Приложение к
Приказу МБУ
«ЦБС городского округа Сызрань»
от 01.12.2022г № 148

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В МБУ «ЦБС ГОРОДСКОГО ОКРУГА СЫЗРАНЬ»

I. Общие положения

1.1. Настоящая политика в отношении обработки и защиты персональных данных в МБУ «ЦБС городского округа Сызрань» (далее – Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее – Закон о ПДн) и является основополагающим внутренним регулятивным документом МБУ «ЦБС городского округа Сызрань» (далее – Учреждение), определяющим ключевые направления ее деятельности в области обработки и защиты персональных данных (далее – ПДн), оператором которых является Учреждение.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Учреждении, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Учреждением как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных настоящая Политика публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на сайте Учреждения.

II. Основные понятия используемые в документе

Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу

(распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Персональные данные, разрешенные субъектом персональных данных для распространения – это персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

Оператор персональных данных (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Оператором является МБУ «ЦБС городского округа Сызрань» расположенное по адресу: г. Сызрань, ул. Советская, 92.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (предоставление, доступ);
- распространение;
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

III. Общие принципы, основания и цель обработки персональных данных, обрабатываемых в Учреждении

3.1. Обработка персональных данных граждан и работников осуществляется на основе принципов:

1) обработка персональных данных должна осуществляться на законной и справедливой основе;

2) обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

3) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

4) обработке подлежат только персональные данные, которые отвечают целям их обработки;

5) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

6) при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Учреждение должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

7) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей

обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Правовым основанием обработки персональных данных является совокупность нормативных правовых актов Российской Федерации, во исполнение которых и в соответствии с которыми Учреждение осуществляет обработку персональных данных, в том числе:

- Конституция Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Федеральный закон от 06.12.2011 N 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 15.12.2001 N 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;
- Устав МБУ «ЦБС городского округа Сызрань»;
- договоры, заключаемые между Оператором и субъектами персональных данных;
- Согласие на обработку персональных данных

3.3. Обработка ПДн в Учреждении осуществляется:

1) с целью реализации прав и обязанностей Учреждения как юридического лица. Обрабатываются ПДн физических лиц, в том числе являющихся контрагентами (возможными контрагентами) Учреждения по гражданско-правовым договорам, ПДн руководителей, и представителей юридических лиц, ПДн иных физических лиц, представленные участниками закупки, физических лиц, ПДн которых используются для осуществления пропускного режима в занимаемых Учреждением помещениях;

2) с целью реализации прав граждан в соответствии с Федеральным законом от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

3) при обращении граждан для получения муниципальных услуг и осуществления муниципальных функций;

4) в связи с деятельностью Учреждения, освещаемой на официальном сайта Учреждения;

3.4. В целях исполнения возложенных на Учреждение функций Учреждение в установленном порядке вправе поручить обработку ПДн третьим лицам.

В договоры с лицами, которым Учреждение поручает обработку ПДп, включаются условия, обязывающие таких лиц соблюдать предусмотренные законодательством требования к обработке и защите ПДн.

3.5. Учреждение предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

IV. Принципы обеспечения безопасности персональных данных

4.1. Основной задачей обеспечения безопасности ПДн при их обработке в Учреждении является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

4.2. Для обеспечения безопасности ПДн Учреждение руководствуется следующими принципами:

1) законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2) системность: обработка ПДн в Учреждении осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Учреждения (далее – ИС) и других имеющихся в Учреждении систем и средств защиты;

4) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

6) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Учреждении с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

7) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

8) минимизация прав доступа: доступ к ПДн предоставляется работникам только в объеме, необходимом для выполнения их должностных обязанностей;

9) гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Учреждения (далее – ИСПДн), а также объема и состава обрабатываемых ПДн;

10) открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн Учреждения (далее – СЗПДн) не дают возможности преодоления имеющихся в Учреждении систем защиты возможными нарушителями безопасности ПДн;

11) научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

12) специализация и профессионализм: реализация мер по обеспечению

безопасности ПДн и эксплуатация СЗПДн осуществляются работниками, имеющими необходимые для этого квалификацию и опыт;

13) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Учреждения предусматривает тщательный подбор персонала и мотивацию работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Учреждения до заключения договоров;

14) наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

15) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

V. Доступ к обрабатываемым персональным данным

5.1. Доступ к обрабатываемым в Учреждении ПДн имеют лица, уполномоченные распоряжением Учреждения, в соответствии с Перечнем должностей МБУ «ЦБС городского округа Сызрань», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, лица, которым Учреждение поручило обработку ПДн на основании заключенного договора, а также лица, чьи ПДн подлежат обработке.

