Приложение к приказу
Управления социальной
защиты населения
администрации
Копейского городского округа
Челябинской области от
_____ №____

Правила
обработки персональных данных
в управлении социальной защиты населения администрации Копейского городского округа Челябинской области

I. Общие положения

1. Настоящие Правила обработки персональных данных в управлении социальной защиты населения администрации Копейского городского округа Челябинской области (далее – Правила, управление) разработаны в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства от 21 марта 2012 г. № 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» и устанавливают порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным субъектов управления.

2. Цель разработки Правил — определение порядка обработки персональных данных работников управления и иных субъектов персональных данных, персональные данные которых подлежат обработке (далее – субъекты ПДн, ПДн); защита ПДн от несанкционированного доступа, неправомерного их использования или утраты.

Управление является оператором ПДн лиц, указанных в пункте 3 настоящих Правил. На основании договора управление может поручать обработку ПДн третьим лицам. Существенным условием договора об оказании услуг по обработке ПДн является обязанность обеспечения этими лицами конфиденциальности и безопасности ПДн субъектов.

Настоящие Правила вступают в силу с момента их утверждения и действуют бессрочно, до замены новыми Правилами.

Все изменения в Правила утверждаются приказом начальника управления.

II. Основные понятия и состав ПДн

3. Под субъектами ПДн подразумеваются следующие лица:

- лица, имеющие трудовые, договорные и иные гражданско-правовые отношения с управлением (далее – работники управления);
- граждане, обратившиеся в управление за получением услуг.

4. Обработка ПДн осуществляется:

- без использования средств автоматизации;
- с использованием средств информационных систем ПДн управления.

5. Состав ПДн, обрабатываемых в информационной системе ПДн управления (далее – ИСПДн управления), определяется «Перечнем ПДн, обрабатываемых в ИСПДн управления».

6. Состав ИСПДн определяется «Перечнем ИСПДн управления»

7. Под обработкой ПДн понимаются действия (операции) с ПДн, включающие:

- сбор, хранение, уточнение (обновление, изменение);
- систематизацию, накопление;
- использование, распространение (в том числе передачу);
- обезличивание, блокирование, уничтожение.

8. Обработка ПДн работников осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении, продвижении по работе, обеспечения личной безопасности работника, контроля качества и количества выполняемой работы и обеспечения сохранности имущества, оплаты труда, пользования льготами, предусмотренными законодательством РФ и нормативными актами управления, а также для осуществления основной деятельности управления.

ПДн работников управления обрабатываются в следующих структурных подразделениях управления в соответствии с исполняемыми функциями:

- отдел бухгалтерского учета и отчетности;
-общий отдел.

9. Обработка ПДн граждан, обратившихся в управление, осуществляется с целью:

- рассмотрения обращений граждан и предоставления ответа на них;
- оказания муниципальных и государственных услуг.

ПДн граждан (клиентов) обрабатываются в следующих структурных подразделениях управления:

- общий отдел;
- отдел бухгалтерского учета и отчетности;
- отдел жилищных субсидий;
- отдел назначения мер социальной поддержки;
- отдел опеки и попечительства;

- отдел организации предоставления социальных услуг;
- отдел социальных выплат;
- отдел программно-технического обеспечения.

Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в управлении при его приеме, переводе и увольнении

10. Информация, представляемая работником при поступлении на работу в управление, должна иметь документальную форму. До заключения трудового договора работнику должны быть разъяснены юридические последствия отказа в предоставлении своих ПДн (приложение 1 к Правилам). При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

1) паспорт или иной документ, удостоверяющий личность;

2) трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

3) страховое свидетельство государственного пенсионного страхования;

4) документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;

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

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

11. При оформлении работника в управление специалистами заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

1) общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

2) сведения о воинском учете;

3) данные о приеме на работу.

В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных гарантиях;
- сведения о месте жительства и контактных телефонах.

12. В структурных подразделениях управления, указанных в пункте 8 настоящих Правил, создаются и хранятся следующие группы документов, содержащие ПДн работников управления в единичном или сводном виде:

1) документы, содержащие ПДн работников администрации (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов и распоряжений по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказам по личному составу; дела, содержащие материалы аттестации работников; служебные расследования; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству управления; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

2) организационно-распорядительная документация управления (порядки, должностные инструкции работников управления, распоряжения начальника); документы по планированию, учету, анализу и отчетности в части работы с работниками управления.

