УТВЕРЖДАЮ:

Директор ООО «Хакасия.ру»

_____ К.С. Пахомов

«27» сентября 2019 г.

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ, КЛИЕНТОВ И КОНТРАГЕНТОВ

г. Абакан, 2019г.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Для целей настоящего Положения ООО «Хакасия.ру» (далее – Общество) является Оператором.

Персональные данные, обрабатываемые в Обществе - персональные данные работников Общества, предоставленные ими в связи с трудовыми отношениями, персональные данные клиентов Общества, персональные данные контрагентов Общества, необходимые при заключении гражданско-правовых договоров с физическими лицами, персональные данные представителей контрагентов – юридических лиц, предоставленные Обществу в порядке, предусмотренном законодательством и необходимые для реализации заключенных между Обществом и контрагентом гражданско-правовых договоров, иные персональные данные, предоставленные Обществу в порядке, предусмотренном законодательством.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Субъект персональных данных – Работник, Клиент, Контрагент.

Защита персональных данных Работника, Клиента, Контрагента – деятельность Общества по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации.

Конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Распространение персональных данных - действия, направленные на передачу персональных данных работников определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным работников каким-либо иным способом.

Использование персональных данных - действия (операции) с персональными данными, совершаемые должностным лицом Организации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных работников, в том числе их передачи.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику;

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Информация - сведения (сообщения, данные) независимо от формы их представления.

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Средства вычислительной техники (СВТ) – совокупность программных и технических элементов систем обработки персональных данных, способных функционировать самостоятельно или в составе других систем

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлениями Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными актами, действующими на территории Российской Федерации.

2.2. Цель разработки Положения.

2.2.1. Определение порядка обработки в ООО «Хакасия.ру» персональных данных его работников, клиентов, представителей контрагентов и контрагентов (физических лиц), персональные данные которых подлежат обработке, на основании полномочий оператора;

2.2.2. Обеспечение защиты прав и свобод человека и гражданина, в т.ч. работника Общества, при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

2.2.3. Установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2.3. Цели обработки персональных данных Субъектов.

2.3.1. Установления договорных отношений с Субъектом персональных данных путем заключения договора, одной из сторон которого, либо выгодоприобретателем по которому является Субъект персональных данных;

2.3.2. Исполнения договора между Обществом и Субъектом персональных данных;

2.3.3. Выполнения требований:

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

- законодательства о воинской обязанности и военной службе при постановке работников на воинский учет и бронировании граждан, пребывающих в запасе;

- 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, учитываемых при начислении страховых взносов на добровольное и обязательное пенсионное страхование и обеспечение;

- заполнения первичной статистической документации в соответствии с Постановлением Госкомстата России от 05.01.2004 года № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты».

2.3.4. Проведения маркетинговых исследований;

2.3.5. Статистической обработки информации, при условии обязательного обезличивания персональных данных Субъектов.

2.4. Принципы обработки персональных данных.

2.4.1. Осуществление обработки персональных данных на законной и справедливой основе;

2.4.2. Ограничение обработки персональных данных достижением конкретных, заранее определенных и законных целей;

2.4.3. Соответствие содержания и объема обрабатываемых персональных данных заявленным целям их обработки, отсутствие избыточности обрабатываемых персональных данных по отношению к целям их обработки;

2.4.4. Недопустимость объединения баз данных, содержащих персональные данные, обработка которых осуществляется в несовместимых между собой целях;

2.4.5. Обеспечение точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных;

2.4.6. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

2.5. Основания обработки персональных данных.

2.5.1. Обработка персональных данных Обществом осуществляется в следующих случаях:

- с согласия субъекта персональных данных на обработку его персональных данных;

- для исполнения договора, стороной которого, либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

- для осуществления прав и законных интересов Общества или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- при необходимости осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- в случае, если такая обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- в случае, когда доступ неограниченного круга лиц к персональным данным субъекта предоставлен самим субъектом персональных данных, либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных);

- в случае, когда персональные данные подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом;

- в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных.

2.5.2. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, судимости, а также биометрических персональных данных Обществом не осуществляется. Обработка указанных данных возможна Обществом только на основании согласия субъекта персональных данных в письменной форме.

2.5.3. Персональные данные могут быть получены не от субъекта персональных данных (от третьего лица или из другого источника). При этом, до начала обработки персональных данных, субъекту направляется уведомление об обработке его персональных данных за исключением следующих случаев:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных оператором;

- персональные данные получены Обществом на основании федерального законодательства или в связи с исполнением договора, стороной которого, либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;

- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

- когда предоставление субъекту персональных данных содержащихся в уведомлении сведений нарушает права и законные интересы третьих лиц.

2.6. Конфиденциальность персональных данных.

2.6.1. Персональные данные Субъектов относятся к категории конфиденциальной информации. Сбор, хранение, использование и распространение информации о частной жизни Работника без письменного его согласия не допускается;

2.6.2. Документы, содержащие информацию о персональных данных Субъектов, являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставится.

2.6.3. Общество при осуществлении своей деятельности может передавать персональные данные Субъектов государственным органам (Федеральной налоговой службе, Федеральной службе судебных приставов, Министерству внутренних дел Российской Федерации, Прокуратуре и др.) в рамках осуществления последними своих полномочий и функций **по их письменному запросу**, а также контрагентам Общества (банкам, страховым компаниям, и др.) в строгом соответствии с требованиями законодательства Российской Федерации и при надлежащем обеспечении безопасности этих данных.

