



ФЕДЕРАЛЬНАЯ ТЕРРИТОРИЯ  
«СИРИУС»

МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ «ЦИФРА.ФТ»  
(МКУ «Цифра.ФТ»)

## ПРИКАЗ

26.03.2026

Ц/101/02-23/17

пгт. Сириус

### Об утверждении локальных нормативных актов в сфере защиты и обработки персональных данных в муниципальном казенном учреждении «Цифра.ФТ»

В соответствии с главой 14 Трудового кодекса Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», необходимостью соблюдения законодательства в области защиты персональных данных в муниципальном казенном учреждении «Цифра.ФТ» (далее – МКУ «Цифра.ФТ»),

#### ПРИКАЗЫВАЮ:

1. Утвердить Правила обработки персональных данных в МКУ «Цифра.ФТ» согласно приложению № 1 к настоящему приказу.
2. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных согласно приложению № 2 к настоящему приказу.
3. Утвердить Правила доступа в помещения МКУ «Цифра.ФТ» в которых ведётся обработка защищаемой информации, в том числе персональных данных согласно приложению № 3 к настоящему приказу.
4. Утвердить Правила работы с обезличенными персональными данными в МКУ «Цифра.ФТ» согласно приложению № 4 к настоящему приказу.
5. Утвердить Правила рассмотрения запросов субъектов персональных данных, или их представителей в МКУ «Цифра.ФТ» согласно приложению № 5 к настоящему приказу.
6. Утвердить Перечень должностей в МКУ «Цифра.ФТ», замещение

которых предусматривает осуществление обработки, хранения, либо доступа к персональным данным согласно приложению № 6 к настоящему приказу.

7. Утвердить Перечень должностей в МКУ «Цифра.ФТ», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных согласно приложению № 7 к настоящему приказу.

8. Утвердить типовую форму обязательства работника МКУ «Цифра.ФТ», непосредственно осуществляющего обработку персональных данных согласно приложению № 8 к настоящему приказу.

9. Утвердить типовую форму согласия субъекта персональных данных на обработку персональных данных согласно приложению № 9 к настоящему приказу.

10. Утвердить типовую форму согласия субъекта персональных данных на распространение (предоставление, передачу) персональных данных третьим лицам согласно приложению № 10 к настоящему приказу.

11. Утвердить типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные согласно приложению № 11 к настоящему приказу.

12. Утвердить типовую форму согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения согласно приложению № 12 к настоящему приказу.

12. Утвердить Перечень информационных систем, в которых осуществляется обработка персональных данных в МКУ «Цифра.ФТ» согласно приложению № 13 к настоящему приказу.

13. Утвердить Перечень персональных данных, обрабатываемых в МКУ «Цифра.ФТ» согласно приложению № 14 к настоящему приказу.

14. Специалисту по организационному и документационному обеспечению управления организацией МКУ «Цифра.ФТ» обеспечить ознакомление с настоящим приказом сотрудников МКУ «Цифра.ФТ».

15. Специалисту по управлению персоналом МКУ «Цифра.ФТ» обеспечивать получение согласий на обработку персональных данных у субъектов персональных данных при их трудоустройстве в МКУ «Цифра.ФТ».

16. Настоящий приказ вступает в силу со дня его подписания.

17. Контроль за исполнением настоящего приказа возложить на ответственное лицо за организацию обработки персональных данных в МКУ «Цифра.ФТ».

Директор



Л.В. Мартыненко

Приложение № 1 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № ц/01/02-23/17

УТВЕРЖДЕНЫ  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № ц/01/02-23-17

Правила  
обработки персональных данных  
в муниципальном казенном учреждении «Цифра.ФТ»

1. Общие положения

1.1. Настоящие Правила обработки персональных данных в муниципальном казенном учреждении «Цифра.ФТ» (далее – Правила) определяют цели и общие принципы обработки персональных данных, для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований, процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в сфере защиты персональных данных, а также реализуемые в муниципальном казенном учреждении «Цифра.ФТ» (далее – Учреждение) меры защиты персональных данных.

1.2. Настоящие Правила разработаны в соответствии с:

- Конституцией Российской Федерации;
- Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);
- постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите

персональных данных при их обработке в информационных системах персональных данных».

1.3. Настоящие Правила являются обязательными для ознакомления работникам Учреждения, непосредственно обрабатывающих персональные данные и/или осуществляющих доступ к персональным данным при выполнении своих должностных обязанностей.

1.4. Настоящие Правила являются публичным документом Учреждения и предназначены для ознакомления неограниченного круга лиц.

1.5. Основные термины и определения, используемые в Правилах, соответствуют терминам и определениям, определенным Федеральным законом «О персональных данных».

## 2. Основные права Учреждения

2.1. Учреждение оставляет за собой право проверять полноту и точность предоставленных персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. В случае выявления ошибочных или неполных персональных данных, Учреждение имеет право прекратить все отношения с субъектом персональных данных.

2.2. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных, полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Учреждением.

2.3. Персональные данные могут быть получены Учреждением от лица, не являющегося субъектом персональных данных, при условии предоставления Учреждением подтверждения наличия оснований, указанных в Федеральном законе «О персональных данных».

2.4. В случае отзыва субъектом персональных данных согласия на обработку персональных данных, Учреждение вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона «О персональных данных».

2.5. Учреждение вправе отказать субъекту персональных данных в выполнении запроса на доступ к своим персональным данным, не соответствующего условиям, предусмотренные частями 4 и 5 статьи 14 Федерального закона «О персональных данных». Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Учреждении.

