Управление труда и занятости Республики Карелия
Государственное казенное учреждение Республики Карелия
«ЦЕНТР ЗАНЯТОСТИ НАСЕЛЕНИЯ РЕСПУБЛИКИ КАРЕЛИЯ

П Р И К А З

г. Петрозаводск

«30» августа 2022 г. № 721-П

О персональных данных
в Государственном казенном учреждении Республики Карелия
«Центр занятости населения Республики Карелия»

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

ПРИКАЗЫВАЮ:

1. Утвердить:

Положение об обработке персональных данных в Государственном казенном учреждении Республики Карелия «Центр занятости населения Республики Карелия» (Приложение №1).

Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Государственного казенного учреждения Республики Карелия «Центр занятости населения Республики Карелия» (Приложение №2);

2. Отделу правовой, кадровой и организационной работы в срок до 15.09.2022г. довести настоящий приказ до сведения заинтересованных работников Учреждения.

3. Признать утратившим силу приказ Государственного казенного учреждения Республики Карелия «Центр занятости населения Республики Карелия» от 25.09.2019 г. № 315-П.

Директор В.А. Шестак

Приложение № 1
к приказу ГКУ ЦЗН РК
от 30 .08.2022 года № 721 -П

ПОЛОЖЕНИЕ
об обработке персональных данных в Государственном казенном учреждении Республики Карелия «Центр занятости населения Республики Карелия»

Общие положения

1.1. Положение об обработке персональных данных в Государственном казенном учреждении Республики Карелия «Центр занятости населения Республики Карелия» (далее - Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»), Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. Целью данного Положения является защита персональных данных от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, определенного действующим законодательством и нормативно-правовыми актами Государственного казенного учреждения Республики Карелия «Центр занятости населения Республики Карелия» (далее - Учреждение), если иное не определено законом.

1.4. Сбор персональных данных в Учреждении осуществляется с целью их последующей обработки в информационной системе персональных данных (далее - ИСПДн).

1.5. Настоящее Положение утверждается и вводится в действие приказом директора Учреждения и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

1.6. Изменения в Положение могут быть внесены приказом директора Учреждения в установленном действующим законодательством порядке.

Состав персональных данных

2.1. В состав персональных данных работников Учреждения входят:

- фамилия, имя, отчество (в том числе предыдущие фамилии, имена и(или) отчества, в случае их изменения);

- число, месяц, год рождения и место рождения;

- информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

- паспортные данные;

- адрес места жительства (адрес регистрации, фактического проживания);

- номер контактного телефона или сведения о других способах связи;

- реквизиты СНИЛС;

- идентификационный номер налогоплательщика;

- акты гражданского состояния;

- семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

- сведения о трудовой деятельности;

- сведения о воинском учете и реквизиты документов воинского учета;

- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

- фотография;

- сведения о профессиональной переподготовке и (или) повышении квалификации;

- номер расчетного счета;

- номер банковской карты;

- имущественное положение и доходы;

- сведения о состоянии здоровья;

- профессия;

2.2. В состав персональных данных субъектов (заявителей) Учреждения входят:

- документы, удостоверяющие личность гражданина Российской Федерации, в том числе военнослужащих, а также документы, удостоверяющие личность иностранного гражданина, лица без гражданства, включая вид на жительство и удостоверение беженца;

- фамилия, имя, отчество (в том числе предыдущие фамилии, имена и(или) отчества, в случае их изменения);

- число, месяц, год рождения и место рождения;

- информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

- адрес места жительства (адрес регистрации, фактического проживания);

- номер контактного телефона или сведения о других способах связи;

- реквизиты СНИЛС;

- идентификационный номер налогоплательщика;

- номер расчетного счета;

- номер банковской карты;

- сведения о воинском учете и реквизиты документов воинского учета;

- акты гражданского состояния;

- семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

- документы, подтверждающие регистрацию по месту жительства или по месту пребывания;