2.6.4. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75-летнего срока хранения, если иное не определено законом;

2.7. Порядок ввода в действие и изменения Положения.

2.7.1. Настоящее Положение вступает в силу с момента его утверждения директором Общества и действует бессрочно, до замены его новым Положением.

2.7.2. Все изменения в Положение вносятся приказом директора Общества.

2.8. Действие настоящего Положения распространяется на всех работников Общества (временных и постоянных), а также работников сторонних организаций,

связанных договорными отношениями с Обществом и тем или иным образом участвующих в бизнес-процессах Общества, подразумевающих обработку персональных данных.

2.9. Все работники Общества должны быть ознакомлены с настоящим Положением под роспись в листе ознакомления, являющимся неотъемлемой частью настоящего Положения по защите персональных данных работников. Подпись работника ООО «Хакасия.ру» в листе ознакомления с Положением означает его согласие и обязательство исполнения.

3. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ

3.1. Персональные данные работников Общества.

3.1.1. В состав персональных данных работников Общества входит информация о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность. К ней относятся:

- общие сведения (фамилия, имя, отчество, дата рождения, место рождения, гражданство, учебные заведения, в которых Работник учился и периоды обучения, квалификация, профессия, предыдущие места работы/службы, с указанием периодов работы/службы и должностей, состояние в браке, наличие детей и их возраст, паспортные данные);
- сведения о воинском учете;
- данные о приеме на работу;
- сведения о присвоении ИНН;
- налоговый статус (резидент/нерезидент);
- сведения о заработной плате работника;
- сведения о социальных гарантиях;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения о месте жительства (по паспорту и фактически) и о контактных телефонах;
- сведения о месте работы или учебы членов семьи и родственников;
- биометрические персональные данные (фотографии);
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- иная, не указанная выше информация, содержащаяся в личных делах и трудовых книжках сотрудников;
- информация, являющаяся основанием к приказам по личному составу;
- информация, содержащаяся в страховом свидетельстве обязательного пенсионного страхования, свидетельстве о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации, страховом медицинском полисе обязательного медицинского страхования граждан, медицинском заключении установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на работу в Общество;
- деловые и иные личные качества, которые носят оценочный характер;
- прочие сведения, которые могут идентифицировать человека (субъекта персональных данных).

3.1.2. К документам, содержащим персональные данные работников Общества, относятся:

- паспорт или иной документ, удостоверяющий личность;
- анкета, автобиография, личный листок по учету кадров, которые заполняются работником при приеме на работу;
- личная карточка работника (форма № Т-2);

- личные дела и трудовые книжки работников;

- справочно-информационные данные по персоналу (картотеки, журналы);

- документы о прохождении обучения, повышению квалификации и переподготовке, стажировки, испытательного срока, аттестации работников;

- документы, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;

- материалы по анкетированию, проведению собеседований с кандидатом на должность;

- документы, связанные с привлечением работника к дисциплинарной ответственности (служебные записки, докладные, объяснительные и прочие);

- документы о составе семьи работника, необходимые для предоставления ему гарантий, связанных с выполнением семейных обязанностей;

- документы о состоянии здоровья детей и других близких родственников, когда с наличием таких документов связано предоставление работнику каких либо гарантий и компенсаций;

- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством РФ;

- документы о беременности работника и возрасте детей для предоставления матери (отцу, другим родственникам) установленных законом условий труда, гарантий и компенсаций;

- лицевой счет и наименование банка, на который перечисляется заработная плата;

- страховое свидетельство государственного пенсионного страхования (СНИЛС);

- свидетельство о присвоении ИНН (при его наличии у работника).

- документы воинского учета - для военнообязанных и лиц, подлежащих воинскому учету;

- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

- справка о том, является или не является лицо подвергнутым административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ;

- дополнительные документы (справка о доходах с предыдущего места работы, справка из органов государственной налоговой службы о предоставлении сведений об имущественном положении, медицинское заключение о состоянии здоровья и др.);

- трудовой договоры и дополнительные соглашения к ним;

- подлинники и копии приказов по личному составу;

- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения;

- реестры сведений о начисленных и уплаченных страховых взносах на обязательное пенсионное страхование и страховом стаже застрахованных лиц;

- реестры на оплату пенсионных взносов, удержанных из заработной платы согласно заявлению и заключенным личным договорам негосударственного пенсионного обеспечения;

- расчеты по начисленным и уплаченным страховым взносам на добровольное и обязательное медицинское и социальное страхование на случай временной нетрудоспособности и в связи с материнством и по обязательному социальному страхованию от несчастных случаев на производстве и профессиональных заболеваний, а также по расходам на выплату страхового обеспечения;

- ведомости на перечисление заработной платы;

- фотографическое изображение работника в личном листке по учёту кадров;

- при необходимости - иные документы, содержащие персональные данные работника.

3.1.4. Персональные данные кандидатов на заключение трудового договора с Обществом, а также персональные данные лиц, связанных с работниками Общества, полученные в порядке, предусмотренном действующим законодательством, обрабатываются Оператором наравне с персональными данными работников Общества.