2.6. Учреждение вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством, на основании заключаемого с этим лицом договора, в том числе государственного (муниципального) контракта, либо путем принятия Учреждением

соответствующего локального акта (далее - поручение Учреждения). В случаях, когда Учреждение поручает обработку персональных данных третьему лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Учреждение. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, несет ответственность перед Учреждением.

### 3. Основные обязанности Учреждения

3.1. Учреждение при обработке персональных данных обязано принимать необходимые нормативные, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. Учреждение до начала обработки персональных данных обязано уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона «О персональных данных».

3.3. Учреждение назначает ответственного за организацию обработки персональных данных.

3.4. Учреждение не собирает персональные данные, не обрабатывает и не передает персональные данные субъектов персональных данных третьим лицам, без согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством.

3.5. Учреждение, работники Учреждения, получившие доступ к персональным данным, обязаны обеспечивать режим конфиденциальности персональных данных – не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3.6. В случаях обезличивания персональных данных Учреждение обеспечивает режим конфиденциальности по отношению к дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания. Обезличенные персональные данные хранятся отдельно от такой информации.

3.7. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных, Учреждение осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим

по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки.

3.8. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его законного представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, Учреждение осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.9. В случае подтверждения факта неточности персональных данных, Учреждение, на основании сведений, представленных субъектом персональных данных или его законным представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные, либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в течение 7 рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

3.10. В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение в срок, не превышающий 3 рабочих дней с даты этого выявления, осуществляет прекращение неправомерной обработки персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению Учреждения.

3.11. В случае если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, осуществляет уничтожение таких персональных данных или обеспечивает их уничтожение. Решение о неправомерности обработки персональных данных и необходимости уничтожения персональных данных принимает ответственный за организацию обработки персональных данных в Учреждении, который доводит соответствующую информацию до руководства. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение субъекта персональных данных или его законного представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.12. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных,

повлекшей нарушение прав субъектов персональных данных, Учреждение обязано с момента выявления такого инцидента Учреждением, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

3.13. В случае достижения цели обработки персональных данных Учреждение прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

3.14. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Учреждение прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных, либо если Учреждение не вправе осуществлять обработку персональных

данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

3.15. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение вносит в них необходимые изменения.

3.16. В срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Учреждение уничтожает такие персональные данные. При этом Учреждение уведомляет субъекта персональных данных или его законного представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.17. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше по тексту в настоящем разделе, Учреждение осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и обеспечивает уничтожение персональных данных в срок не превышающий 6 месяцев, если иной срок не установлен федеральными законами.

#### 4. Обязанности ответственного за обработку персональных данных

4.1. Лицо, ответственное за организацию обработки персональных данных определяется приказом директора Учреждения, получает указания непосредственно от него и подотчетно ему.

4.2. Лицо, ответственное за организацию обработки персональных данных, обязано:

4.2.1. организовывать принятие мер, необходимых для обеспечения защиты обрабатываемых персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;

4.2.2. осуществлять внутренний контроль за соблюдением требований законодательства в области персональных данных, в том числе требований к защите персональных данных;

4.2.3. обеспечить доведение до сведения лиц, непосредственно связанных с реализацией настоящих Правил, положений законодательства в области персональных данных, иных локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

4.2.4. организовать прием и обработку обращений (запросов) субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений (запросов);

4.2.5. в случае нарушения требований к защите персональных данных, принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

4.3. Лицо, ответственное за организацию обработки персональных данных, вправе:

4.3.1. в установленном порядке привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, в том числе для проведения внутренних проверок работников Учреждения, а также инициировать возложение на них соответствующих обязанностей и закреплением ответственности (по согласованию с директором Учреждения);

4.3.2. иметь доступ к информации, касающейся обработки персональных данных и включающей:

- цели обработки персональных данных;
- категории обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовые основания обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых способов обработки персональных данных;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- дату начала обработки персональных данных;
- срок или условия прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

## 5. Основные права субъекта персональных данных

5.1. Субъект персональных данных принимает решение о предоставлении Учреждению своих персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

5.2. Субъект персональных данных вправе отозвать согласие на обработку персональных данных, направив в адрес Учреждения письменное заявление в произвольной форме, содержащее:

- фамилия, имя, отчество (при наличии) субъекта персональных данных;
- перечень персональных данных, согласие на обработку которых отзывается;
- обоснование причин отзыва согласия на обработку персональных данных;

- дату направления заявления и подпись субъекта персональных данных.

5.3. В целях обеспечения своих законных интересов субъект персональных данных или его представитель имеет право:

- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом «О персональных данных»;

- требовать уточнение его персональных данных, их блокирование или уничтожение в случаях, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. Субъект персональных данных при отказе Учреждением исключить или исправить, заблокировать или уничтожить его персональные данные имеет право заявить в письменной форме о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект персональных данных имеет право дополнить заявлением, выражающим его собственную точку зрения;

- требовать от Учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные, устаревшие, неточные, незаконно полученные или не являющиеся необходимыми для заявленной цели обработки персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них, в том числе блокирование или уничтожение этих данных третьими лицами;

- обжаловать в суде или в уполномоченном органе по защите прав субъектов персональных данных любые неправомерные действия или бездействие Учреждения при обработке и защите персональных данных субъекта персональных данных, если субъект персональных данных считает, что Учреждение осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы.