- документы на транспортное средство и его составные части, в том числе регистрационные документы;

- сведения о трудовой деятельности;

- имущественное положение и доходы;

- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);

- фотография;

- сведения о состоянии здоровья;

- документы Архивного фонда Российской Федерации и другие архивные документы в соответствии с законодательством об архивном деле в Российской Федерации, переданные на постоянное хранение в государственные или муниципальные архивы;

- документы, выданные (оформленные) органами дознания, следствия либо судом в ходе производства по уголовным делам, документы, выданные (оформленные) в ходе гражданского судопроизводства либо судопроизводства в арбитражных судах, в том числе решения, приговоры, определения и постановления судов общей юрисдикции и арбитражных судов;

- решения, заключения и разрешения, выдаваемые органами опеки и попечительства в соответствии с законодательством Российской Федерации об опеке и попечительстве;

- правоустанавливающие документы на объекты недвижимости, права на которые зарегистрированы / не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

- документы, выдаваемые федеральными государственными учреждениями медико-социальной экспертизы;

- удостоверения и документы, подтверждающие право гражданина на получение социальной поддержки, а также документы, выданные федеральными органами исполнительной власти, в которых законодательством предусмотрена военная и приравненная к ней служба, и необходимые для

осуществления пенсионного обеспечения лица в целях назначения и перерасчета размера пенсий;

- документы о государственных и ведомственных наградах, государственных премиях и знаках отличия;

- сведения о судимости;

- социальное положение;

- профессия;

- дополнительные сведения, предусмотренные требованиями Федеральных Законов, определяющих случаи и особенности обработки персональных данных.

Хранение персональных данных

3.1. Хранение персональных данных субъектов осуществляется в отделе правовой, кадровой и организационной работы, отделе финансово - экономического обеспечения и социальных выплат, а также в иных отделах Учреждения, в соответствии с Положением о данных отделах Учреждения, на бумажных и электронных носителях с ограниченным доступом к данной информации.

3.2. Личные дела хранятся в печатном виде в папках в металлических шкафах, обеспечивающих защиту от несанкционированного доступа.

3.3. Отделы Учреждения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждённого постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

Обработка персональных данных в Учреждении

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

4.2. В целях обеспечения прав и свобод человека и гражданина операторы при обработке персональных данных обязаны соблюдать следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении, продвижении по службе, оказании государственных услуг, обеспечении личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

- при определении объема и содержания обрабатываемых персональных данных, оператор должен руководствоваться Конституцией Российской Федерации и иными федеральными законами;

- получение персональных данных осуществляется от субъекта ПДн или его официального представителя;

- если персональные данные возможно получить только у третьей стороны, то лицо должно быть уведомлено об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить лицу о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа лица дать письменное согласие на их получение. Согласие субъекта персональных данных не требуется в случае, если обработка персональных данных ведется для осуществления и выполнения, возложенных законодательством Российской Федерации на Учреждение функций, полномочий и обязанностей, не предусматривающих получение согласия субъекта на обработку персональных данных;

- оператор не имеет права получать и обрабатывать персональные данные лиц о политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни (информация о жизнедеятельности в сфере семейных, бытовых, личных отношений) могут быть получены и обработаны оператором только с письменного согласия лица;

- оператор не имеет право получать и обрабатывать персональные данные лица о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

4.3. 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 и карается в соответствии с законодательством.

4.4. Передача персональных данных возможна только с согласия лица или в случаях, прямо предусмотренных законодательством. При передаче персональных данных оператор должен соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия лица, за исключением случаев, когда это необходимо в целях

предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом;

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

- 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 федеральными законами;

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

- передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;

- при передаче персональных данных потребителям (в том числе и в коммерческих целях) за пределы организации оператор не должен сообщать эти данные третьей стороне без письменного согласия лица, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью или в случаях, установленных федеральным законом.