Комплекс документов, сопровождающий процесс оказания государственных муниципальных услуг населению

13. Информация, представляемая гражданами в управление, должна иметь документальную форму или форму электронного документа. Граждане предъявляют в установленных случаях следующие документы:

1) 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;

2) документы воинского учета;

3) свидетельства о государственной регистрации актов гражданского состояния;

4) документы, подтверждающие регистрацию по месту жительства или по месту пребывания;

5) документы о трудовой деятельности, трудовом стаже и заработке гражданина;

6) документы о соответствующих образовании и (или) профессиональной квалификации, об ученых степенях и ученых званиях и документы, связанные с

прохождением обучения, выдаваемые организациями, осуществляющими образовательную деятельность;

7) справки, заключения и иные документы, выдаваемые медицинскими организациями, осуществляющими медицинскую деятельность и входящими в государственную, муниципальную или частную систему здравоохранения;

8) 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;

9) решения, приговоры, определения и постановления судов общей юрисдикции и арбитражных судов;

10) учредительные документы юридического лица;

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

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

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

14) удостоверения и документы, подтверждающие право гражданина на получение социальной поддержки;

15) документы о государственных и ведомственных наградах, государственных премиях и знаках отличия.

14. В дальнейшем в ИСПДн обрабатываются ПДн согласно «Перечню ПДн, обрабатываемых в ИСПДн».

III. Сбор, обработка и защита ПДн

Правила получения ПДн

15. Все ПДн работников управления и прочих физических лиц следует получать у них самих. Если ПДн возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо управления должно сообщить о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа субъекта дать письменное согласие на их получение (приложение 2 к Правилам).

16. Управление не имеет права получать и обрабатывать ПДн работников администрации и прочих физических лиц об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

17. Управление вправе обрабатывать ПДн физических лиц по их запросу, а также при регистрации субъекта ПДн на едином или региональном портале государственных и муниципальных услуг, без их письменного согласия в

соответствии с требованиями статьи 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

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

19. Информация о субъектах ПДн, зафиксированная в автоматизированных системах и на бумажных носителях, должна храниться в условиях, исключающих несанкционированный доступ к ней.

Правила обработки ПДн субъектов ПДн, осуществляемой с использованием средств автоматизации, содержание ПДн

20. Безопасность ПДн, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного доступа к ПДн.

21. Уполномоченными должностными лицами при обработке ПДн в ИСПДн должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

22. Обмен ПДн при их обработке в ИСПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

23. Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи ПДн к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети Интернет, не допускается.

24. Доступ пользователей (операторов ИСПДн) к ПДн в ИСПДн должен требовать обязательного прохождения процедуры идентификации и аутентификации.

25. Структурными подразделениями управления (должностными лицами), ответственными за обеспечение безопасности ПДн при их обработке в ИСПДн, должно быть обеспечено:

1) своевременное обнаружение фактов несанкционированного доступа к ПДн и немедленное доведение этой информации до руководства;

2) недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

3) возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

4) постоянный контроль за обеспечением уровня защищенности ПДн;

5) знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

6) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;

7) при обнаружении нарушений правил предоставления ПДн незамедлительное приостановление предоставления ПДн пользователям ИСПДн до выявления причин нарушений и устранения этих причин;

8) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

26. В случае выявления нарушений правил обработки ПДн в ИСПДн уполномоченными должностными лицами принимаются меры по установлению причин нарушений и их устранению.

Правила обработки ПДн субъектов ПДн, осуществляемой без использования средств автоматизации

27. Обработка ПДн без использования средств автоматизации уполномоченным должностным лицом осуществляется на материальных (бумажных) носителях ПДн для целей, указанных в пунктах 8 и 9 настоящих Правил.

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

1) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, фамилию, имя, отчество и адрес субъекта ПДн, чьи ПДн вносятся в указанную типовую форму, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки;

2) типовая форма должна предусматривать поле, в котором субъекты ПДн могут поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, при необходимости получения согласия на обработку ПДн;

3) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, чьи ПДн содержатся в типовой форме, при ознакомлении со

своими ПДн, не имел возможности доступа к ПДн иных лиц, содержащимся в указанной типовой форме;

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

29. Уничтожение или обезличивание ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

30. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем изготовления нового материального носителя с уточненными ПДн.