5.4. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Учреждения или направить ему повторный запрос в целях получения сведений и ознакомления с персональными данными не ранее, чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

5.5. Субъект персональных данных вправе обратиться повторно до истечения 30-дневного срока в случае, если сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

## 6. Принципы, цели, условия и порядок обработки персональных данных и соответствующие им перечни обрабатываемых данных

6.1. Обработка персональных данных Учреждением осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в области персональных данных:

- обработка персональных данных осуществляется на законной и справедливой основе;

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

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

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

- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки;

- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных, принимаются необходимые меры, либо обеспечивается их принятие по удалению или уточнению неполных или неточных данных;

- хранение персональных данных осуществляется 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.

6.2. Обработка персональных данных Учреждением выполняется с использованием средств автоматизации или без использования таких средств и включает сбор, запись, систематизацию, накопление, хранение, уточнение

(обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных субъектов персональных данных, персональные данные которых обрабатываются Учреждением.

6.3. Обработка персональных данных без использования средств автоматизации может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

6.4. К субъектам персональных данных, персональные данные которых обрабатываются Учреждением, в соответствии с настоящими Правилами относятся:

- 1) работники Учреждения;
- 2) члены семей работников Учреждения, в случаях, предусмотренных законодательством Российской Федерации;
- 3) бывшие работники Учреждения и члены их семей, в случаях, предусмотренных законодательством Российской Федерации;
- 4) соискатели на вакантные должности;
- 5) граждане Российской Федерации, обратившиеся в соответствии с Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее – Федеральный закон «Об обращении граждан»);
- 6) граждане Российской Федерации – участники информационного обмена (пользователи информационных систем), персональные данные которых обрабатываются в информационных системах, оператором которых является Учреждение;
- 7) физические лица, пребывающие на территории Учреждения.

6.5. Обработка персональных данных лиц, указанных в подпунктах 1-5 пункта 6.4 настоящих Правил, в соответствии с пунктом 2 части 1 статьи 6 Федерального закона «О персональных данных» осуществляется без согласия субъекта персональных данных на обработку его персональных данных для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Учреждение функций, полномочий и обязанностей.

6.6. Обработка персональных данных лиц, указанных в подпунктах 6 и 7 пункта 6.4 настоящих Правил, в соответствии с пунктом 2 части 1 статьи 6 Федерального закона «О персональных данных» осуществляется с письменного согласия субъекта персональных данных на обработку его персональных данных.

6.7. Персональные данные субъектов персональных данных, указанных в подпунктах 1-3 пункта 6.4 настоящих Правил, обрабатываются в целях ведения кадрового и бухгалтерского учета.

6.8. Персональные данные субъектов персональных данных, указанных в подпункте 4 пункта 6.4 настоящих Правил, обрабатываются в целях подбора персонала (соискателей на вакантные должности).

6.9. Персональные данные субъектов персональных данных, указанных в подпункте 5 пункта 6.4 настоящих Правил, обрабатываются в целях рассмотрения обращения граждан.

6.10. Персональные данные субъектов персональных данных, указанных в подпункте 6 пункта 6.4 настоящих Правил, обрабатываются в целях предоставления доступа пользователей к информационным системам Учреждения, а также обработке информации в соответствии с целями создания (функционирования) информационной системы.

6.11. Персональные данные субъектов персональных данных, указанных в подпунктах 7 пункта 6.4 настоящих Правил, обрабатываются в целях обеспечения пропускного режима на территорию Учреждения.

6.12. В целях, указанных в пункте 6.7 настоящих Правил, обрабатываются следующие категории персональных данных субъектов персональных данных, указанных в подпунктах 1-3 пункта 6.4 настоящих Правил:

- фамилия, имя, отчество;
- год рождения;
- месяц рождения;
- дата рождения;
- место рождения;
- семейное положение;
- доходы;
- адрес электронной почты;
- адрес места жительства;
- адрес регистрации;
- номер телефона;
- СНИЛС;
- ИНН;
- гражданство;
- данные документа, удостоверяющего личность;
- реквизиты банковской карты;
- номер расчетного счета;
- номер лицевого счета;
- профессия;
- должность;
- сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);
- отношение к воинской обязанности, сведения о воинском учете; сведения об образовании;
- фотография для карточки Т2;
- сведения о составе семьи;
- реквизиты свидетельств государственной регистрации актов гражданского состояния и содержащиеся в них сведения;

- сведения об образовании (наименование образовательной и (или) иной организации, год окончания, уровень профессионального образования, реквизиты документов об образовании, направление подготовки, специальность и квалификация по документу об образовании, ученая степень, ученое звание (дата присвоения, реквизиты диплома, аттестата);

- сведения о дополнительном профессиональном образовании (профессиональной переподготовке, повышении квалификации) (наименование образовательной и (или) научной организации, год окончания, реквизиты документа о переподготовке (повышении квалификации), квалификация и специальность по документу о переподготовке (повышении квалификации), наименование программы обучения, количество часов обучения).

6.13. Обработка персональных данных и биометрических персональных данных субъектов персональных данных, указанных в подпунктах 1-3 пункта 6.4 настоящих Правил, осуществляется без их согласия в целях, определенных пунктом 6.7 настоящих Правил, в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных» и Трудовым кодексом Российской Федерации.

6.14. Обработка специальных категорий персональных данных субъектов персональных данных осуществляется без их согласия в целях, указанных в пункте 6.7 настоящих Правил, в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10 Федерального закона «О персональных данных», за исключением случаев получения персональных данных у третьей стороны в соответствии с пунктом 3 статьи 86 Трудового кодекса Российской Федерации.