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

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

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

Доступ к персональным данным

5.1. Право внутреннего доступа (доступ внутри организации) к персональным данным, имеют:

- директор Учреждения;

- сотрудники организации при выполнении ими своих служебных обязанностей;

- само лицо, носитель данных.

5.2. Право внешнего доступа к персональным данным имеют:

- надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

Защита персональных данных

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

6.1. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

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

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

6.4. «Внутренняя защита». Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации. Для обеспечения внутренней защиты персональных данных 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 работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

- знание работником требований нормативно - методических документов по защите информации и сохранении тайны;

- наличие необходимых условий 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;

- организация порядка уничтожения информации;

- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

6.5. «Внешняя защита». Как результат мер, принимаемых по защите конфиденциальной информации, создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделах, занимающихся обработкой персональных данных. Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;

- пропускной режим организации;

- технические средства охраны, сигнализации;

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

- требования к защите информации при интервьюировании и собеседованиях.

6.6. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных.

6.7. По возможности персональные данные обезличиваются.

6.8. Кроме мер защиты персональных данных, установленных законодательством, оператор может вырабатывать совместные меры защиты персональных данных.

Права и обязанности

7.1. Субъекты персональных данных, указанные имеют право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон);

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

9.1) информацию о способах исполнения оператором обязанностей, установленных статьей 18 Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных»;

10) иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

7.2. Сведения, указанные в пункте 7.1 Положения, предоставляются субъекту персональных данных или его представителю Учреждением в течение десяти рабочих дней с момента обращения либо получения Учреждением запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Учреждение предоставляет сведения, указанные в пункте 7.1 Положения, субъекту

персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

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

7.4. В предоставляемых сведениях указанные в пункте 7.1 Положения, не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

10. Если в соответствии с федеральным законом предоставление персональных данных и (или) получение Управлением согласия на обработку персональных данных являются обязательными, Управление обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку».

11. Сроки предоставления информации субъекту персональных данных устанавливаются в соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных».

12. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Управление обязано прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Управлением и субъектом персональных данных либо если Управление не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами. В случае обращения субъекта персональных данных в Управление с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий десяти рабочих дней с даты получения Управлением соответствующего требования, прекратить их обработку за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 настоящего Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных». Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Управлением в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации».

Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

8.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

8.2. 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.

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

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

8.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

8.6. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

8.7. Должностные лица, в обязанность которых входит ведение 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.

8.8. 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.

8.9. 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 в соответствии с УК РФ.

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

Приложение № 1
к Положению об обработке
персональных данных

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(фамилия, имя, отчество)

зарегистрированный (ая) по адресу:

_____
(адрес места жительства/пребывания)

_____

документ, удостоверяющий личность: _____ серия _____

номер _____ выдан « » _____
(дата и орган, выдавший документ)

_____

действующий(ая) по своей воле и в своих интересах даю согласие Государственному казенному учреждению Республики Карелия «Центр занятости населения Республики Карелия», юридический адрес: 185030, Республика Карелия, г. Петрозаводск, ул. Маршала Мерецкова, д. 14, на автоматизированную, а также без использования средств автоматизации обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) моих персональных данных (фамилия, имя, отчество, адрес, паспортные данные и иные персональные данные, содержащиеся в предоставленных документах) в объеме, необходимом для получения государственных (муниципальных) услуг в соответствии с административными регламентами, порядками, правилами и иными документами, определяющими порядок предоставления услуг:

_____
(наименование услуги)

Настоящее согласие действует с момента подписания в течении 3 лет. Если по истечении данного срока согласие не будет отозвано его действие продлевается на 10 лет. Я уведомлен (а) о своем праве отозвать согласие на обработку персональных данных путем подачи соответствующего заявления в письменном виде.