3.2. Персональные данные клиентов Общества.

- фамилия, имя и (если иное не вытекает из закона или национального обычая) отчество;
- дата и место рождения;
- гражданство;
- реквизиты документа, удостоверяющего личность: серия и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (если имеется);
- адрес регистрации и фактического места жительства;
- идентификационный номер налогоплательщика (если имеется);
- место работы;
- образование, профессия, специальность, занимаемая должность;
- номера контактных телефонов и факсов (если имеются).
- адрес электронной почты;
- номер пенсионного удостоверения;

3.2.2. Документы, содержащие персональные данные клиента:

- копия документов удостоверяющих личность субъекта персональных данных;
- анкета клиента;
- свидетельство о присвоении ИНН;
- доверенности, подтверждающие полномочия представителя клиента, и оформленные в соответствии с требованиями законодательства РФ;
- договоры заключаемые с клиентом, а также изменения и дополнения к этим договорам;
- приказы по основной деятельности;
- переписка с клиентом;
- служебные записки;
- приказы о допуске представителей клиента, контрагента;
- документы, касающиеся претензионно-исковой работы с должником клиентом;
- иные документы, касающиеся правоотношений между клиентом и Обществом, где включение персональных данных клиента необходимо согласно действующему законодательству.

3.3. Персональные данные Контрагента Общества:

- фамилия, имя и (если иное не вытекает из закона или национального обычая) отчество;
- дата и место рождения;
- гражданство;
- реквизиты документа, удостоверяющего личность: серия и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (если имеется);
- адрес регистрации и фактического места жительства; - идентификационный номер налогоплательщика (если имеется);
- место работы;
- образование, профессия, специальность, занимаемая должность;
- номера контактных телефонов и факсов (если имеются).
- адрес электронной почты;
- номер пенсионного удостоверения;

3.3.2. Документы, содержащие персональные данные контрагента:

- копия документов удостоверяющих личность субъекта персональных данных;

- анкета контрагента;
- свидетельство о присвоении ИНН;
- доверенности, подтверждающие полномочия представителя контрагента, и оформленные в соответствии с требованиями законодательства РФ;
- договоры заключаемые с контрагентом, а также изменения и дополнения к этим договорам;
- приказы по основной деятельности;
- переписка с контрагентом;
- служебные записки;
- приказы о допуске представителей клиента, контрагента;
- разовые или временные пропуска;
- документы, касающиеся претензионно-исковой работы с должником-контрагентом;
- иные документы, касающиеся правоотношений между контрагентом и Обществом, где включение персональных данных контрагента необходимо согласно действующему законодательству.

4. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В целях обеспечения прав и свобод человека и гражданина Общество и (или) его представители при обработке персональных данных должны соблюдаться следующие общие требования:

4.1.1. Обработка персональных данных должна осуществляться на законной и справедливой основе, исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия выполнения договорных обязательств в соответствии с законодательством РФ;

4.1.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.1.3. Получение Обществом персональных данных может осуществляться как путем представления их самим работником, клиентом, контрагентом так и путем получения их из иных источников.

4.1.4. Персональные данные получаются Обществом непосредственно у самого работника, клиента, контрагента. Если персональные данные работника возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Общество должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

4.1.5. Общество не имеет права получать и обрабатывать персональные данные работника, клиента, контрагента о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни работника, клиента, контрагента (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны Обществом только с его письменного согласия.

4.1.6. Общество не имеет право получать и обрабатывать персональные данные работника, клиента, контрагента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

4.2. Использование персональных данных возможно только в соответствии с целями, определившими их получение. Персональные данные не могут быть использованы в целях

причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено действующим законодательством Российской Федерации.

4.3. При принятии решений, затрагивающих интересы клиента или контрагента, Оператор не имеет права основываться на персональных данных клиента или контрагента, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.

4.4. При идентификации клиента или контрагента Общество может затребовать предъявления документов, удостоверяющих личность и подтверждающих полномочия представителя.

4.5. Обработка персональных данных клиентов, контрагентов - физических лиц (в том числе являющихся индивидуальными предпринимателями), с которыми непосредственно у организации заключены договоры, может осуществляться без согласия на обработку персональных данных и без уведомления уполномоченного органа при условии, что эти данные не будут распространяться и предоставляться третьим лицам без согласия субъекта персональных данных и будут обрабатываться только в целях заключения с ними соответствующих договоров. Если же Оператор намерен осуществлять обработку персональных данных в иных случаях, не связанных с исполнением договора, то он обязан получить согласие на обработку персональных данных.

4.6. Передача персональных данных возможна только с согласия работника, клиента, контрагента или в случаях, прямо предусмотренных законодательством Российской Федерации.

4.7. При передаче персональных данных Общество должно соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия работника, клиента, контрагента за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, клиента, контрагента, а также в случаях установленных законодательством Российской Федерации;

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

- предупредить лиц, получающих персональные данные, 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 персональные данные, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными в порядке, установленном законодательством Российской Федерации;

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

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4.8. Передача персональных данных от Общества и (или) его представителей третьей стороне может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

4.9. При передаче персональных данных третьей стороне (в том числе и в коммерческих целях) Общество не должно сообщать эти данные третьей стороне без письменного согласия работника, клиента, контрагента за исключением случаев, установленных законодательством Российской Федерации.