6.15. Обработка персональных данных субъектов персональных данных, указанных в подпунктах 1-3 пункта 6.4 настоящих Правил, осуществляется с их согласия в следующих случаях:

- при передаче персональных данных третьим лицам в случаях, не предусмотренных законодательством Российской Федерации;

- при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

6.16. В случаях, предусмотренных пунктом 6.15 настоящих Правил, согласие субъектов персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

6.17. Обработка персональных данных субъектов персональных данных, указанных в подпунктах 1-3 пункта 6.4 настоящих Правил, осуществляется уполномоченными должностными лицами Учреждения и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

6.18. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных осуществляется путем:

- получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые субъектом персональных данных);
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования персональных данных в ходе кадровой работы;
- внесения персональных данных в информационные системы Учреждения.

6.19. Запрещается получать, обрабатывать и приобщать к личному делу субъектов персональных данных, указанных в подпунктах 1-3 пункта 6.4 настоящих Правил, персональные данные, не предусмотренные пунктом 6.12 настоящих Правил, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

6.20. В целях, указанных в пункте 6.8 настоящих Правил, обрабатываются следующие категории персональных данных субъектов персональных данных, указанных в подпункте 4 пункта 6.4 настоящих Правил:

- фамилия, имя, отчество;
- год рождения;
- месяц рождения;
- дата рождения;
- место рождения;
- семейное положение;
- адрес электронной почты;
- адрес места жительства;
- адрес регистрации;
- номер телефона;
- гражданство;
- данные документа, удостоверяющего личность;
- сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);
- отношение к воинской обязанности, сведения о воинском учете; сведения об образовании;
- сведения об образовании (наименование образовательной и (или) иной организации, год окончания, уровень профессионального образования, реквизиты документов об образовании, направление подготовки, специальность и квалификация по документу об образовании, ученая степень, ученое звание (дата присвоения, реквизиты диплома, аттестата);
- сведения о дополнительном профессиональном образовании (профессиональной переподготовке, повышении квалификации) (наименование образовательной и (или) научной организации, год окончания, реквизиты

документа о переподготовке (повышении квалификации), квалификация и специальность по документу о переподготовке (повышении квалификации), наименование программы обучения, количество часов обучения).

6.21. Обработка персональных данных субъектов персональных данных, указанных в подпункте 4 пункта 6.4 настоящих Правил, осуществляется без их согласия в целях, определенных пунктом 6.8 настоящих Правил, в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных» и Трудовым кодексом Российской Федерации.

6.22. Обработка специальных категорий персональных данных субъектов персональных данных осуществляется в случаях, определенных настоящими Правилами и Федеральным законом «О персональных данных».

6.23. Обработка персональных данных субъектов персональных данных, указанных в подпункте 4 пункта 6.4 настоящих Правил, осуществляется уполномоченными должностными лицами Учреждения и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

6.24. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных осуществляется путем:

- получения оригиналов необходимых документов;
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования персональных данных в ходе кадровой работы;
- внесения персональных данных в информационные системы Учреждения.

6.25. Запрещается получать, обрабатывать и приобщать к личному делу субъектов персональных данных, указанных в подпункте 4 пункта 6.4 настоящих Правил, персональные данные, не предусмотренные пунктом 6.20 настоящих Правил, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

6.26. В целях, указанных в пункте 6.9 настоящих Правил, обрабатываются следующие категории персональных данных субъектов персональных данных, указанных в подпункте 5 пункта 6.4 настоящих Правил:

- фамилия, имя, отчество;
- адрес электронной почты;
- адрес места жительства;
- адрес регистрации;
- номер телефона;
- иные, указанные субъектом персональных данных в обращении сведения.

6.27. Обработка персональных данных субъектов персональных данных, указанных в подпункте 5 пункта 6.4 настоящих Правил, осуществляется уполномоченными должностными лицами Учреждения и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

6.28. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных осуществляется путем:

- получения оригиналов необходимых документов;
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- внесения персональных данных в информационные системы Учреждения.

6.29. В целях, указанных в пункте 6.10 настоящих Правил, обрабатываются следующие категории персональных данных субъектов персональных данных, указанных в подпункте 6 пункта 6.4 настоящих Правил:

- фамилия, имя, отчество;
- год рождения;
- месяц рождения;
- дата рождения;
- место рождения;
- социальное положение;
- пол;
- адрес электронной почты;
- адрес места жительства;
- адрес регистрации;
- номер телефона;
- СНИЛС;
- ИНН;
- гражданство;
- данные документа, удостоверяющего личность;
- данные документа, содержащиеся в свидетельстве о рождении;
- реквизиты банковской карты;
- номер расчетного счета; номер лицевого счета;
- профессия;
- сведения об образовании;
- биометрические данные характеризующие внешний облик человека;
- иные персональные данные, вносимые пользователями информационных систем в рамках обработки информации.

6.30. Обработка персональных данных субъектов персональных данных, указанных в подпункте 6 пункта 6.4 настоящих Правил, осуществляется уполномоченными должностными лицами Учреждения

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

6.31. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных осуществляется путем:

- получения оригиналов необходимых документов;
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- внесения персональных данных в информационные системы Учреждения.

