данной информации в кадровых документах 2. Оформления бухгалтерской, налоговой отчетности 3. Внесение данных в 1С 4. Оформления доверенности
Сведения о заработной плате, доходах с прежних мест работы	1. Для произведения необходимых вычетов из заработной платы, установленных законодательством.
Документы, подтверждающие степень родства	1. Отражение данной информации в кадровых документах 2. Предоставление льгот и гарантий согласно действующему законодательству (например, предоставление отпусков без сохранения заработной платы) и других 3. Предоставление льгот и гарантий, предусмотренных локальными нормативными актами ООО «СУЭС»
Фотография, изображение, полученное при помощи видеофиксации,	1. Внесение данных в 1с (для пропускной системы)

Кому, и с какой целью	Персональные данные
Банку АО «Агропромкредит», для оформления безналичного счета, на который будет перечисляться заработная плата, доходах	Фамилия, имя, отчество Гражданство Дата, месяц, год рождения Место рождения Паспортные данные Адрес прописки Адрес фактического проживания Контактный телефон Электронная почта ИНН СНИЛС Сведения о начислениях заработной платы, других доходов
Страховой компании (ООО «АльфаСтрахование»), для оформления полиса добровольного медицинского страхования	Фамилия, имя, отчество Дата, месяц, год рождения Паспортные данные Адрес проживания Семейное положение, ФИО и дата рождения родственников (при оформлении ДМС родственникам)
Типографии – для оформления открыток, наград	Фамилия, имя, отчество Юбилейная дата Должность Подразделение

Медицинское учреждение, для прохождения предварительного, периодического медицинских осмотров	Фамилия, имя, отчество Дата, месяц, год рождения СНИЛС Адрес прописки Должность
Сторонние компании ООО «Корпорация СТС», ООО «СУСХ» ПАО «СУЭНКО» АО «ЭК «Восток», для участия в корпоративных спортивных соревнованиях, награждении в связи с профессиональными праздниками	Фамилия, имя, отчество Подразделение Должность
Сторонние организации, для организации спортивных или профессиональных соревнований	Фамилия, имя, отчество Дата, месяц, год рождения Должность Подразделение Трудовая деятельность Стаж работы
Сторонние организации (Администрация города, Правительство области, Областная дума, Министерство Энергетики, ЖКХ) для оформления внешних наград к профессиональным праздникам	Фамилия, имя, отчество Дата, месяц, год рождения Должность Подразделение Образование Трудовая деятельность Стаж работы Имеющиеся награды Паспортные данные Адрес прописки Адрес фактического проживания ИНН СНИЛС Контактный телефон
Военные комиссариаты Тюменской и Курганской Области	Фамилия, имя, отчество Дата, месяц, год рождения Должность Подразделение Образование Трудовая деятельность Стаж работы Имеющиеся награды Паспортные данные Адрес прописки Адрес фактического проживания ИНН СНИЛС Контактный телефон

Даю согласие на получение, обработку и передачу расчетных листов, реестров, платежных поручений, а также любой информации, касающейся сведений о моих доходах в ООО «СУЭС», следующим должностным лицам:

- генеральному директору;
- заместителю генерального директора по экономике и финансам;
- главному бухгалтеру;
- заместителю главного бухгалтера;
- начальнику сектора по начислению заработной платы;
- бухгалтеру по расчетам с персоналом;
- начальнику службы управления персоналом;
- экономисту по труду и заработной плате;
- руководителю структурного подразделения, в подчинение которого я трудоустроен(а).

в течение:

1. периода действия трудового договора;
2. архивного срока хранения документов, в которых содержатся мои персональные данные – 75 лет;
3. в информационной системе после даты моего увольнения.

Мне известно, что настоящее согласие может быть отозвано мной путем направления письменного уведомления (отзыва) Оператору а также то, что в случае отзыва согласия Оператор вправе продолжить обработку моих персональных данных без моего согласия при наличии предусмотренных действующим законодательством оснований.

(Ф.И.О. Субъекта)

(подпись Субъекта)

« _____ » _____ 20 ____ г.

СОГЛАСИЕ
контрагента на обработку персональных данных
с перечнем лиц, которым данные могут быть переданы

Настоящим я,

_____ (ФИО, адрес, номер основного документа, удостоверяющего личность, сведения о
_____, date выдачи указанного документа и выдавшем его органе)

действую от себя лично/ по доверенности (нужное подчеркнуть)

ЗАПОЛНЯЕТСЯ ПРИ ОБРАЩЕНИИ ПО ДОВЕРЕННОСТИ
на основании доверенности
(реквизиты доверенности или иного документа, подтверждающего полномочия
_____, представителя (при получении согласия от представителя субъекта
персональных данных)
от имени

(ФИО, адрес, номер основного документа, удостоверяющего личность Субъекта персональных данных -
_____, представляемого, сведения о date выдачи указанного документа и
выдавшем его органе)

даю ООО «СУЭС» (далее – Оператор) согласие на обработку моих персональных данных на следующих условиях.

Цели обработки персональных данных:

-организация договорных отношений, в том числе исполнение обязанностей и реализация прав, предоставленных в рамках договоров (соглашений) между Оператором и мной,
-исполнение иных обязанностей, налагаемых на Оператора в соответствии с действующим законодательством, а также реализация иных прав, предоставленных Оператором в соответствии с действующим законодательством.

