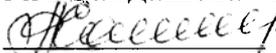


УТВЕРЖДЕНО:

ИП Сайдашева Альбина Саидзяновна

 Сайдашева А.С.

Приказ № 1-З/Д

«29» декабря 2017г.

ПОЛОЖЕНИЕ

О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

ИП Сайдашева Альбина Саидзяновна

**г. Пермь
2018 год**

I. Общие положения

1.1. Настоящим Положением определяется порядок обращения с персональными данными сотрудников и клиентов (далее - лица) ИП Сайдашевой А.С.(далее — ИП, Компания, Оператор).

1.2. Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и интересов Компании, ее сотрудников и клиентов в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих персональные данные, а также обеспечить защиту персональных данных лиц от несанкционированного доступа, неправомерного использования или утраты.

1.3. Персональные данные сотрудника и клиента - любая информация, относящаяся к данному лицу (субъекту персональных данных) и необходимая Компании в связи с трудовыми отношениями и отношениями с клиентами, в том числе:

- фамилия, имя, отчество лица;
- дата и место рождения лица;
- место проживания;
- семейное, социальное, имущественное положение;
- образование, профессия;
- доходы, имущество и имущественные обязательства лица;
- состояние здоровья и наличие заболеваний
- другая аналогичная информация, на основании которой возможна безошибочная идентификация субъекта персональных данных.

1.4. Сведения о персональных данных сотрудников и клиентов относятся к числу конфиденциальных (составляющих охраняемую законом тайну Компании). Режим конфиденциальности в отношении персональных данных снимается:

- в случае их обезличивания;
- в других случаях, предусмотренных федеральными законами.

1.5. Настоящее Положение утверждается и вводится в действие приказом Индивидуального предпринимателя и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников и клиентов.

II. Основные понятия. Состав персональных данных Сотрудников и Клиентов

2.1. Для целей настоящего Положения используются следующие основные понятия:

- персональные данные лица - в соответствии с определением п. 1.3 настоящего Положения;
- обработка персональных данных лица - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;
- конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;
- распространение персональных данных - действия, направленные на передачу персональных данных сотрудников/клиентов определенному кругу лиц (передача персональных данных) или ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных лиц в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или представление доступа к персональным данным лиц каким-либо иным способом;
- использование персональных данных - действия (операции) с персональными данными, совершаемые уполномоченным должностным лицом Компании в целях принятия решений или совершения иных действий, порождающих юридические последствия в

отношении лиц 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 лиц, в том числе их передачи;

- уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных лиц или в результате которых уничтожаются материальные носители персональных данных лиц;

- обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту;

- общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия лица, 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.

2.2. При поступлении на работу работник представляет сотрудникам отдела кадров следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;

- страховое свидетельство государственного пенсионного страхования;

- свидетельство о регистрации индивидуального налогового номера (ИНН);

- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;

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

2.3. При оформлении договора о сотрудничестве клиент представляет следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность, гражданство;

- свидетельство ИНН;

- свидетельство ОГРН;

- в отдельных случаях с учетом специфики взаимоотношений, действующим законодательством РФ может предусматриваться необходимость предъявления дополнительных документов.

2.4. Запрещается требовать от лица, поступающего на работу (или прием), документы помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

2.5. После того, как будет принято решение о приеме работника на работу, а также впоследствии в процессе трудовой деятельности, к документам, содержащим персональные данные субъекта, также будут относиться:

- трудовой договор;

- приказ о приеме на работу;

- приказы о поощрениях и взысканиях;

- приказы, связанные с прохождением учебы сотрудников;

- карточка унифицированной формы Т-2, утвержденная постановлением

Госкомстата России от 05.01.04 №1;

- другие документы согласно законодательству Российской Федерации

2.5. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, электронные базы). В общедоступные источники персональных данных могут включаться фамилия, имя, отчество, должность, подразделение, служебные и личные телефоны и адрес электронной почты.

2.5. К числу массовых потребителей персональных данных вне учреждения относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, областных и муниципальных органов управления. Надзорно - контрольные органы имеют доступ к информации только в сфере своей компетенции.

III. Порядок обработки персональных данных сотрудников и клиентов

3.1. Обработка персональных данных субъекта может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, количества и качества выполняемой работы, обследования, наблюдения и лечения клиентов и обеспечения сохранности имущества оператора, работника (клиента) и третьих лиц.

3.2. Обработка персональных данных может осуществляться для статистических или иных научных целей при условии обязательного обезличивания персональных данных.

3.3. При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ и иными федеральными законами.

3.4. Информация о персональных данных субъекта предоставляется оператору субъектом устно, либо путем заполнения личных карточек формы Т-2 для работников, которые хранятся в личном деле в отделе кадров (регистратуре/архиве). Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом и от него должно быть получено письменное согласие (либо письменный отказ). В письменном уведомлении оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

3.5. Оператор не имеет права получать и обрабатывать персональные данные субъекта, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

3.6. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.7. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

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

IV. Передача персональных данных

4.1. При передаче персональных данных субъектов сотрудники Компании, имеющие доступ к персональным данным, должны соблюдать следующие требования:

4.1.1. Не сообщать персональные данные субъекта третьей стороне без письменного согласия работника субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных Трудовым кодексом РФ или иными федеральными законами. Учитывая, что Трудовой кодекс РФ не определяет критерии ситуаций, представляющих угрозу жизни или здоровью субъекта, оператор в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных субъекта, либо отсутствует письменное согласие субъекта на предоставление его персональных сведений, либо, по мнению оператора, отсутствует угроза жизни или здоровью субъекта, оператор обязан отказать в предоставлении персональных данных лицу.