6.32. В целях, указанных в пункте 6.11 настоящих Правил, обрабатываются следующие категории персональных данных субъектов персональных данных, указанных в подпункте 7 пункта 6.4 настоящих Правил:

- фамилия, имя, отчество;
- данные документа, удостоверяющего личность.

6.33. Обработка персональных данных субъектов персональных данных, указанных в подпункте 7 пункта 6.4 настоящих Правил, осуществляется уполномоченными должностными лицами Учреждения и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

6.34. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных осуществляется путем:

- получения оригиналов необходимых документов;
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- внесения персональных данных в информационные системы Учреждения.

6.35. Хранение персональных данных субъектов персональных данных на бумажном носителе осуществляется структурными подразделениями Учреждения к полномочиям которых относится обработка персональных данных в соответствии с действующими нормативными актами и определены в соответствии с номенклатурой дел Учреждения.

6.36. Персональные данные субъектов персональных данных, указанных в подпунктах 1 – 4 пункта 6.4 настоящих Правил, хранятся в течении:

- 75 лет, в случае если документация, содержащая персональные данные закончена делопроизводством до 1 января 2003 года;
- 50 лет, в случае если документация, содержащая персональные данные закончена делопроизводством после 1 января 2003 года,

после чего носители персональных данных передаются на постоянное хранение в архивные фонды в соответствии со статьей 22.1 Федерального закона от 22 октября 2004 года № 125-ФЗ «Об архивном деле в Российской Федерации».

6.37. Персональные данные субъектов персональных данных, указанных в подпунктах 5-7 пункта 6.4 настоящих Правил, хранятся до достижения цели обработки персональных данных, после чего уничтожаются.

6.38. Срок хранения персональных данных, внесенных в информационные системы Учреждения, должен соответствовать сроку хранения оригиналов (персональных данных на бумажных носителях).

6.39. Доступ к персональным данным разрешен работникам Учреждения, занимающим должности, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

6.40. Перед допуском к работе с персональными данными, предоставлением персональных данных для выполнения служебных обязанностей работник Учреждения дает письменное обязательство о неразглашении персональных данных.

6.41. Все персональные данные Учреждение получает непосредственно от субъекта персональных данных. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект персональных данных должен быть заранее уведомлен о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

6.42. Отказ субъекта персональных данных от своих прав на конфиденциальность недействителен.

## 7. Условия и порядок автоматизированной обработки персональных данных субъектов персональных данных

7.1. Должностным лицам Учреждения, имеющим право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе, в соответствии с функциями, предусмотренными должностными регламентами.

7.2. Информация вносится как в автоматическом режиме, так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

7.3. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах Учреждения, достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным, в том числе принятием мер по обеспечению безопасности персональных данных, предусмотренных разделом 12 настоящих Правил.

7.4. Доступ работников Учреждения к персональным данным, находящимся в информационных системах Учреждения, предусматривает обязательное прохождение процедуры идентификации и аутентификации.

7.5. Обмен персональными данными при их обработке в информационных системах Учреждения осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и применения программных и технических средств в соответствии со статьей 19 Федерального закона «О персональных данных».

7.6. В случае выявления нарушений порядка обработки персональных данных в информационных системах Учреждения уполномоченными должностными лицами Учреждения принимаются меры по установлению причин нарушений и их устранению с момента обнаружения таких нарушений.

## 8. Условия и порядок неавтоматизированной обработки персональных данных субъектов персональных данных

8.1. Обработка персональных данных без использования средств автоматизации персональных данных может осуществляться в виде документов на бумажных или электронных носителях.

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

8.3. При неавтоматизированной обработке персональных данных на бумажных носителях не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы.

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

8.5. Документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

8.6. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовые формы), должны соблюдаться следующие условия:

8.6.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес Учреждения, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

8.6.2. Типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных,

при необходимости получения письменного согласия на обработку персональных данных.

8.6.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

8.6.4. Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

8.7. При обработке персональных данных на электронных носителях без использования средств автоматизации:

8.7.1. неавтоматизированная обработка персональных данных в электронном виде осуществляется на электронных носителях информации.

8.7.2. при несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

8.7.3. при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия таких персональных данных.

8.7.4. при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

8.8. Подготовка и учет документов, содержащих персональные данные.

8.8.1. Бланки типовых форм документов (справки, карточки, талоны, ведомости и такое прочее) могут изготавливаться при помощи средств вычислительной техники или на компьютере.

8.8.2. Персональные данные (переменная часть) в типовые формы документов вносятся при помощи средств вычислительной техники, рукописным способом.

8.8.3. После внесения переменной части в типовые формы, последние становятся документами и подлежат немедленному учету в журнале изданных документов с присвоением им учетного номера.

8.8.4. Для каждого вида документов заводятся свои журналы учета.

8.9. Получение (отправление) документов и их учет.

8.9.1. Все документы, поступающие из других организаций и учреждений, подлежат регистрации по журналу учета поступивших документов. На самом документе в правом нижнем углу первого листа документа проставляется отметка о поступлении, которая содержит входящий номер, присвоенный документу, дату поступления.

8.9.2. Поступившие документы должны обрабатываться и передаваться на рассмотрение директору Учреждения, либо заместителю директора Учреждения, курирующему направление деятельности в день их получения и оперативно доводиться до исполнителей.

8.9.3. Пересылка документов может осуществляться через органы специальной связи или через почтовое отделение связи.

8.9.4. Об отправленных документах производятся соответствующие отметки в учетных формах.

8.10. Копирование документов.

8.10.1. При действительной служебной необходимости в дополнительных экземплярах документов производится их копирование.

