УТВЕРЖДАЮ

Директор
ГБУ РК «ЦСО Ленинского района»

_____ Е.А. Гуменюк

«____» _____ 201_ г.

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В *ГБУ РК ЦСО «Ленинского района»*

2019 г.

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»**,** Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»**,** Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»**,** Приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», и определяет правила и условия обработки персональных данных в *ГБУ РК ЦСО «Ленинского района»* (далее - Организация).

1.2. Организация является оператором персональных данных, самостоятельно или совместно с другими лицами организующим и (или) осуществляющим обработку персональных данных субъектов персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.3. Цели обработки персональных данных.

- сбор
- уточнение
- использование

2. Правила обработки персональных данных

2.1. Обработка персональных данных осуществляется с письменного согласия субъектов персональных данных, которое действует со дня их поступления на работу и на время ее прохождения, при подаче заявлений от физических лиц на срок указанный в соответствующих нормативно правовых актах, так и без использования таких средств.

2.2. Руководитель Организации обеспечивает защиту персональных данных, содержащихся в базах данных, от неправомерного их использования или утраты.

2.3. Персональные данные и иные сведения, содержащиеся в базах данных персональных данных, относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации).

2.4. При обработке персональных данных в целях реализации возложенных на организацию полномочий лица, допущенные к обработке персональных данных (далее - уполномоченные должностные лица), обязаны соблюдать следующие требования:

а) объем и характер обрабатываемых персональных данных, способы обработки персональных данных должны соответствовать целям обработки персональных данных;

б) защита персональных данных от неправомерного их использования или уничтожения обеспечивается в порядке, установленном нормативными правовыми актами Российской Федерации;

в) передача персональных данных не допускается без письменного согласия субъекта персональных данных, за исключением случаев, установленных федеральными законами. В случае если лицо, обратившееся с запросом, не обладает соответствующими полномочиями на получение персональных данных либо отсутствует письменное согласие субъекта персональных данных на передачу его персональных данных, Организация вправе отказать в предоставлении персональных данных. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации;

г) обеспечение конфиденциальности персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

д) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, 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 персональных данных оформляется актом;

е) опубликование и распространение персональных данных допускается в случаях, установленных законодательством Российской Федерации.

2.5. Обработка биометрических персональных данных и специальных категорий персональных данных в Организации не производятся.

2.6. В целях обеспечения защиты персональных данных субъекты персональных данных вправе:

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

б) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, за исключением случаев, предусмотренных Федеральным законом «О персональных данных»;

в) требовать внесения необходимых изменений, уничтожения или блокирования персональных данных, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

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

2.7. Организация в рамках трудового законодательства вправе осуществлять обработку (в том числе автоматизированную) персональных данных граждан при формировании кадрового состава.

2.8. Трансграничная передача персональных данных на территории Российской федерации и иностранных государств не производится.

2.9. Организация в соответствии с Федеральным Законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» вправе осуществлять обработку (в том числе автоматизированную) персональных данных иных лиц с их согласия.

3. Правила обработки персональных данных, осуществляемой без использования средств автоматизации

3.1. Обработка персональных данных без использования средств автоматизации осуществляется, как на бумажных носителях, так и в электронном виде на материальных носителях информации.

3.2. Неавтоматизированная обработка персональных данных в электронном виде должна осуществляться на съемных материальных носителях информации.

3.3. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на съемных материальных носителях информации необходимо принимать организационные (охрана помещений) и технические (установка сертифицированных средств защиты информации) меры, исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

3.4. Учет материальных носителей информации, содержащих персональные данные, осуществляется ответственным лицом.

3.5. При обработке персональных данных без использования средств автоматизации уполномоченными должностными лицами не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы.

3.6. Обработка персональных данных на бумажных носителях осуществляется в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а так же с учетом локальных актов организации.

3.7. При разработке и использовании типовых форм документов, необходимых для реализации возложенных на организацию полномочий, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

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

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

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, чьи персональные данные содержатся в типовой форме, при ознакомлении со своими персональными данными не имел возможности доступа к персональным данным других лиц, содержащихся в указанной типовой форме;

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

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

3.9. Уточнение персональных данных при их обработке без использования средств автоматизации производится путем изготовления нового материального носителя с уточненными персональными данными.

4. Правила обработки персональных данных в информационных системах персональных данных

4.1. Обработка персональных данных в информационных системах персональных данных осуществляется после завершения работ по созданию системы защиты персональных данных в информационной системе, проверки ее комиссией, назначаемой приказом (наименование организации), и оценки соответствия информационной системы персональных данных требованиям безопасности информации.

4.2. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

4.3. Выбор методов и способов защиты информации в информационных системах персональных данных осуществляется в соответствии с Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» на основе угроз безопасности персональных данных (модели угроз) в зависимости от требуемого уровня защищенности информационной системы персональных данных.

