УТВЕРЖДАЮ
Директор
МБУ «ДМО» городского
округа Жигулевск Самарской
области
«29» 12 2017 г.

ПОЛОЖЕНИЕ
о порядке обеспечения безопасности персональных данных в МБУ « ДМО» городского округа Жигулевск Самарской области

1. Общие положения.

1.1. Настоящее Положение о порядке обеспечения безопасности персональных данных в МБУ «ДМО» (далее – Положение) определяет меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в МБУ «ДМО» (далее –Учреждение).

1.2. Настоящее Положение разработано в соответствии с:

Федеральным законом «О персональных данных» (далее – Федеральный закон);

Федеральным законом «Об информации, информационных технологиях и о защите информации»;

Трудовым кодексом Российской Федерации:

Кодексом Российской Федерации об административных правонарушениях;

Федеральным законом «О муниципальной службе в Российской Федерации»,

Федеральным законом «О противодействии коррупции»;

Федеральным законом «Об организации предоставления государственных и муниципальных услуг»;

Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации»;

Указом Президента Российской Федерации от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;

постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее – Положение об особенностях обработки персональных данных);

постановлением Правительства Российской Федерации от 21.03.2012 № 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»;

постановлением Правительства Российской Федерации от 6.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

1.3. Настоящее Положение не распространяется на отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, и в случаях, предусмотренных действующим законодательством.

1.4. Обработка персональных данных в Учреждении осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в области персональных данных, и Положением о порядке обработки персональных данных.

1.5. В настоящем Положении используются основные понятия, определенные в Федеральном законе.

1.6. Положение является обязательным для исполнения всеми муниципальными служащими Учреждения (далее – работниками), имеющими доступ к персональным данным.

1.7. Обработку персональных данных в Учреждении осуществляют работники в соответствии со Списком лиц, допущенных к работе с персональными данными, утвержденным приказом директора Учреждения от 29.12.2017 №215, №217 от 29.12.2017

1.8. Работники, непосредственно осуществляющие обработку персональных данных, в случае расторжения с ними трудового договора(контракта) и прекращения обработки персональных данных, ставших известными им в связи с исполнением должностных обязанностей, подписывают соответствующее обязательство, типовая форма которого утверждена приказом директора Учреждения от _____ №_____.

2. Обеспечение безопасности обработки персональных данных

2.1. Обработка персональных данных в целях, указанных в Положении от «29» 12 2017г. № 215, осуществляется:

- главным бухгалтером;
- юрисконсультом;

- специалистом по работе с молодежью по трудоустройству несовершеннолетних.

и включают в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

2.2. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных лиц, указанных в Положении осуществляется путем:

2.2.1. Получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые в Учреждение) непосредственно от лиц, указанных в Положении;

2.2.2. Копирования оригиналов документов;

2.2.3. Внесения сведений в учетные формы (на бумажных и электронных носителях);

2.2.4. Формирования персональных данных в ходе кадровой работы;

2.2.5. Внесения персональных данных в ИСПДн АС

2.3. Запрещается получать, обрабатывать и приобщать к личному делу сотрудника Учреждения и лица, замещающего должность руководителя подведомственного учреждения, персональные данные, не предусмотренные п. 1 Перечня Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.4. Обработка персональных данных, необходимых в связи с предоставлением государственных и муниципальных услуг и исполнением муниципальных функций, осуществляется без согласия субъектов персональных данных.

2.5. Обработка персональных данных в Учреждении осуществляется в информационных системах персональных данных (далее – ИСПДн) на защищенных в соответствии с требованиями нормативных документов автоматизированных рабочих местах.

2.6. Автоматизированные рабочие места ИСПДн содержат персональные данные сотрудников Учреждения и предполагают обработку персональных данных в соответствии с п.1,2 Перечня Положения.

2.7. Обеспечение безопасности персональных данных, обрабатываемых в Учреждении, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

2.7.1. Определением угроз безопасности персональных данных при их обработке в ИСПДн Учреждения;

2.7.2. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн Учреждения, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных

данных;

2.7.3. Применением прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

2.7.4. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;

2.7.5. Учетом машинных носителей персональных данных;

2.7.6. Обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

2.7.7. Восстановлением персональных данных, модифицированных, удаленных или уничтоженных вследствие несанкционированного доступа к ним;

2.7.8. Установлением правил доступа к персональным данным, обрабатываемым в ИСПДн Учреждения;

2.7.9. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности ИСПДн;

2.7.10. Выполнением Порядка доступа муниципальных служащих Учреждения в помещения, в которых ведется обработка персональных данных, утвержденного приказом директора Учреждения;

2.8. Для обеспечения соответствующего уровня защищенности персональных данных при их обработке в ИСПДн приказом директора Учреждения назначается должностное лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн.

2.9. Должностное лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн, руководствуется Инструкцией ответственному за обеспечение безопасности персональных данных.

2.10. Обеспечение безопасности персональных данных в ИСПДн без использования средств автоматизации осуществляется в соответствии с настоящим Положением, в том числе путем хранения материальных носителей информации в закрываемых шкафах, ящиках, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

2.11. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

2.12. При неавтоматизированной обработке персональных данных на бумажных носителях:

не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

персональные данные должны обособляться от иной информации, в частности, путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков).

2.13. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться условия, утвержденные приказом директора Учреждения от « » _____ 2017г.

2.14. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляет системный администратор Учреждения.

2.15. Обработка персональных данных без использования средств автоматизации в электронном виде осуществляется, на внешних электронных носителях информации. При отсутствии технологической возможности осуществления обработки персональных данных в электронном виде без использования средств автоматизации на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

3. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

3.1. Системным администратором Учреждения, ответственным за документооборот и архивирование, осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

3.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании комиссии по защите персональных данных, проверке обработки и уничтожению документов с персональными данными.

По итогам заседания составляются протокол и Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами комиссии Учреждения и утверждается директором Учреждения.

3.3. Уничтожение документов, содержащих персональные данные, проводится с использованием уничтожителей документов (шредеров). Возможно уничтожение в подрядной организации, имеющей необходимую производственную базу для обеспечения установленного порядка уничтожения документов. Члены комиссии, сопровождают документы, содержащие персональные данные, до производственной базы подрядчика и присутствуют при процедуре уничтожения документов (сжигание или химическое уничтожение).

4.4. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной

информации.

4.5. По окончании процедуры уничтожения, членами комиссии, производившими уничтожение, или представителем подрядной организации (в случае уничтожения в подрядной организации), составляется соответствующий Акт об уничтожении документов, содержащих персональные данные.