8.10.2. На некоторых документах может стоять отметка о том, что снятие копий с этого документа не разрешается. Такие документы копированию не подлежат.

8.10.3. Разрешение на копирование (снятие копий) документов могут давать соответствующие должностные лица (руководители структурных подразделений Учреждения), наделенные правом распоряжения сведениями.

8.10.4. Документы, поступившие из других организаций, должны копироваться с письменного разрешения директора Учреждения, либо заместителя директора Учреждения, курирующего направление деятельности или с письменного разрешения издавших их организаций.

8.10.5. Разрешение на изготовление дополнительных экземпляров (копий) учетного документа оформляется на обороте последнего листа экземпляра, с которого производится копирование. В разрешении указываются номера документов или страниц, с которых необходимо сделать копию, а также количество копий.

8.10.6. Подлежащие копированию документы регистрируются в журнале учета копирования документов.

8.10.7. На копиях экземпляров документа проставляются их номера. При этом номера копий продолжают номера ранее изготовленных экземпляров.

8.11. Обеспечение защиты персональных данных при неавтоматизированной обработке.

8.11.1. Организация хранения документов предполагает, что помещения, где хранятся документы, должны соответствовать требованиям технической безопасности, противопожарной безопасности, а также установленным санитарным нормам.

8.11.2. Для обеспечения физической сохранности документов, дел, а также для предотвращения разглашения содержащейся в них информации устанавливается специальный режим их хранения и обращения.

## 9. Правила работы с обезличенными данными в случае обезличивания персональных данных

9.1. Обезличивание персональных данных проводится в целях снижения ущерба от разглашения персональных данных, повышения уровня защищенности информационных систем Учреждения и предотвращения несанкционированного использования персональных данных, если иное не предусмотрено законодательством Российской Федерации.

9.2. Обезличивание персональных данных Учреждением осуществляется в статистических или иных исследовательских целях с соблюдением требований, установленных подпунктом «з» пункта 1 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, утвержденным постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211.

9.3. На основании целей обезличивания, указанных в пункте 9.2 Настоящих Правил, сроки обработки и хранения персональных данных, полученных в результате обезличивания, устанавливаются уполномоченными лицами Учреждения исходя из служебной необходимости.

9.4. Получение согласия субъекта на обработку персональных данных, полученных в результате обезличивания, не требуется на основании пункта 9 части 1 статьи 6 Федерального закона «О персональных данных».

9.5. Обезличивание персональных данных, осуществляется в соответствии с требованиями и методами, установленными постановлением Правительства Российской Федерации от 01 августа 2025 № 1154 «Об утверждении требований к обезличиванию персональных данных, методов обезличивания персональных данных и Правил обезличивания персональных данных».

## 10. Порядок уничтожения персональных данных

10.1. Персональные данные подлежат уничтожению в следующих случаях:

- при достижении цели обработки персональных данных или в случае утраты необходимости в достижении цели обработки персональных данных, если иное не предусмотрено Федеральным законом «О персональных данных»;
- при изменении, признании утратившими силу нормативных правовых актов, устанавливающих правовые основания обработки персональных данных;
- при выявлении факта неправомерной обработки персональных данных;
- при отзыве субъектом персональных данных согласия, если иное не предусмотрено Федеральным законом «О персональных данных»;
- по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных в случае выявления фактов совершения Учреждением неправомерных действий с персональными

данными, когда устранение соответствующего нарушения не представляется возможным.

10.2. Структурным подразделением Учреждения, либо конкретным уполномоченным лицом, ответственным за документооборот и архивирование, осуществляется систематический контроль и выявление документов, содержащих персональные данные с истекшими сроками хранения.

10.3. Вопрос об уничтожении материальных носителей, содержащих персональные данные с истекшими сроками хранения, рассматривается на заседании комиссии, состав которой утверждается приказом руководителя Учреждения.

10.4. Способ уничтожения материальных носителей персональных данных определяется комиссией. Допускается применение следующих способов:

- сжигание;
- шредирование (измельчение);
- передача на специализированные полигоны (свалки);
- уничтожение специализированной организацией;
- химическая обработка.

10.5. По итогам уничтожения и итогового заседания комиссии составляется акт об уничтожении персональных данных. Акт об уничтожении персональных данных, подписывается председателем и членами комиссии и утверждается руководителем Учреждения.

10.6. При необходимости уничтожения большого количества материальных носителей, содержащих персональные данные субъекта, или применения специальных способов уничтожения, допускается привлечение специализированных организаций. В этом случае, комиссия Учреждения должна присутствовать при уничтожении материальных носителей персональных данных. При этом, к акту об уничтожении персональных данных необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

10.7. Уничтожение полей баз данных информационных систем Учреждения, содержащих персональные данные субъекта, выполняется по заявке руководителя структурного подразделения Учреждения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

10.8. Уничтожение достигается путем шредирования (измельчения), затирания информации на носителях информации (в том числе и резервных копиях) или путем механического нарушения целостности носителя информации, не позволяющего в дальнейшем произвести считывание или восстановление персональных данных. При этом составляется акт об уничтожении персональных данных, приложением к которому оформляется выгрузка из журнала регистрации событий базы данных (информационной

системы), в которой такие данные были уничтожены, при наличии технической возможности.

10.9. Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определенного срока предусмотрены соответствующими нормативными или договорными документами.