_____
(дата, ФИО, собственноручная подпись)

Приложение № 2
к Положению об обработке
персональных данных

СОГЛАСИЕ
на обработку персональных данных по доверенности

Я, _____,

(фамилия, имя, отчество)

зарегистрированный (ая) по адресу: _____

(адрес места жительства/пребывания)

_____

документ, удостоверяющий личность: _____ серия _____

номер _____ выдан _____ « » _____

(дата и орган, выдавший документ)

_____

даю согласие от имени заявителя-доверителя_____

_____,

(фамилия, имя, отчество)

паспортные данные заявителя_____

на основании доверенности_____

(реквизиты доверенности)

Государственному казенному учреждению Республики Карелия «Центр занятости населения Республики Карелия», юридический адрес: 185030, Республика Карелия, г. Петрозаводск, ул. Маршала Мерецкова, д. 14, на автоматизированную, а также без использования средств автоматизации обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) персональных данных доверителя (фамилия, имя, отчество, адрес, паспортные данные и иные персональные данные, содержащиеся в предоставленных документах) в объеме, необходимом для получения государственных (муниципальных) услуг в соответствии с административными регламентами, порядками, правилами и иными документами, определяющими порядок предоставления услуг:

_____

(наименование услуги)

Настоящее согласие действует с момента подписания в течении 3 лет. Если по истечении данного срока согласие не будет отозвано его действие продлевается на 10 лет. Я уведомлен (а) о своем праве отозвать согласие на обработку персональных данных путем подачи соответствующего заявления в письменном виде.

_____

(дата, ФИО, собственноручная подпись)

Приложение № 3
к Положению об обработке
персональных данных

СОГЛАСИЕ
законного представителя
на обработку персональных данных субъекта

Я, _____,
паспорт серии _____ номер_____ выдан «_____» _____,
_____,
(дата и орган, выдавший документ)

даю согласие Государственному казенному учреждению Республики Карелия «Центр занятости населения Республики Карелия», юридический адрес: 185030, Республика Карелия, г. Петрозаводск, ул. Маршала Мерецкова, д. 14, на автоматизированную, а также без использования средств автоматизации обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) персональных данных
моего/моей_____
(дочь, сын, опекаемый, подопечный и т.д.)

_____
_____
(фамилия, имя, отчество, адрес, паспортные данные и иные персональные данные, содержащиеся в предоставленных документах)

в объеме, необходимом для получения государственных (муниципальных) услуг в соответствии с административными регламентами, порядками, правилами и иными документами, определяющими порядок предоставления услуг:

_____
(наименование услуги)

Настоящее согласие действует с момента подписания в течении 3 лет. Если по истечении данного срока согласие не будет отозвано его действие продлевается на 10 лет. Я уведомлен (а) о своем праве отозвать согласие на обработку персональных данных путем подачи соответствующего заявления в письменном виде.

_____
(ФИО, собственноручная подпись)

«____» _____ 20 ____ г.

Приложение № 4
к Положению об обработке
персональных данных

СОГЛАСИЕ
на обработку персональных данных
(для опубликования на сайте)

Я, _____ ,
(фамилия, имя, отчество)

документ, удостоверяющий личность: _____ серия _____

номер _____ выдан «___» _____
(дата и орган, выдавший документ)

Действующий(ая) по своей воле и в своих интересах даю согласие на размещение моих персональных данных (фамилия, имя, отчество, занимаемая должность в Учреждении) в сети Интернет на официальном сайте Государственному казенному учреждению Республики Карелия «Центр занятости населения Республики Карелия».

Настоящее согласие действует с момента подписания в течении 3 лет. Если по истечении данного срока согласие не будет отозвано его действие продлевается на 10 лет. Я уведомлен (а) о своем праве отозвать согласие на обработку персональных данных путем подачи соответствующего заявления в письменном виде.