Правила обработки ПДн работников управления

31. Обработка ПДн работников управления осуществляется с их письменного согласия, которое действует со дня их поступления на работу в управление в течение трудовой деятельности в управлении (приложение 3 к Правилам).

32. Лицо, уполномоченное на обработку ПДн работников управления (далее - специалист) обеспечивает защиту ПДн работников управления, содержащихся в личных делах, от неправомерного их использования или утраты.

33. Обработка ПДн работников управления осуществляется как с использованием средств автоматизации, так и без использования таких средств.

34. При обработке ПДн работников управления специалист обязан соблюдать следующие требования:

1) объем и характер обрабатываемых ПДн, способы обработки ПДн должны соответствовать целям обработки ПДн;

2) защита ПДн работников управления от неправомерного их использования или уничтожения обеспечивается в порядке, установленном нормативными правовыми актами Российской Федерации;

3) передача ПДн работников управления не допускается без письменного согласия работника управления (приложение 4 к Правилам), за исключением случаев, установленных федеральными законами. В случае если лицо, обратившееся с запросом, не обладает соответствующими полномочиями на получение ПДн работников управления, либо отсутствует письменное согласие работника управления на передачу его ПДн, специалист вправе отказать в предоставлении ПДн. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации;

4) обеспечение конфиденциальности ПДн работников управления, за исключением случаев обезличивания ПДн и в отношении общедоступных ПДн;

5) хранение ПДН должно осуществляться в форме, позволяющей определить работников управления и иное лицо, являющееся субъектом ПДн, не дольше, чем этого требуют цели их обработки. Указанные сведения подлежат уничтожению по достижении цели обработки или в случае утраты необходимости в их достижении, если иное не установлено законодательством Российской Федерации. Факт уничтожения ПДн оформляется соответствующим актом;

6) опубликование и распространение ПДн работников управления допускается в случаях, установленных законодательством Российской Федерации.

35. В целях обеспечения защиты ПДн работники управления вправе:

1) получать полную информацию о своих ПДн и способе обработки этих данных (в том числе автоматизированной);

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

3) требовать внесения необходимых изменений, уничтожения или блокирования соответствующих ПДн, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

4) обжаловать в порядке, установленном законодательством Российской Федерации, действия (бездействие) уполномоченных должностных лиц.

36. Управление в соответствии со статьей 33 Федерального закона от 02.03.2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации» вправе осуществлять обработку ПДн муниципальных служащих при формировании кадрового резерва.

37. Управление в соответствии со статьей 17 Федерального закона от 02.03.2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации» вправе осуществлять обработку ПДн кандидатов на замещение вакантных должностей муниципальной службы.

IV. Передача и хранение ПДн

38. При передаче ПДн субъектов управление должно соблюдать следующие требования:

1) не сообщать ПДн субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, установленных федеральным законом;

2) предупредить лиц, получивших ПДн субъектов, 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, получившие ПДн субъектов, обязаны соблюдать режим конфиденциальности.

Данные Правила не распространяются на обмен ПДн субъектов в порядке, установленном федеральными законами;

3) осуществлять передачу ПДн субъектов в пределах управления в соответствии с настоящим Правилами;

4) разрешать доступ к ПДн субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн субъектов, которые необходимы для выполнения конкретной функции;

5) передавать ПДн субъектов представителям в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми ПДн субъектов, которые необходимы для выполнения указанными представителями их функции;

6) не допускается отвечать на вопросы, связанные с передачей ПДн субъектов по телефону или факсу.

Хранение и использование ПДн

39. ПДн субъектов обрабатываются и хранятся на бумажных носителях в помещениях управления и на учтённых машинных носителях в соответствии с Инструкцией по учёту машинных носителей.

40. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде — в локальной компьютерной сети, в компьютерных программах и электронных базах данных.

41. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого является субъект ПДн. ПДн субъектов должны удаляться из ИСПДн управления по достижении целей обработки, при этом допускается хранить документы, содержащие ПДн, срок хранения которых регулирует Федеральный закон от 22 октября 2004 г. №125-ФЗ «Об архивном деле в Российской Федерации».