10.10. При отсутствии технической возможности осуществить уничтожение персональных данных, содержащихся в базах данных или невозможности осуществления затирания информации на носителях, допускается проведение обезличивания путем перезаписи полей баз данных. Перезапись должна быть осуществлена таким образом, чтобы дальнейшая идентификация субъекта персональных данных была невозможна.

10.11. Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных Учреждения. После уничтожения персональных данных, ответственный за организацию обработки персональных данных Учреждения уведомляет субъекта персональных данных или его представителя об уничтожении персональных данных.

## 11. Рассмотрение запросов субъектов персональных данных или их представителей

11.1. Субъекты персональных данных имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Учреждением;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Учреждением способы обработки персональных данных;
- наименование и место нахождения Учреждения, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании федерального закона, за исключением сведений о работниках Учреждения непосредственно осуществляющих обработку персональных данных;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

- информацию о способах исполнения Учреждением обязанностей, установленных статьей 18.1 Федерального закона «О персональных данных»;

- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

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

11.3. Сведения, указанные в пункте 11.1 настоящих Правил, должны быть предоставлены субъекту персональных данных Учреждением в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных;

11.4. Сведения, указанные в пункте 11.1 настоящих Правил, предоставляются субъекту персональных данных или его представителю уполномоченным должностным лицом структурного подразделения Учреждения, осуществляющим обработку соответствующих персональных данных, в течение десяти рабочих дней с момента обращения либо получения Учреждением запроса субъекта персональных данных или его представителя. Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

- сведения, подтверждающие участие субъекта персональных данных в отношениях с Учреждением либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением;

- подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

11.5. В случае если сведения, указанные в пункте 11.1 настоящего раздела, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Учреждению или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором,

стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

11.6. Субъект персональных данных вправе обратиться повторно к Учреждению или направить повторный запрос в целях получения сведений, указанных в пункте 11.1 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 11.5 настоящих Правил, в случае если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 11.4 настоящих Правил, должен содержать обоснование направления повторного запроса.

11.7. Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 11.5 и 11.6 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Учреждении.

11.8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

## 12. Меры по обеспечению безопасности персональных данных при их обработке

12.1. Учреждение при обработке персональных данных принимает необходимые нормативные, организационные и технические меры и обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

12.2. Обеспечение безопасности персональных данных Учреждением достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах Учреждения;

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах Учреждения, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации (сертифицированные средства защиты информации);
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационных системах Учреждения, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах Учреждения;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности персональных данных, обрабатываемых в информационных системах Учреждения.

### 13. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

13.1. Оценкой вреда, который может быть причинен субъектам персональных данных, в случае нарушения требований по обработке и обеспечению безопасности персональных данных является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных.

13.2. Учреждение проводит оценку вреда в соответствии с приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 октября 2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

13.3. Процедура проведения оценки вреда, который может быть причинен субъектам персональных данных, закрепляется в локальном нормативном акте Учреждения.

### 14. Внутренний контроль соответствия обработки персональных данных установленным требованиям

14.1. Внутренний контроль выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях Учреждения осуществляется

с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, правильности обработки персональных данных ответственными лицами в структурных подразделениях, а также выработки мер по их устранению и недопущению в дальнейшем.

14.2. Внутренний контроль осуществляет ответственный за организацию обработки персональных данных в Учреждении.

14.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных устанавливаются внутренними нормативными актами Учреждения.

## 15. Ответственность за нарушение норм, регулирующих обработку и защиты персональных данных

15.1. Лица виновные в нарушении норм, регулирующих получение, обработку, передачу, хранение и защиту персональных данных субъекта персональных данных, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности в соответствии с действующим законодательством Российской Федерации.

## 16. Заключительные положения

16.1. Контроль исполнения требований настоящих Правил осуществляется ответственным за организацию обработки персональных данных Учреждения.

16.2. Настоящие Правила подлежат пересмотру в ходе периодического анализа со стороны руководства Учреждения, а также в случаях изменения законодательства Российской Федерации в области персональных данных.

16.3. Во всем, что не урегулировано настоящими Правилами, работники Учреждения руководствуются действующим законодательством Российской Федерации в области персональных данных.

Приложение № 2 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № 4/01/02-23/17

УТВЕРЖДЕНЫ  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № 4/01/02-23/17

## Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

### 1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных в муниципальном казенном учреждении «Цифра.ФТ» (далее – Учреждение) требованиям к защите персональных данных, установленных законодательством Российской Федерации и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3. Настоящими Правилами в своей работе должны руководствоваться работники Учреждения, осуществляющие внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных.

### 2. Структура процессов по внутреннему контролю

2.1. Контроль выполнения требований по защите персональных данных в структурных подразделениях Учреждения осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработки мер по их устранению и недопущению в дальнейшем.

2.2. Контроль выполнения требований по защите персональных данных в структурных подразделениях Учреждения осуществляет ответственный за организацию обработки персональных данных в Учреждении (далее – Ответственный за ПДн).

2.3. Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

2.4. Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

2.5. Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов персональных данных или нарушения требований по защите персональных данных.

2.6. Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений Учреждения не позднее, чем за 24 часа до начала проверки.

2.7. Проверки по частным вопросам могут проводиться без уведомления руководителей структурных подразделений Учреждения.

2.8. Периодичность и сроки проведения плановых проверок Учреждения устанавливаются Ответственным за ПДн.

### 3. Порядок подготовки к проверке

3.1. Общий контроль выполнения требований по обеспечению безопасности персональных данных в Учреждении осуществляется Ответственным за ПДн в соответствии с планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных.