4.10. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

4.11. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

4.12. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

4.13. Период хранения и обработки персональных данных определяется в соответствии с Законом «О персональных данных». Обработка персональных данных начинается с момента поступления персональных данных в информационные системы персональных данных и прекращается:

- в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, Общество устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений, Общество в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных Общество уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Общество уведомляет также указанный орган;

- в случае достижения цели обработки персональных данных Общество незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, и уведомляет об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Общество уведомляет также указанный орган;

- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Общество прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных Общество уведомляет субъекта персональных данных.

- в случае прекращения деятельности Общества.

4.14. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.15. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

4.16. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

4.17. Особый порядок сбора и обработки персональных данных Субъектов, поступающих на любой электронный адрес Общества, в целях возможного дальнейшего трудоустройства.

4.17.1. Субъект самостоятельно принимает решение о предоставлении своих персональных данных и предоставляет согласие на обработку таких персональных данных свободно, своей волей и в своем интересе. Согласие на обработку персональных данных может быть дано Субъектом путем направления персональных данных на любой электронный адрес Общества.

4.17.2. Резюме соискателя, который его прислал на электронный адрес Общества, хранению не подлежит. Соискателю, компетенции которого подходят под требования вакантной должности, направляется форма анкеты кандидата и форма согласия на обработку персональных данных; соискатель приглашается на собеседование.

4.17.3. Резюме, размещенные на публичных сайтах по поиску работы, обрабатываются без сохранения на рабочий компьютер.

4.18. Обработка персональных данных с использованием средств автоматизации.

4.18.1. Правила доступа, хранения, пересылки и уничтожения персональных данных.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

Программное обеспечение на СВТ Общества, предназначенные для обработки персональных данных, устанавливается исключительно специалистами Отдела информационных технологий.

Вход в информационную систему учёта персональных данных работников Общества выполняется с учётом правил разграничения доступа.

Каждому работнику Общества, допущенному к обработке персональных данных, должны соответствовать следующие реквизиты: имя пользователя, персональный пароль и уровень доступа в соответствии с исполняемыми должностными обязанностями, допуск лиц к обработке персональных данных в информационной системе без соответствующих разрешительных документов и ключей (паролей) доступа запрещается.

Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и(или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

При изъятии АРМ (сервера), обрабатывающего персональные данные, из состава рабочих станций (серверов) структурного подразделения ее передача на склад, в ремонт или в другое структурное подразделение для решения иных задач осуществляется только после того, как системного администратора отдела информационных технологий Общества

снимет с данной рабочей станции (сервера) средства защиты от несанкционированного доступа и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Уничтожение данных на жёстком диске компьютера осуществляется комиссионно. Факт уничтожения данных оформляется Актом о затирании остаточной информации, хранившейся на диске компьютера.

4.18.2. Общие требования по защите персональных данных в автоматизированных системах.

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

б) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

а) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

б) учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

д) описание системы защиты персональных данных.

4.18.3. Общие требования к пользователю.

Пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ.

Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

Обязанности пользователя:

- выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;

- при работе с персональными данными не допускать присутствии в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами;

- соблюдать правила работы со средствами защиты информации и установленный режим разграничении доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;

- оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальник о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;

- не допускать «загрязнения» ПЭВМ посторонними программными средствами;

- обращаться к системному администратору (представителю УК ООО « ГК «Хакасия.ру») в случае обнаружения неисправностей в ПЭВМ;

- помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;

- при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

4.18.4. Пользователю ПЭВМ запрещается:

- записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;

- осуществлять несанкционированное копирование обрабатываемых Оператором персональных данных, в том числе с использованием отчуждаемых (сменных) носителей информации, мобильных устройств копирования и переноса информации, запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов), а также устройств фото и видеосъемки;

- самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;

- самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

- использовать внешние электронные почтовые ящики, не входящие в домен @khakasia.ru для приёма или передачи любых сведений и документов Общества, содержащих персональные данные;

- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;

- объединять созданные для несовместимых между собой целей обработки баз данных информационных систем персональных данных;

- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

- разглашать информацию о системе обеспечения безопасности информации Общества и её компонентах (в том числе о применяемых программных и программно-аппаратных комплексах);

- передавать кому-либо или оставлять без контроля на рабочем месте личный пароль к ПЭВМ и информационным ресурсам Общества, полученный для работы;

- вскрывать корпуса (разбирать) ПЭВМ Общества, предназначенных для обработки персональных данных;

- отключать (блокировать) средства защиты информации;

- открывать общий доступ, разрешать изменение системных файлов по сети, использовать для соединения с сетью Интернет модемы мобильных телефонов, средства беспроводных сетей и иные, неразрешённые в Обществе, способы доступа к информационным сетям Общества и Интернет;

- производить какие-либо изменения в подключении и размещении технических средств;

- осуществлять сканирование информационных ресурсов Общества, с целью выявления их топологии;

- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями;

- оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

4.18.5. Пользователь ПЭВМ имеет право:

- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.

- обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

4.18.6. Пользователь ПЭВМ несет ответственность за:

- надлежащее выполнение требований настоящей Инструкции;

- соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;

- сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;

- сохранность персональных данных.

Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

4.18.7. Проведение мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных

Мониторинг аппаратного обеспечения.