42. При получении ПДн не от субъекта (за исключением случаев, если ПДн были предоставлены управлению на основании федеральных законов или если ПДн являются общедоступными), управление до начала обработки таких ПДн обязана предоставить субъекту ПДн следующую информацию:

1) наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

2) цель обработки ПДн и ее правовое основание;

3) предполагаемые пользователи ПДн;

4) установленные Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» права субъекта ПДн.

43. В случае выявления неправомерной обработки ПДн, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в

срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению оператора. В случае если обеспечить правомерность обработки ПДн невозможно, оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн оператор обязан уведомить субъект ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

44. В случае достижения цели обработки ПДн оператор обязан прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных федеральными законами.

45. В случае отзыва субъектом ПДн согласия на обработку своих ПДн оператор обязан прекратить обработку ПДн и уничтожить ПДн в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом ПДн. Об уничтожении ПДн оператор обязан уведомить субъекта ПДн.

46. В случае отсутствия возможности уничтожения ПДн в течение сроков, указанных выше, оператор осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение ПДн в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

V. Доступ к ПДн

47. Перечень лиц, имеющих право доступа к ПДн, определяется списком лиц, которым необходим доступ к ПДн, утверждаемым приказом начальника управления. Начальник управления имеет право доступа ко всем ПДн. Доступ к ПДн может быть предоставлен иному сотруднику управления, должность которого не поименована в списке лиц, имеющих доступ к ПДн, если этого требует производственная необходимость и выполняемая им трудовая функция. Для этого работнику управления следует составить докладную записку на имя начальника управления с визой непосредственного руководителя.

48. Субъект ПДн, чьи ПДн обрабатываются в ИСПДн, имеет право:

1) получать доступ к своим ПДн и знакомиться с ними, включая право на безвозмездное получение копий любой записи, содержащей ПДн этого субъекта;

2) требовать от управления уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для оператора ПДн;

3) получать от оператора:

- сведения о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ;

- перечень обрабатываемых ПДн и источник их получения;

- сроки обработки ПДн, в том числе сроки их хранения;

- сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его ПДн.

4) требовать извещения оператором всех лиц, которым ранее были сообщены неверные или неполные ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях;

5) копировать и делать выписки ПДн субъекта разрешается исключительно в служебных целях с письменного разрешения начальника управления.

VI. Защита ПДн

49. Под угрозой или опасностью утраты ПДн 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.

50. 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.

51. Защита ПДн представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности ПДн и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе деятельности управления.

52. Защита ПДн от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральными законами.

«Внутренняя защита»

53. Основным виновником несанкционированного доступа к ПДн является, как правило, должностное лицо, работающее с документами и базами данных. Регламентация доступа работников управления к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами управления.

54. Для обеспечения внутренней защиты ПДн необходимо соблюдать ряд мер:

1) ограничение и регламентация состава работников управления, функциональные обязанности которых требуют конфиденциальных знаний;

2) строгое избирательное и обоснованное распределение документов и информации между работниками управления;

3) рациональное размещение рабочих мест работников управления, при котором исключалось бы бесконтрольное использование защищаемой информации;

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

5) наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

6) определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

7) организация правил уничтожения информации;

8) своевременное выявление нарушения требований разрешительной системы доступа работниками управления;

9) воспитательная и разъяснительная работа с работниками управления по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

10) если управлению оказывают услуги юридические и/или физические лица на основании заключенных гражданско-правовых договоров и в силу этих договоров они должны иметь доступ к ПДн работников управления, то соответствующие данные предоставляются только после подписания с ними соглашения об их неразглашении.

«Внешняя защита»

55. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

56. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности управления, 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 управлении.

57. Для обеспечения внешней защиты ПДн необходимо соблюдать ряд мер:

- правила приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и правила выдачи удостоверений;
- технические средства охраны, сигнализации;
- правила охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

58. Все лица, связанные с получением, обработкой и защитой ПДн, обязаны подписать обязательство о неразглашении ПДн (приложение 5 к Правилам).

59. По возможности ПДн обезличиваются.

60. Кроме мер защиты ПДн, установленных законодательством, управление и работники управления могут вырабатывать совместные меры защиты ПДн.