Модель угроз разрабатывается на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных

данных» утвержденной Федеральной службой по техническому и экспортному контролю 15 февраля 2008 г и других документов в области защиты персональных данных.

4.4. Уровень защищенности информационной системы персональных данных определяется в соответствии с Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.5. Определение (пересмотр) требуемого уровня защищенности информационной системы персональных данных проводится комиссией организации с привлечением специалистов по обеспечению безопасности информации на этапе создания или в ходе эксплуатации информационной системы.

4.6. Разрешением на обработку персональных данных в организации является приказ о вводе в эксплуатацию объекта информатизации (ОИ), который издается на основании положительных выводов комиссии и результатов оценки соответствия требованиям безопасности информации.

4.7. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

4.8. Персональные данные могут быть предоставлены для ознакомления:

а) сотрудникам, допущенным к обработке персональных данных с использованием средств автоматизации, в части, касающейся их должностных обязанностей;

б) уполномоченным работникам федеральных органов исполнительной власти в порядке, установленном законодательством Российской Федерации.

4.9. Уполномоченными должностными лицами при обработке персональных данных в информационных системах персональных данных обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

4.10. Обмен персональными данными при их обработке в информационной системе осуществляется по каналам связи, защита которых обеспечивается путем реализации организационных мер и путем применения программных и технических средств.

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

4.12. Доступ пользователей к персональным данным в информационной системе персональных данных разрешается после обязательного прохождения процедур идентификации и аутентификации.

4.13. Должностными лицами Организации, ответственными за обработку и безопасность персональных данных при их обработке в информационных системах, должно быть обеспечено:

а) своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации руководителю Организации;

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

в) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) постоянный контроль за обеспечением уровня защищенности персональных данных;

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

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;

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

4.14. В случае выявления нарушений порядка обработки персональных данных в информационных системах Организации ответственными должностными лицами принимаются меры по установлению причин нарушений и их устранению.

5. Правила допуска и доступа к персональным данным

5.1. Уполномоченные должностные лица допускаются к информации, содержащей персональные данные, в соответствии с занимаемой должностью и в объеме, необходимом для выполнения ими должностных обязанностей на основании распоряжения.

5.2. Допуск к персональным данным разрешается руководителем Организации с соблюдением требований настоящего Положения.

5.3. Фактом ознакомления с разрешением на допуск к персональным данным является подпись уполномоченного должностного лица в листе ознакомления с распоряжением.

5.4. Доступ уполномоченных должностных лиц к персональным данным в информационной системе осуществляется после прохождения процедуры, установленной в п. 4.12 настоящего Положения.

5.5. В соответствии с частью 3 статьи 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» Организация вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных

данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного контракта, либо на основании правового акта организации.

Лицо, осуществляющее обработку персональных данных по поручению организации, обязано соблюдать принципы и правила обработки персональных данных.

5.6. В поручении (правовом акте, контракте, договоре, соглашении) организации должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

5.7. Допуск к персональным данным, в том числе содержащимся в информационной системе персональных данных сторонних организаций, деятельность которых не связана с исполнением функций организации, регламентируется законодательством Российской Федерации, контрактами (договорами, соглашениями) и другими нормативными и правовыми актами Российской Федерации.

5.8. Доступ к техническим (программно-техническим) средствам информационной системы Организации предоставляется сторонним организациям, выполняющим работы на договорной основе.

Порядок допуска указанных организаций определяется в договоре на выполнение работ (оказание услуг). Решением о допуске является подписанный в установленном порядке договор на выполнение работ (оказание услуг).

5.9. Доступ к персональным данным сторонних организаций осуществляется на основании письменных запросов или письменных соглашений (договоров) сторон об обмене информацией.

В письменном запросе (соглашении, договоре) должны быть указаны следующие сведения:

цель получения информации;

конкретное наименование информации (состав персональных данных);

способ доступа (предоставления), а также сведения о регистрации в уполномоченных органах по защите прав субъектов персональных данных, осуществляющих функции по контролю и надзору в сфере информационных технологий и связи.

При наличии соглашения со сторонней организацией о допуске к персональным данным (предоставлении информации) доступ к персональным данным осуществляется в порядке, указанном в подписанном соглашении (договоре).

5.10. Доступ к персональным данным, в том числе содержащимся в информационной системе персональных данных сторонних организаций,

выполняющих работы на договорной основе, осуществляется на основании подписанного договора на оказание услуг, а также настоящего Положения.

5.11. Запрещается передача электронных копий баз данных, содержащих персональные данные, любым сторонним организациям, за исключением случаев, предусмотренных законодательством Российской Федерации.

Ответственный за защиту информации -
_____
_____
_____ _____