Мониторинг работоспособности аппаратных компонент автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

Мониторинг парольной защиты.

Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- установление сроков действия паролей (не более 3 месяцев);
- периодическую (не реже 1 раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

Мониторинг целостности.

Мониторинг целостности программного обеспечения включает следующие действия:

- проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- обнаружение дубликатов идентификаторов пользователей;
- восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

Мониторинг попыток несанкционированного доступа.

Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;
- выявление фактов сканирования определенного диапазона сетевых портов, в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

Мониторинг производительности.

Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, производится по обращениям пользователей, в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

Системный аудит.

Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, тому уровню безопасности, удовлетворяющему требованиям политики безопасности. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующим специально составленному списку для проверки.

Обзоры безопасности должны включать:

- отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;
- проверку содержимого файлов конфигурации на соответствие списку для проверки;
- обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);

- проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;

- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т.е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то, с целью нейтрализации уязвимостей, необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствующем журнале; уведомлением каждого сотрудника, кого касается изменение; выслушиванием претензий в случае, если это изменение причинило кому-нибудь вред; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

Антивирусный контроль.

Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;

- утилиты для обнаружения и анализа новых вирусов.

К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

При подозрении на наличие невыявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает

неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т.п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;
- проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

Необходимо организовать регулярное обновление антивирусных баз на всех рабочих станциях и серверах.

Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которые распространяются вирусы. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т.д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

Анализ инцидентов.

Если администратор системы, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

- факт попытки несанкционированного доступа (НСД);
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- когда происходила попытка НСД;
- как и при каких обстоятельствах была предпринята попытка НСД;

- точка входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД.

Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к их области деятельности.

При анализе системных журналов администратору необходимо произвести следующие действия:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;
- выявить наличие неудачных попыток входа в систему.

В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки изменения таблиц маршрутизации и адресных таблиц;
- проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- проверить целостность системных программ;
- проверить систему аутентификации и авторизации.

В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.

4.19. Обработка персональных данных без использованием средств автоматизации.

Условия хранения персональных данных.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающее одновременное копирование иных персональных данных, не подлежащих распространению и использованию).

Использование типовых форм документов и журналов учета

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

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

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

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

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

Порядок уничтожения или обезличивания персональных данных.

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, вымарывание).

5. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

5.1. Право доступа к персональным данным работников имеют:
- директор Общества;
- сотрудники службы персонала;
- сотрудники финансовой службы;
- главный бухгалтер;
- юрисконсульт;
- системный администратор;
- руководители структурных подразделений по направлению деятельности (доступ к персональным данным только работников своего подразделения);
- прочие работники организации, которым в силу выполнения своих трудовых обязанностей, необходим доступ к персональным данным;
- субъект персональных данных – только свои данные.

5.2. Работники Общества выполняют действия по обработке персональных данных в соответствии с возложенными на работников функциями.

5.3. Доступ к персональным данным предоставляется только лицам, замещающим должности, указанных в п. 5.1.

5.4. Работники имеют доступ на ввод и коррекцию персональных данных в пределах, определенных должностными обязанностями.

5.5. Лица, получившие доступ к персональным данным, должны хранить в тайне известные им сведения конфиденциального характера и информировать ответственное лицо за организацию обработки персональных данных об утечке персональных данных, о фактах нарушения порядка обращения с ними, о попытках несанкционированного доступа к персональным данным.

5.6. Лица, получившие доступ к персональным данным, должны использовать эти данные лишь в целях, для которых они сообщены, обязаны соблюдать режим конфиденциальности.

5.7. Доступ Субъектов к персональным данным.

5.7.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, объем и содержание которой указаны в ч. 7 ст. 14 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ.

5.7.2. В соответствии с ч. 1 ст. 20 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ Общество обязано сообщить Субъекту или его представителю информацию о наличии персональных данных, относящихся к соответствующему Субъекту, а также предоставить возможность ознакомления с этими персональными данными в течение тридцати дней с момента получения запроса Субъекта или его представителя.

Согласно ст. 62 Трудового кодекса Российской Федерации, Работникам предоставляется возможность ознакомления со своими персональными данными в течение трех рабочих дней с момента получения письменного запроса Работника.

5.7.3. Право Субъекта на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ.

5.7.4. Выбор формы обращения (запроса) для реализации своего права на получение сведений зависит от воли Субъекта. Информация, касающаяся обработки персональных данных Субъекта, может быть предоставлена субъекту персональных данных или его представителю для ознакомления в случае:

- устного обращения к Работникам Общества, сопровождающегося обязательным предоставлением основного документа, удостоверяющего личность Субъекта или его представителя, а также документа, подтверждающего полномочия этого представителя;

- предоставления запроса в Общество, который может быть исполнен как на бумажном носителе (при личном обращении субъекта или его представителя), так и в форме электронного документа, подписанного электронной подписью в соответствии с законодательством РФ. Запрос должен содержать: номер основного документа, удостоверяющего личность клиента или его представителя; сведения о дате выдачи указанного документа и выдавшем его органе; сведения, подтверждающие участие Субъекта в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом свидетельствующие об обработке персональных данных Обществом; подпись Субъекта или его представителя.