_____
(дата, ФИО, собственноручная подпись)

Приложение № 5
к Положению об обработке
персональных данных

Заявление
об отзыве согласия на обработку персональных данных

Я, _____,
паспорт серии _____ номер_____ выдан «_____» _____,
_____,
(дата и орган, выдавший документ)

Прошу Вас прекратить обработку моих персональных данных в связи с:

_____
(указать причину)

_____
(ФИО, собственноручная подпись)

«____» _____ 20 ____ г.

Приложение № 6
к Положению об обработке
персональных данных

_____
(наименование оператора)

_____
(Ф.И.О. субъекта персональных данных)

_____
(адрес регистрации субъекта персональных данных)

_____
(номер основного документа, удостоверяющего его личность)

_____
(дата выдачи указанного документа)

_____
(наименование органа, выдавшего документ)

Согласие субъекта
на передачу его персональных данных третьей стороне

Я, _____ ,

Паспорт: серии _____ номер_____ выдан «_____» _____ ,

_____ ,
(дата и орган, выдавший документ)

в соответствии со статьей 88 Трудового Кодекса Российской Федерации _____
(согласен / не согласен)

на передачу моих персональных данных, а именно:

_____
_____
_____
(указать состав персональных данных (Ф.И.О, паспортные данные, адрес)

Для обработки в целях _____
_____
_____
(указать цели обработки)

следующим лицам (кредитные учреждения, аккредитованные УЦ, организации, предоставляющие охранные услуги:

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

Мне разъяснены и понятны все возможные последствия моего отказа дать письменное согласие на их передачу.

Настоящее согласие действует с момента подписания и до момента прекращения трудовых правоотношений. Я уведомлен (а) о своем праве отозвать согласие на обработку персональных данных путем подачи соответствующего заявления в письменном виде.

_____
(ФИО, собственноручная подпись)

«____» _____ 20 ____ г.

Приложение № 7
к Положению об обработке
персональных данных

Журнал учёта передачи персональных данных

№ п/п	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/отказа в передаче персональных данных	Подпись запрашивающего лица	Подпись ответственного работника

Приложение № 8
к Положению об обработке
персональных данных

Обязательство о неразглашении персональных данных работников

Я, _____
(фамилия, имя, отчество)

паспорт серии _____ номер _____ выдан «_____» _____ 20___г.
_____
(дата и орган, выдавший документ)

понимаю, что получаю доступ к персональным данным работников и кандидатов на вакантные должности Учреждения.

Я понимаю, что во время исполнения своих функциональных обязанностей, мне необходимо заниматься сбором, обработкой и хранением персональных данных.

Я также понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В соответствии с действующим законодательством Российской Федерации, даю обязательство, что при работе (сборе, обработке и хранении) с персональными данными обязуюсь соблюдать все описанные в Положении о защите персональных данных требования.

Я подтверждаю, что не имею права разглашать сведения:

- анкетные и биографические данные;
- паспортные данные;
- о трудовом и общем стаже;
- об образовании;
- о составе семьи;
- о воинском учёте;
- о заработной плате работника;
- о социальных льготах;
- специальность и занимаемая должность;
- адрес места жительства (номер домашнего телефона);
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- приказы по личному составу (основания к приказам по личному составу);
- личные дела и трудовые книжки работников;
- дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;
- отчёты, направляемые в органы статистики.

Я предупрежден(а) о том, что в случае разглашения мною сведений, касающихся персональных данных или их утраты (порчи) несу ответственность в соответствии со статьей 90 Трудового Кодекса Российской Федерации. С Положением о защите персональных данных ознакомлен(а).

_____
(ФИО, собственноручная подпись)

«____» _____ 20 ____ г.