5.2. Доступ работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Учреждения.

Допущенные к обработке ПДн работники под роспись знакомятся с документами Учреждения, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных работников.

5.3. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Учреждением, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Учреждения.

VI. Реализуемые требования к защите персональных данных

6.1. Учреждение принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Законом о ПДн и принятыми в соответствии с ним нормативными правовыми актами, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

6.2. Состав указанных в пункте 5.1 Политики мер, включая их содержание и выбор средств защиты ПДн, определяется, а внутренние регулятивные документы об обработке и защите ПДн утверждаются (издаются) Учреждением исходя из требований:

Закона о ПДн;

главы 14 Трудового кодекса Российской Федерации;

постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

приказа ФСТЭК России 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";

постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

постановления Правительства Российской Федерации РФ от 6 июля 2008 г. № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";

иных нормативных правовых актов Российской Федерации об обработке и защите ПДн.

6.3. В предусмотренных законодательством случаях обработка ПДн осуществляется Учреждением с согласия субъектов ПДн.

Учреждением производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

6.4. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше чем этого требуют цели обработки ПДн, если срок хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

6.5. Учреждением осуществляется ознакомление работников Учреждения, непосредственно осуществляющих обработку ПДн, с положениями законодательства о ПДн, в том числе требованиями к защите ПДн, Политикой и иными внутренними регулятивными документами по вопросам обработки ПДн, и (или) обучение указанных работников по вопросам обработки и защиты ПДн.

6.6. При обработке ПДн с использованием средств автоматизации Учреждением, в частности, применяются следующие меры:

1) назначается ответственное лицо за организацию обработки ПДн;

2) утверждаются (издаются) внутренние регулятивные документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;

3) осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн Закону о ПДн и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике и внутренним

регулятивным документам Учреждения;

4) проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Закона о ПДн, определяется соотношение указанного вреда и принимаемых Учреждением мер, направленных на обеспечение исполнения обязанностей, предусмотренных Законом о ПДн.

6.7. Обеспечение безопасности ПДн в Учреждении при их обработке в ИСПДн достигается в Учреждении, в частности, путем:

1) определения угроз безопасности ПДн. Тип актуальных угроз безопасности ПДн и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;

2) определения в установленном порядке состава и содержания мер по обеспечению безопасности ПДн, выбора средств защиты информации.

3) применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших процедуру оценки соответствия в установленном порядке, когда применение таких средств необходимо для нейтрализации актуальных угроз.

В Учреждении, в том числе, осуществляются:

оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

учет машинных носителей ПДн, обеспечение их сохранности;

обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер;

восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

установление правил доступа к обрабатываемым ПДн, а также обеспечение регистрации и учета действий, совершаемых с ПДн;

организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

контроль за принимаемыми мерами по обеспечению безопасности ПДн, уровня защищенности ИСПДн.

6.8. Обеспечение защиты ПДн в Учреждении при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

1) обособления ПДн от иной информации;

2) недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;

3) использования отдельных материальных носителей для обработки каждой категории ПДн;

4) принятия мер по обеспечению раздельной обработки ПДн при несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же

носителе ПДн;

5) соблюдения требований:

к раздельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;

уточнению ПДн;

уничтожению или обезличиванию части ПДн;

использованию типовых форм документов, характер информации в которых предполагается или допускается включение в них ПДн;

ведению журналов, содержащих ПДн, необходимых для выдачи однократных пропусков субъектам ПДн в занимаемые Учреждением здания и помещения;

хранению ПДн, в том числе к обеспечению раздельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.