5.7.5. Для реализации своего права на получение информации, касающейся обработки его персональных данных, Субъект, в случае оформления им письменного запроса, должен подписать и передать его лично или через своего представителя в Общество по месту нахождения Общества.

5.7.6. В случае получения запроса от представителя Субъекта полномочия данного представителя на подачу запроса от имени Субъекта должны проверяться при приеме запроса.

5.7.7. В случае отказа в предоставлении информации, касающейся персональных данных о соответствующем Субъекте, Общество обязано дать заявителю в письменной форме мотивированный ответ, содержащий ссылку на положение ч. 8 ст. 14 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 дней со дня обращения Субъекта или его представителя, либо с момента получения запроса Субъекта или его представителя.

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Защита персональных данных от неправомерного их использования или утраты обеспечивается Оператором в порядке, установленном законодательством РФ.

6.2. Для обеспечения безопасности персональных данных, обрабатываемых в информационных системах Общества, применяются организационные, технические, программные и криптографические методы и средства защиты информации.

6.3. Работники, клиенты или контрагенты до предоставления своих персональных данных должны иметь возможность ознакомиться с настоящим Положением.

6.4. Защите подлежит:

- информация о персональных данных субъекта;
- документы, содержащие персональные данные субъекта;
- персональные данные, содержащиеся на электронных носителях.

6.5. В соответствии с требованиями ст. 22.1 Федерального закона «О персональных данных» от 27.07.2006 г. № 152-ФЗ приказом директора Общества назначается лицо, ответственное за организацию обработки персональных данных, как в информационных системах Общества, в которых обрабатываются персональные данные, так и при обработке персональных данных без использования средств автоматизации.

6.6. Оператор издает документы, определяющие политику оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

6.7. Оператор принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных» от 27.07.2006 года № 152-ФЗ в том числе:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

6.8. Оператор осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону «О персональных данных» от 27.07.2006 года №152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

6.9. Оператор осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

6.10. По возможности персональные данные должны быть обезличены.

6.11. Анализ угроз.

Обеспечение безопасности персональных данных, а также разработка и внедрение средств защиты персональных данных основывается на анализе угроз безопасности персональных данных. Общество, при возникновении необходимости разрабатывает и поддерживает Частную модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - Частная модель угроз). Частная модель угроз отражает актуальное состояние защищенности информационных системах персональных данных и актуальные угрозы безопасности персональных данных. Разработка Частной модели угроз осуществляется на основании анализа существующих угроз безопасности и возможности их реализации в обследуемой информационных системах персональных данных.

6.12. Ответственное лицо за организацию обработки персональных данных.

6.12.1. Ответственное лицо за организацию обработки персональных данных получает указания непосредственно от директора Общества и подотчетно ему.

6.12.2. В соответствии с ч. 4 ст. 22.1 Федерального закона «О персональных данных» Ответственное лицо за организацию обработки персональных данных обязано:

- осуществлять внутренний контроль за соблюдением Обществом, как оператором персональных данных, и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников Общества положения законодательства РФ о персональных данных, локальных актов Общества по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов Субъектов или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

6.12.3. На Ответственное лицо за организацию обработки персональных данных возлагается задача по организации выполнения законодательных требований при обработке персональных данных в Обществе.

6.12.4. На время отсутствия Ответственного лица за организацию обработки персональных данных его обязанности исполняет сотрудник, замещающий его по штатному расписанию.

6.12.5. Ответственными за организацию выполнения требований локальных актов Общества по вопросам обработки персональных данных и их защите в структурных подразделениях Общества являются руководители этих подразделений. На время отсутствия этих руководителей ответственными являются лица, штатно замещающие их.

6.12.6. Ответственными лицами за выполнение требований локальных актов Общества по вопросам обработки персональных данных и их защите на своих рабочих местах в рамках определенных соответствующими должностными инструкциями являются лица, уполномоченные в установленном порядке обрабатывать в Обществе персональные данные.

6.12.7. Ответственные лица соответствующих подразделений, хранящих персональные данные на бумажных носителях и машинных носителях информации, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному Постановлением правительства РФ 15 сентября 2008 г. № 687.

6.12.8. Ответственные лица структурных подразделений, обрабатывающие персональные данные в информационных системах персональных данных и машинных носителях информации, обеспечивают защиту в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативными, нормативно – методическими, методическими документами.

6.12.9. Внутренняя защита.

Для защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний; строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны; наличие необходимых условии в

помещении для работы с конфиденциальными документами и базами данных; определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника (сервер организации);

- организация порядка уничтожения информации;

- 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;

- не допускать выдачи личных дел работников на рабочее место непосредственного руководителя. Ознакомление с личными делами производится в кабинете «отдел персонала». Личные дела могут выдаваться на рабочие места только руководителю организации, и в исключительном случае, по письменному разрешению генерального директора ООО «Хакасия.ру», - руководителю структурного подразделения.

Защита персональных данных работника на электронных носителях: все персональные компьютеры (далее ПК), содержащие персональные данные работника, защищены паролями, которые знают работники организации - пользователи данных ПК, допущенные к обработке персональных данных.

Защита персональных данных на бумажных носителях: все документы, содержащие персональные данные работника, хранятся в кабинете отдела персонала, кабинете бухгалтерии с применением специального оборудования (металлические несгораемые шкафы, сейфы).