Перечень персональных данных, на обработку которых дается согласие:

-фамилия, имя, отчество;
-дата (день, месяц, год) и место рождения;
-адрес места жительства (по регистрации и фактический) и дата (день, месяц, год) регистрации по месту жительства или по месту пребывания, дата (день, месяц, год) снятия с регистрационного учета;
-сведениям о постановке на учет в качестве налогоплательщика;
-данные СНИЛС;
-сведения о регистрации в качестве индивидуального предпринимателя;
-сведения о заключенных договорах и иных имущественных сделках с моим участием, о которых стало известно Оператору;

- сведения, необходимые для исполнения Оператором обязательств по договору, заключенному со мной в том числе, но не ограничиваясь:
- контактная информация: почтовый адрес, номер телефона, электронный адрес, указанный мной в качестве контактной информации;
- паспортные данные или данные иного документа, удостоверяющего личность (серия и номер, дата (день, месяц, год) выдачи, наименование органа, выдавшего документ) и гражданство;
- сведения об объеме и стоимости оказываемой в рамках договора услуги;
- сведения о задолженности мной за оказанные услуги, об оплате.

Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ без распространения), обезличивание, блокирование, удаление, уничтожение с использованием средств автоматизации или без использования таких средств без трансграничной передачи.

Я предоставляю право Оператору поручить обработку персональных данных на вышеуказанных условиях третьим лицам (включая структурные подразделения указанных организаций): организациям, обеспечивающим доставку документов в рамках исполнения договора (ФГУП «Почта России», иные курьерские или почтовые компании).

Также передача персональных данных может осуществляться Оператором организациям связи, банкам, кредитным организациям, лицам, осуществляющим деятельность по приему платежей физических лиц (платежным агентам) на основании договоров (соглашений), органам государственной власти, органам местного самоуправления, судебным и правоохранительным органам в соответствии с законодательством РФ.

Срок, в течение которого действует согласие определяется (за исключением случаев, предусмотренных законодательством РФ) до истечения срока исковой давности (течение срока исковой давности определяется в соответствии с нормами действующего законодательства); до даты получения Оператором отзыва согласия субъекта персональных данных на обработку его персональных данных; до ликвидации или иного прекращения (ограничения) правоспособности Оператора; либо при наступлении обстоятельств, при которых обработка персональных данных должна быть прекращена, в соответствии с требованиями законодательства РФ.

Мне известно, что настоящее согласие может быть отозвано мной путем направления письменного уведомления (отзыва) Оператору а также то, что в случае отзыва согласия Оператор вправе продолжить обработку моих персональных данных без моего согласия при наличии предусмотренных действующим законодательством оснований.

Контрагент

подпись

« _____ » 20 ____ г.

Приложение №3
к Положению о защите персональных данных ООО «СУЭС»

Руководителю ООО
«СУЭС» (Оператору)

от _____

ФИО, должность

СОГЛАСИЕ
на передачу персональных данных третьей стороне

Я, _____

даю согласие на предоставление в _____

_____ (указать организацию)

следующих моих персональных данных:

- дата приема на работу;
- должность, по которой я выполняю трудовые обязанности в ООО «СУЭС»;

Настоящее согласие действительно в течение одного месяца с момента его получения.

(фамилия, инициалы)

(подпись)

« _____ » _____ 20__ г.

**Обязательство о неразглашении конфиденциальной
информации (персональных данных)**

Я, _____
(ФИО)
исполняющий (ая) должностные обязанности по занимаемой должности

(должность, наименование структурного подразделения)

предупрежден (а), что на период исполнения должностных обязанностей в соответствии с должностным регламентом, мне будет предоставлен допуск к конфиденциальной информации (персональным данным). Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному начальнику.

4. Не использовать конфиденциальные сведения с целью получения выгоды.

5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.

6. После прекращения права на допуск к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

(фамилия, инициалы)

(подпись)

« _____ » _____ 20 __ г.

ОТЗЫВ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Тюмень

«_____» _____ 20 г.

Субъект персональных данных,

Я,

(Фамилия, Имя, Отчество полностью)

отзываю у Оператора

Общества с ограниченной ответственностью «Сибирско-Уральский энергетический сервис»

свое согласие о намерении осуществлять обработку персональных данных, обновление, изменение, использования, распространение, обезличивание, в том числе передача и разглашение персональных данных, в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

Настоящий отзыв согласия действует через 2 недели с момента передачи документа в службу управления персоналом.

Подпись субъекта персональных данных:

(Ф.И.О. полностью, подпись)

ЛИСТ СОГЛАСОВАНИЯ
Положение о защите персональных данных в
ООО «Сибирско-Уральский энергетический сервис»
(наименование документа)

Разработчик:

Начальник службы
управления персоналом



Е.В. Фомина
«25» 07 2018 г.

СОГЛАСОВАНО:

Начальник юридического отдела



А.С. Рыбьякова
«25» 07 2018 г.

Начальник службы экономической безопасности



А.В. Сапин
«25» 07 2018 г.

**ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«Сибирско-Уральский энергетический сервис»
(ООО «СУЭС»)**

ПРИКАЗ

«15» июль 2018 г.

г. Тюмень

№ 10-02

О введении в действие Положения о защите персональных данных в
ООО «Сибирско-Уральский энергетический сервис»

В целях закрепления механизмов обеспечения защиты прав работников, контрагентов и кандидатов Общества при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну,

ПРИКАЗЫВАЮ:

1. Ввести в действие с 25.07.2018г. утвержденное Положение о защите персональных данных в ООО «Сибирско-Уральский энергетический сервис».
2. Службе управления персоналом ознакомить всех начальников структурных подразделений с настоящим Положением под роспись.
3. Начальникам всех структурных подразделений ознакомить подчиненный персонал с настоящим Положением под роспись. Оригиналы листов ознакомлений сдать в службу управления персоналом.
4. Действие Положения «О работе с персональными данными» ООО «Кургансетсервис» в прежней редакции считать утратившим силу с 25.07.2018г.
5. Контроль за исполнением настоящего приказа возложить на Е.В. Фомину, начальника службы управления персоналом.

Генеральный директор



А.В. Худяков