VII. Ответственность за нарушение норм, регулирующих обработку и защиту ПДн

61. Разглашение ПДн субъекта, то есть передача посторонним лицам, не имеющим к ним доступа; публичное раскрытие; утрата документов и иных носителей, содержащих ПДн субъекта; иные нарушения обязанностей по их защите, обработке и хранению, установленных настоящими Правилами, а также иными локальными нормативными актами управления, должностным лицом, ответственным за получение, обработку и защиту ПДн субъекта, влекут наложение на него дисциплинарного взыскания - выговора, увольнения.

62. В случае причинения ущерба управлению работник, имеющий доступ к ПДн субъектов и совершивший указанный дисциплинарный поступок, несет полную материальную ответственность в соответствии с п. 7 ч. 1 ст. 243 Трудового кодекса РФ.

63. Работник управления, имеющий доступ к ПДн субъектов и незаконно использовавший или разгласивший указанную информацию без согласия субъекта из корыстной или иной личной заинтересованности и тем самым причинивший крупный ущерб, несет уголовную ответственность на основании ст. 188 Уголовного кодекса РФ.

VIII. Процедуры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством

64. К процедурам, направленным на предотвращение и выявление нарушений законодательства в отношении обработки ПДн и устранение таких последствий относятся:

1) осуществление внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам;

2) оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

3) ознакомление работников управления, непосредственно осуществляющих обработку ПДн, с правилами законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику управления в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников управления.

65. Обеспечение безопасности ПДн достигается в частности:

1) определением угроз безопасности ПДн при их обработке в ИСПДн;

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

3) применением прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

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

5) учетом машинных носителей ПДн;

6) обнаружением фактов несанкционированного доступа к ПДн и принятием мер;

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

8) установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн.

Заместитель начальника управления Е.В. Клем

ПРИЛОЖЕНИЕ 1
к Правилам

Разъяснения
юридических последствий отказа в предоставлении своих персональных данных

Мне, _____
разъяснены юридические последствия отказа в предоставлении своих персональных данных управлению социальной защиты населения администрации Копейского городского округа.

В соответствии со статьями 16, 30 Федерального закона от 02 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации», Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденного Указом Президента Российской Федерации от 30 мая 2005 г. № 609, определен перечень персональных данных, которые я, как субъект персональных данных, обязан представить в управление социальной защиты населения администрации Копейского городского округа в связи с поступлением или прохождением муниципальной службы.

Мне, как субъекту персональных данных, разъяснено, что:

- без представления обязательных для заключения трудового договора документов и сведений, при предоставлении подложных документов или заведомо ложных сведений гражданин не может быть принят на муниципальную службу;

- на основании пункта 5 статьи 15 Федерального закона от 02 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации» непредставление муниципальным служащим сведений о своих доходах, об имуществе и обязательствах имущественного характера, а также о доходах, об имуществе и обязательствах имущественного характера своих супруги (супруга) и несовершеннолетних детей в случае, если представление таких сведений обязательно, либо представление заведомо недостоверных или неполных сведений является правонарушением, влекущим увольнение муниципального служащего с муниципальной службы.

«_____ »_____ 20 ___ г _____ _____
(дата) (подпись) (расшифровка подписи)

Разъяснения
юридических последствий отказа в предоставлении своих персональных данных

Мне, _____

разъяснены юридические последствия отказа в предоставлении своих персональных данных управлению социальной защиты населения администрации Копейского городского округа.

При поступлении на работу в управление социальной защиты населения администрации Копейского городского округа я, как субъект персональных данных обязан представить перечень информации о себе, определенный статьями 57, 65, 69 Трудового кодекса Российской Федерации.

Без представления обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

На основании пункта 11 части 1 статьи 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

«_____»_____ 20 ___ г _____ _____
(дата) (подпись) (расшифровка подписи)

ПРИЛОЖЕНИЕ 2
к Правилам

Управление социальной защиты населения администрации
Копейского городского округа

Начальнику отдела
_____
Ф.И.О.

Уведомление
о получении персональных данных от третьих лиц (пример)

Уважаемый _____!

В соответствии с Вашим заявлением об утрате трудовой книжки и просьбе оказать содействие в сборе сведений о предыдущих местах работы и периодах трудовой деятельности управление социальной защиты населения администрации Копейского городского округа запросит эти персональные данные от третьих лиц.

Цель запроса - подтверждение страхового стажа.

Сведения будут запрашиваться в письменной форме при помощи средств почтовой связи.

Просим Вас дать согласие на получение персональных данных от третьих лиц (п. 3 ст. 86 ТК РФ).