Ключи от специального оборудования в рабочее время хранятся у менеджера по персоналу и главного бухгалтера без права передачи третьим лицам, на время их отсутствия ключи хранятся у бухгалтера по расчету заработной платы.

6.12.10. Внешняя защита.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности организации, посетители, работники других организационных структур. Посторонние лица не должны знать распределения функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров.

Для защиты персональных данных работников необходимо соблюдать ряд мер:

- технические средства охраны, сигнализации;

- порядок охраны территории, зданий, помещений, транспортных средств;

-требования к защите информации при интервьюировании и собеседованиях, в соответствии с Инструкцией о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.

7. ОБЩИЕ ПРАВИЛА ХРАНЕНИЯ И ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных.

Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», «О порядке рассмотрения обращений граждан Российской Федерации», действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими положением о защите персональных данных и инструкциями по работе со служебными документами, и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

В структурных подразделениях ООО «Хакасия.ру» - финансовой службе, службе персонала, отделе продаж, отделе электронного документооборота, Саяногорском отделении, отделе 1С, клиентском отделе, ИТС, веб-студия - формируются и ведутся перечни конфиденциальных данных с указанием регламентирующих документов, мест хранения и ответственных за хранение и обработку данных по прилагаемой форме (Приложение 1). Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

8. ПРЕКРАЩЕНИЕ ОБРАБОТКИ, УТОЧНЕНИЕ, БЛОКИРОВАНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. В соответствии с Федеральным законом «О персональных данных» в случае выявления неправомерной обработки персональных данных при обращении Субъекта или его представителя либо по запросу Субъекта или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Общество обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому Субъекту с момента такого обращения или получения указанного запроса.

8.2. В соответствии с Федеральным законом «О персональных данных» в случае выявления неточных (неполных, устаревших) персональных данных при обращении Субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Общество обязано осуществить блокирование персональных данных, относящихся к этому Субъекту с момента такого обращения или получения указанного запроса, если блокирование персональных данных не нарушает права и законные интересы Субъекта или третьих лиц.

8.3. Решение о блокировании персональных данных соответствующего Субъекта принимает Ответственное лицо за организацию обработки персональных данных.

8.4. Проверку факта неправомерной обработки персональных данных или неточности обрабатываемых персональных данных инициирует и организует Ответственное лицо за организацию обработки персональных данных. Проверка проводится силами специалистов и руководителей подразделений Общества, в которых обрабатываются персональные данные, относящиеся к соответствующему Субъекту, с

привлечением по необходимости специалистов иных подразделений Общества по распоряжению Ответственного лица за организацию обработки персональных данных. Результаты проведенной проверки незамедлительно докладываются Ответственному лицу за организацию обработки персональных данных способом и в форме, определенными им в распоряжении или иным порядком.

8.5. Если при обращении Субъекта или его представителя будут обнаружены неточные (неполные, устаревшие) персональные данные, которые можно в присутствии обратившегося и с его согласия оперативно откорректировать, то действия, приведенные в п. 7.4. настоящего Положения, допускается не выполнять.

8.6. В соответствии с Федеральным законом «О персональных данных» Общество обязано прекратить обработку персональных данных и уничтожить персональные данные (либо провести обезличивание) в случае:

8.6.1. достижения цели обработки персональных данных;

8.6.2. утраты необходимости в достижении целей обработки персональных данных;

8.6.3. отзыва Субъектом согласия на обработку его персональных данных.

8.7. Уничтожение (либо обезличивание) выполняется в срок, не превышающий 30 дней с момента наступления события, приводящего к необходимости уничтожения (обезличивания), если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект, иным соглашением между Обществом и Субъектом персональных данных, а также если Общество не вправе осуществлять обработку персональных данных без согласия Субъекта на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

8.8. Ответственным за уничтожение персональных данных является уполномоченное лицо, назначаемое приказом директора Общества.

8.9. Уполномоченное лицо является председателем комиссии Общества по уничтожению персональных данных. Назначение комиссии по уничтожению персональных данных производится приказом директора Общества.

8.10. При наступлении любого из событий, повлекших, согласно законодательства РФ, необходимость уничтожения персональных данных, уполномоченное лицо обязано:

- уведомить членов комиссии о работах по уничтожению персональных данных;
- определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);
- установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональных данных, подлежащие уничтожению (и/или материальные носители персональных данных);
- определить технологию (приём, способ) уничтожения персональных данных (и/или материальных носителей персональных данных);
- определить технические (материальные, программные и иные) средства, посредством которых будет произведено уничтожение персональных данных;
- руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных);
- оформить соответствующий Акт об уничтожении персональных данных (и/или материальных носителей персональных данных) и представить Акт об уничтожении персональных данных (и/или материальных носителей персональных данных) на утверждение директору Общества;
- в случае необходимости уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

8.11. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в п. 8.7 настоящего Положения, Общество в соответствии с ч. 6 ст. 21 Федеральным законом «О персональных данных» осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем 6 месяцев, если иной срок не установлен законодательством РФ.

8.12. Факт отсутствия возможности уничтожения персональных данных по различным причинам докладывается Работником, являющимся ответственным за организацию (выполнение) процедуры уничтожения, Ответственному лицу за организацию обработки персональных данных, который на основании полученного доклада принимает решение об обеспечении уничтожения персональных данных в срок не более чем 6 месяцев или иной срок, установленный федеральными законами. Решение оформляется распорядительным порядком.