Приложение № 9
к Положению об обработке
персональных данных

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных, ставших известными в связи выполнением служебных (трудовых) обязанностей

Я,

_____
(Фамилия, Имя, Отчество)

исполняющий(ая) должностные обязанности по занимаемой должности

_____
(наименование должности, отдела)

Государственному казенному учреждению Республики Карелия «Центр занятости населения Республики Карелия» предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностным регламентом, мне будет предоставлен допуск к персональным данным. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам персональные данные, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. Не передавать и не раскрывать третьим лицам персональные данные, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
3. В случае попытки третьих лиц получить от меня персональные данные, сообщать непосредственному руководителю, а также сотрудникам отдела по защите информации.
4. Не использовать персональные данные с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.
6. В течение года после прекращения права на допуск к персональным данным не разглашать и не передавать третьим лицам известные мне персональные данные.

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

_____ _____
(фамилия, инициалы) (подпись)

«_____»_____20__г.

Один экземпляр обязательств о неразглашении персональных данных получил.

_____ _____
(фамилия, инициалы) (подпись)

Приложение № 2
к приказу ГКУ ЦЗН РК
от ___.08.2022 года № ____-П

ПОЛОЖЕНИЕ

по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Государственного казенного учреждения Республики Карелия «Центр занятости населения Республики Карелия»

Общие положения

Назначение документа

1.1.1 Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – Положение) определяет содержание и порядок осуществления мероприятий по защите персональных данных в Государственном казенном учреждении Республики Карелия «Центр занятости населения Республики Карелия» (далее - Учреждение).

1.1.2 Настоящее Положение разработано в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и «Положением об обработке персональных данных».

1.1.3 Цель Положения – регулирование работ по защите персональных данных и обеспечение функционирования информационных систем персональных данных Учреждения в соответствии с требованиями действующего федерального законодательства в области информационной безопасности.

Область действия документа

1.2.1 Действие Положения распространяется на информационные системы персональных данных (далее – ИСПДн) Учреждения, в которых осуществляется обработка персональных данных (далее – ПДн).

1.2.2 Все работники Учреждения, допущенные к работе с персональными данными, в обязательном порядке должны быть ознакомлены с настоящим Положением под подпись.

Вступление в силу документа

1.3.1 Настоящее Положение вступает в силу с момента его утверждения директором Учреждения и действует бессрочно до замены его новым Положением.

1.3.2 Все изменения в Положение вносятся приказом директора Учреждения.

Организация и проведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Планирование работ по обеспечению безопасности персональных данных

2.1.1 В целях исполнения настоящего Положения ответственный за защиту ПДн и администратор безопасности составляют и утверждают у директора план работ по обеспечению безопасности ПДн, обрабатываемых в Учреждении.

Проводимые в Учреждении мероприятия по обеспечению безопасности персональных данных учитываются в плане мероприятий по защите персональных данных в Учреждении.

Выполнение работ по обеспечению безопасности персональных данных

2.2.1 В целях организации и проведения работ по обеспечению безопасности персональных данных в Учреждении приказом директора назначаются:

- лицо, ответственное за проведение мероприятий по обеспечению безопасности персональных данных и поддержание необходимого уровня информационной безопасности;
- администратор информационной безопасности, ответственный за установку, настройку и обслуживание средств защиты информации, применяемых в Учреждении для обеспечения безопасности персональных данных, а также за организацию и проведение инструктажа работников по основам информационной безопасности при работе с персональными данными;
- комиссия по проведению классификации информационных систем.

2.2.2 Указанные лица ответственны за проведение следующих мероприятий по обеспечению безопасности персональных данных:

- определение и описание информационных систем персональных данных;
- классификацию информационных систем персональных данных;
- определение актуальных угроз безопасности персональных данных;
- проектирование системы защиты персональных данных, включающей организационные, физические и технические меры и средства защиты;
- закупку, установку и настройку технических средств защиты информации;

- внедрение организационных мер и разработку соответствующих регламентов и положений;

- инструктаж и обучение лиц, которые будут использовать средства защиты информации.

2.2.3. Начальники структурных подразделений, в которых происходит обработка персональных данных, являются лицами, ответственными за соблюдение требований Положения об обработке персональных данных и других установленных в Учреждении требований.