4.1.2. Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

4.1.3. Предупредить лиц, получающих персональные данные субъекта, 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.

4.1.4. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения конкретных функций.

4.1.5. Все сведения о передаче персональных данных субъекта регистрируются в Журнале учета передачи персональных данных в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана.

4.1.6. Передавать персональные данные работника представителю работника в порядке, установленном Трудовым кодексом РФ и настоящим Положением, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанным представителем его функций.

V. Права субъектов персональных данных

5.1. В целях обеспечения защиты персональных данных, хранящихся у оператора, субъекты имеют право на:

5.1.1. Полную и безвозмездную информацию об их персональных данных и обработке этих данных.

5.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных федеральным законом.

5.1.3. Определение своих представителей для защиты своих персональных данных.

5.1.4. Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса РФ или иного федерального закона. При отказе оператора исключить или исправить персональные данные субъекта он имеет право заявить в письменной форме оператору о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.1.5. Требование об извещении оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях.

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

VI. Ответственность за нарушение норм, регулирующих обработку персональных данных

6.1. Сотрудники Компании, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии действующим законодательством.

6.2. Руководитель Компании за нарушение порядка обращения с персональными данными несет административную ответственность согласно ст. ст. 5.27 и 5.39 Кодекса об административных правонарушениях РФ, а также возмещает сотруднику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные об этом сотруднике.

6.3. Каждый сотрудник Компании, получающий для работы сведения, содержащие персональные данные, несет единоличную ответственность за сохранность носителя и конфиденциальность персональных данных.

6.4. За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы с персональными данными Компания вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

6.5. Должностные лица, в обязанность которых входит ведение персональных данных лица, 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.

VII. Заключительные положения

7.1. Настоящее Положение вступает в силу с момента его утверждения Индивидуальным предпринимателем.

7.2. Настоящее Положение доводится до сведения всех субъектов ПД Индивидуального предпринимателя.

СВЕДЕНИЯ О РЕАЛИЗУЕМЫХ ТРЕБОВАНИЯХ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ У ИП САЙДАШЕВА АЛЬБИНА САИДЗЯНОВНА.

Защита персональных данных, обрабатываемых ИП Сайдашевой А.С. (далее - Оператор), обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований законодательства в области защиты персональных данных.

Правовые меры включают:

1. разработку локальных актов Оператора, реализующих требования законодательства Российской Федерации, в том числе Положения о защите персональных данных ИП Сайдашевой А.С.;
2. отказ от любых способов обработки персональных данных, не соответствующих целям, заранее predetermined Оператором.

Организационные меры включают:

1. назначение лица, ответственного за организацию обработки персональных данных;
2. назначение лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных;
3. ограничение состава работников Оператора, имеющих доступ к персональным данным, и организацию разрешительной системы доступа к ним;
4. ознакомление работников Оператора, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, с Положением, другими локальными актами Оператора по вопросам обработки персональных данных;
5. обучение всех категорий работников, непосредственно осуществляющих обработку персональных данных, правилам работы с ними и обеспечения безопасности обрабатываемых данных;
6. регламентацию процессов обработки персональных данных;
7. организацию учёта материальных носителей персональных данных и их хранения, обеспечивающих предотвращение хищения, подмены, несанкционированного копирования и уничтожения;
8. определение угроз безопасности персональных данных при их обработке в информационных системах, формирование на их основе моделей угроз;
9. размещение технических средств обработки персональных данных в пределах охраняемой территории Оператора;
10. ограничение допуска посторонних лиц в помещения Оператора, недопущение их нахождения в помещениях, где ведется работа с персональными данными и размещаются технические средства их обработки, без контроля со стороны работников Оператора.

Технические меры включают:

1. определение типа угроз безопасности персональных данных, актуальных для информационных систем персональных данных с учетом оценки возможного вреда субъектам персональных данных, который может быть причинен в случае нарушения требований безопасности, определение уровня защищенности персональных данных и реализацию требований к защите персональных данных при их обработке в информационных системах, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
2. разработку на основе модели угроз системы защиты персональных данных для установленных Правительством Российской Федерации уровней защищенности персональных данных при их обработке в информационных системах;
3. использование для нейтрализации актуальных угроз средств защиты информации, прошедших процедуру оценки соответствия;

4. оценку эффективности принимаемых мер по обеспечению безопасности персональных данных;

5. реализацию разрешительной системы доступа работников к персональным данным, обрабатываемым в информационных системах, и программно-аппаратным и программным средствам защиты информации;

6. выявление вредоносного программного обеспечения (применение антивирусных программ) на всех узлах информационной сети Оператора, обеспечивающих соответствующую техническую возможность;

7. безопасное межсетевое взаимодействие (применение межсетевого экранирования);

8. обнаружение вторжений в информационную систему Оператора, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

9. восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (систему резервного копирования и восстановления персональных данных);

10. периодическое проведение мониторинга действий пользователей, разбирательств по фактам нарушения требований безопасности персональных данных;

**ПРИКАЗ
№1-ЗПД**

«29» декабря 2017г.

г.Пермь

Об утверждении Положения о защите персональных данных

ИП Сайдашева Альбина Саидзяновна

ПРИКАЗЫВАЮ:

1. Утвердить Положение о защите персональных данных ИП Сайдашева Альбина Саидзяновна
2. Разместить указанное Положение на официальном сайте ИП Сайдашева Альбина Саидзяновна
3. Контроль за исполнением приказа оставляю за собой.

Приложение: Положение о защите персональных данных ИП Сайдашева Альбина Саидзяновна

 А.С.Сайдашева