8.13. В соответствии с ч. 3 ст. 20 и ч. 3 ст. 21 Федерального закона «О персональных данных» об устранении допущенных нарушений, в результате которых персональные данные были неполными, неточными или неактуальными и подлежали изменению, или об уничтожении персональных данных (в случае неправомерной обработки персональных данных, т е. когда они являются незаконно полученными или не являются необходимыми для заявленной цели обработки), Общество обязано уведомить Субъекта или его представителя.

8.14. Общество также обязано принять разумные меры для уведомления третьих лиц, которым были переданы персональные данные Субъекта в случае, когда с целью устранения допущенных нарушений было необходимо обеспечить изменение переданных персональных данных ввиду их неполноты, неточности или неактуальности.

8.15. Решение о конкретном составе мер, описанных в пп. 8.10 и 8.11 настоящего Положения, и об их исполнении принимает Ответственное лицо за организацию обработки персональных данных.

9. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА

9.1. Работники и их представители должны быть ознакомлены под расписку с документами Общества, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

9.2. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

9.3. Работник обязан:

- передавать Обществу и (или) его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации.
- своевременно сообщать Обществу об изменении своих персональных данных.

9.4. Работники ставят Общество в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании

представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

9.5. В целях защиты частной жизни, личной и семейной тайны работники вправе отказываться от обработки персональных данных без их согласия.

10. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТОВ И КОНТРАГЕНТОВ

10.1. В целях обеспечения защиты персональных данных, хранящихся у Оператора, клиенты и контрагенты имеют право на:

10.1.1. Полную информацию о составе персональных данных и их обработке, в частности клиент или контрагент имеет право знать, кто и в каких целях использует или использовал информацию о его персональных данных.

10.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные клиента или контрагента, за исключением случаев, предусмотренных законодательством РФ.

10.1.3. Определение своих представителей для защиты своих персональных данных.

10.1.4. Требование об исключении или исправлении неверных или неполных устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Оператора персональных данных. При отказе Оператора исключить или исправить персональные данные клиента или контрагента он имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия.

10.1.5. Требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные клиента или контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях.

10.1.6. Обжалование в суд любых неправомерных действий или бездействия Оператора при обработке и защите его персональных данных.

10.2. В целях обеспечения достоверности персональных данных, клиент и контрагент обязан:

10.2.1. При заключении договора предоставить Оператору полные и достоверные данные о себе в письменном виде;

10.2.2. В случае изменения сведений, составляющих персональные данные клиента или контрагента, незамедлительно, но не позднее пяти рабочих дней, предоставить данную информацию Оператору в письменном виде.

11. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ РАБОТНИКОВ

11.1. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

11.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

11.3. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

11.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-

правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

11.4.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера Общество вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

11.4.2. Должностные лица, в обязанность которых входит обработка персональных данных, 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 - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

11.4.3. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

11.4.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом.

11.5. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

12. ОБЯЗАННОСТИ РАБОТНИКОВ ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

12.1. В целях охраны конфиденциальности информации все работники обязаны:

12.1.1. Не разглашать сведения, составляющие коммерческую тайну Общества, за исключением случаев, когда есть письменное согласие руководителя Общества.

12.1.2. Не использовать сведения, составляющие коммерческую тайну Общества, для занятия другой деятельностью, в процессе работы для другой организации, предприятия, учреждения, по заданию физического лица или в ходе осуществления предпринимательской деятельности, а также в личных целях.

12.1.3. Выполнять установленный Обществом режим коммерческой тайны.

12.1.4. Незамедлительно ставить в известность непосредственного руководителя и руководителя Общества о необходимости отвечать либо об ответах на вопросы должностных лиц компетентных органов (налоговая инспекция, органы предварительного следствия и т.п.), находящихся при исполнении служебных обязанностей, по вопросам коммерческой тайны Общества.

12.1.5. Незамедлительно сообщать руководителю Общества об утрате или недостаче носителей информации, составляющей коммерческую тайну, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению коммерческой тайны Общества, а также о причинах и условиях возможной утечки информации, составляющей коммерческую тайну Общества.

12.1.6. В случае попытки посторонних лиц получить от работника сведения, содержащие коммерческую тайну Общества, незамедлительно известить об этом непосредственного руководителя и руководителя Общества.

12.1.7. Не создавать условия для утечки информации, составляющей коммерческую тайну, и предпринимать все усилия для пресечения такой утечки, если ему стало известно, что утечка имеет место или что складываются условия для возможности таковой.

12.1.8. Не разглашать и не использовать для себя или других лиц коммерческую тайну в течение трех лет после прекращения трудового договора с Обществом (независимо от причин увольнения).

12.1.9. Передать Обществу при прекращении трудового договора или гражданско-правового договора имеющиеся в пользовании работника материальные носители с информацией, составляющей коммерческую тайну.

СОГЛАСОВАНО:

Юрисконсульт _____ В.В. Федотов, «24» сентября 2019г.

Системный администратор _____ И.В. Михалев, «24» сентября 2019г.

Руководитель службы персонала _____ Г.В. Юркина, «24» сентября 2019г.