2.2.4. Для обеспечения безопасности персональных данных в Учреждении применяются следующие меры безопасности:

- организационные меры безопасности:

- инструктаж работников по правилам обеспечения безопасности обрабатываемых персональных данных;

- учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;

- мониторинг и реагирование на инциденты информационной безопасности, связанные с персональными данными, включая проведение внутренних проверок, разбирательств и составление заключений;

- постоянный контроль за соблюдением требований по обеспечению безопасности персональных данных (реализуется путем внутренних аудитов);

- меры физической безопасности:

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации. Приказом директора устанавливается контролируемая зона, вводятся в действие Список помещений с ограниченным доступом и Список лиц, имеющих право посещать помещения Учреждения с ограниченным доступом. Лица, не указанные в Списке, в том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств), при наличии необходимости могут посещать помещения с ограниченным доступом в сопровождении ответственных лиц;

- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

- технические меры безопасности:

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

- регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

- резервирование технических средств, дублирование массивов и носителей информации;

- использование защищенных каналов связи;

- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

2.2.5 Ремонтно-восстановительные работы технических средств обработки информации проводятся администратором безопасности. В случае необходимости ремонт технических средств может быть проведен с привлечением сторонних специалистов на договорной основе с составлением актов выполненных работ.

Контроль выполнения работ по обеспечению безопасности персональных данных

2.3.1 Контроль выполнения работ по обеспечению безопасности персональных данных в Учреждении (далее – Контроль) осуществляется путем проведения периодических контрольных мероприятий (в рамках внутренних аудитов) и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

2.3.2 В рамках проведения контрольных мероприятий выполняются:

- проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности персональных данных за истекший период;

- проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности персональных данных;

- проверка соответствия перечня лиц, которым предоставлен доступ к персональным данным, фактическому состоянию;

- проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности персональных данных, в соответствии с требованиями эксплуатационной и технической документации;

- инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности персональных данных (при необходимости);

- проверка соответствия моделей угроз для информационных систем персональных данных условиям функционирования данных систем;

- проверка соответствия организационно-распорядительной документации по обеспечению безопасности персональным данных действующим требованиям законодательства РФ, руководящих документов ФСБ России, ФСТЭК России.

2.3.3 Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

2.3.4 Контрольные мероприятия проводятся как периодически в соответствии с планом и программой аудита, так и внепланово по решению директора и в случае возникновения инцидентов информационной безопасности.

2.3.5 Внутренние проверки в Учреждении в обязательном порядке проводятся в случае выявления следующих фактов:

- нарушение конфиденциальности, целостности, доступности персональных данных;

- халатность и несоблюдение требований к обеспечению безопасности персональных данных;

- несоблюдение условий хранения носителей персональных данных;

- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

2.3.6 Задачами внутренней проверки являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

- установление лиц, непосредственно виновных в данном нарушении;

- выявление причин и условий, способствовавших нарушению.

Совершенствование системы защиты персональных данных

2.4.1 Ежегодно ответственный за защиту персональных данных предоставляет директору отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности персональных данных вместе с перечнем предложений по совершенствованию системы защиты персональных данных.

2.4.2 Необходимость реализации мероприятий по совершенствованию системы защиты персональных данных может быть обусловлена:

- результатами проведенных аудитов и контрольных мероприятий;

- изменениями федерального законодательства в области персональных данных;

- изменениями структуры процессов обработки персональных данных в пенсионном фонде;

- результатами анализа инцидентов информационной безопасности;

- результатами мероприятий по контролю и надзору за обработкой персональных данных, проводимых уполномоченным органом; □ жалоб и запросов субъектов персональных данных.

2.4.3 На основании решения, принятого директором по результатам рассмотрения ежегодного отчета и предложений по совершенствованию системы защиты персональных данных, ответственный за защиту персональных данных составляет план работ по обеспечению безопасности персональных данных, обрабатываемых в Учреждении, на следующий год.