Согласие
на получение персональных данных от третьих лиц (пример)

Начальнику управления социальной
защиты населения администрации
Копейского городского округа
Щербе И.Г.
от начальника отдела
_____
Ф.И.О.
Паспорт_____
выдан_____,
зарегистрированного по адресу:
_____

Я, _____,
в соответствии со статьей 9 Федерального закона от 27.07.06 г. № 152-ФЗ «О персональных данных» настоящим даю согласие управлению социальной защиты населения администрации Копейского городского округа, расположенному по адресу: Челябинская обл., г. Копейск, ул.Ленина, 52, на получение моих персональных данных о предыдущих местах работы и периодах трудовой деятельности от третьих лиц.

Настоящее Согласие действует со дня его подписания до дня отзыва в письменной форме.

Дата, подпись

ПРИЛОЖЕНИЕ 3
к Правилам

СОГЛАСИЕ СУБЪЕКТА
на обработку персональных данных

№_____ «___»_____20__г.

Я, _____ ,
(фамилия, имя, отчество субъекта)
основной документ, удостоверяющий личность _____
_____
(номер, сведения о дате выдачи указанного документа и выдавшем его органе)
в дальнейшем «Субъект», даю согласие _____
_____
(наименование оператора персональных данных)
расположенным по адресу: _____
далее «Оператор», на обработку персональных данных на следующих условиях:

1. Субъект дает согласие на обработку Оператором своих персональных данных, то есть совершение, в том числе, следующих действий:
сбор, систематизацию, накопление, хранение, уточнение, использование, распространение, обезличивание, блокирование, уничтожение персональных данных
2. Оператор обязуется использовать данные Субъекта в целях целях исполнения отдельных государственных полномочий в сфере социальной защиты населения, решения вопросов местного значения в сфере социальных отношений.
3. Типовой перечень персональных данных, передаваемых Оператору на обработку Фамилия, имя, отчество, дата рождения; место рождения; биографические сведения; сведения о местах обучения, сведения о местах работы; сведения о родителях; сведения о доходах, сведения о месте регистрации, проживания; контактная информация; паспортные данные
4. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п.4 ст.14 ФЗ №152-ФЗ от 27.06.2006г.).
5. При поступлении Оператору письменного заявления Субъекта о прекращении действия Согласия, персональные данные уничтожаются установленным способом в: _____
(указать срок уничтожения персональных данных)
6. Настоящее разрешение действует в течение: _____
(указать срок хранения персональных данных субъекта)

Субъект _____ /_____/
(Подпись) (Ф.И.О.)

ПРИЛОЖЕНИЕ 4
к Правилам

Примерная форма
письменного согласия работника о передаче
его персональных данных третьим лицам

Начальнику управления социальной
защиты населения администрации
Копейского городского округа
Щербе И.Г.

_____
Ф.И.О.
Паспорт_____
выдан_____
_____,
зарегистрированного по адресу:
_____
_____
_____

ЗАЯВЛЕНИЕ

В целях осуществления бухгалтерского учета, персонифицированного учета в системе государственного пенсионного страхования, оформления полисов обязательного медицинского страхования, проведения профилактических прививок, воинского учета и в других целях, определенных законодательством Российской Федерации и связанных с моей трудовой деятельностью в управлении социальной защиты населения администрации Копейского городского округа в соответствии со статьей 88 Трудового кодекса Российской Федерации выражаю свое согласие на передачу третьим лицам следующих персональных данных: Ф.И.О., место работы, содержащиеся в документах сведения о трудовой деятельности, о стаже работы, дата рождения, адрес регистрации, паспортные данные, данные СНИЛС, данные ИНН.

Дата, подпись.

ПРИЛОЖЕНИЕ 5
к Правилам

ОБЯЗАТЕЛЬСТВО
о неразглашении информации, содержащей персональные данные

Я,_____,
(ФИО муниципального служащего)
исполняющий(ая) должностные обязанности по замещаемой должности
_____
_____
(должность, наименование структурного подразделения)

предупрежден(а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом, мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. После прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

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

_____ _____
(Подпись) (ФИО)

«_____»_____20__г.

Лист ознакомления

Дата ознакомления	ФИО сотрудника, ознакомившегося с документом	Должность сотрудника, ознакомившегося с документом	Подпись сотрудника, ознакомившегося с документом