3.2. Директор Учреждения своим решением может инициировать внеплановый контроль выполнения требований по обеспечению безопасности персональных данных в Учреждении.

3.3. Для проведения контроля выполнения требований по обеспечению безопасности персональных данных в Учреждении совместно с Ответственным за ПДн, директором Учреждения могут быть назначены проверяющие лица из числа сотрудников Учреждения.

3.4. Ответственный за ПДн, проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки проверяющие должны изучить материалы предыдущих проверок данного структурного подразделения.

### 4. Порядок проведения проверки

4.1. Руководители структурных подразделений в Учреждении обязаны оказывать содействие проверяющим лицам и в случае необходимости определяют должностное лицо, ответственное за сопровождение проверки.

4.2. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

4.3. Должны быть согласованы конкретные вопросы по объему, содержанию, срокам проведения проверки, а также каких работников необходимо привлечь к проверке и какие помещения следует посетить.

4.4. Общий порядок проведения проверки включает:

- выявление работников, задействованных в обработке персональных данных;

- проверка факта ознакомления работников с нормативными документами, регламентирующими вопросы обработки и защиты персональных данных

в Учреждении;

- получение при содействии работников документов, касающихся обработки и защиты персональных данных в данном структурном подразделении;

- анализ полученной документации;

- непосредственная проверка выполнения установленных в Учреждении нормативных документов в области обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

4.5. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении рассматриваются следующие показатели работ по защите персональных данных:

- наличие согласий на обработку персональных данных субъектов персональных данных в случаях предусмотренных законодательством Российской Федерации;

- соответствие состава и сроков обработки целям обработки персональных данных;

- соответствие перечня должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

- соответствие перечня лиц, имеющих доступ в помещения, в которых ведется обработка персональных данных;

- наличие нормативных документов по защите персональных данных в Учреждении;

- знание нормативных документов и уровень подготовки работников Учреждения, имеющих доступ к персональным данным;

- полнота и правильность выполнения требований нормативных документов работниками Учреждения, имеющими доступ к персональным данным;

- наличие документов, подтверждающих учет и сохранность материальных носителей персональных данных;

4.6. В ходе осуществления контроля выполнения требований по защите персональных данных дополнительно рассматриваются следующие показатели работ по защите персональных данных:

- соответствие информации, указанной в уведомлении об обработке персональных данных реальному положению дел;

- наличие и корректность перечня информационных систем;

- наличие документа, подтверждающего правильность определения уровня защищенности персональных данных, обрабатываемых

в информационных системах, а также классов защищенности информационных систем;

- наличие документа, подтверждающего факт определения угроз безопасности персональных данных, а также его актуальность;

- соответствие состава средств вычислительной техники информационных систем указанному в документации на информационную систему;

- соответствие требованиям по организации разграничения доступа пользователей к информационным ресурсам (в том числе сетевым);

- порядок защиты персональных данных при передаче по сети;

- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных.

4.7. Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

4.8. Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

## 5. Оформление результатов проверки

5.1. Результаты проверки оформляются актом.

5.2. Акт составляется в одном экземпляре и подписывается проверяющими. Оригинал документа с результатами проверки хранится у Ответственного за ПДн.

5.3. При необходимости принятия решений по результатам проверки, Ответственным за ПДн готовится соответствующая служебная записка на имя директора Учреждения.

## 6. Корректирующие мероприятия и контроль за их исполнением

6.1. Директор Учреждения анализирует акт о результатах внутренней проверки и в пятидневный срок утверждает перечень мероприятий, необходимых для устранения выявленных нарушений и причин их возникновения.

6.2. Перечень мероприятий формируется Ответственным за ПДн.

6.3. Если корректирующие мероприятия касаются других структурных подразделений Учреждения, то к анализу привлекаются руководители или работники соответствующих структурных подразделений.

6.4. Выполнение корректирующих мероприятий и их достаточность определяется Ответственным за ПДн.

6.5. Внутренняя проверка считается оконченной после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

Приложение № 3 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № 12/01/02-23/17

УТВЕРЖДЕНЫ  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № 12/01/02-23/17

## Правила доступа в помещения муниципального казенного учреждения «Цифра.ФТ» в которых ведётся обработка защищаемой информации, в том числе персональных данных

### 1. Общие положения

1.1. Настоящие Правила доступа в помещения муниципального казенного учреждения «Цифра.ФТ» в которых ведётся обработка защищаемой информации, в том числе персональных данных (далее – Правила) устанавливают порядок доступа в помещения муниципального казенного учреждения «Цифра.ФТ» (далее – Учреждение), в которых ведётся обработка защищаемой (конфиденциальной) информации, в том числе персональных данных (далее – Информация).

1.2. Правила разработаны в целях обеспечения безопасности Информации обрабатываемой в Учреждении на средствах вычислительной техники информационных систем, на материальных носителях Информации, а также для обеспечения внутриобъектового режима.

1.3. Настоящий Порядок устанавливает правила доступа в следующие помещения Учреждения (далее – Помещения):

- помещения, в которых происходит обработка Информации, как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;

- помещения, в которых хранятся материальные носители Информации и их резервные копии;

- помещения, в которых установлены средства криптографической защиты информации (далее – СКЗИ) и хранятся носители ключевой информации, в том числе средства электронной подписи (далее – Спецпомещения).

1.4. Настоящие Правила разработаны в соответствии с:

- Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

- постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

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

- приказом Федеральной службы безопасности Российской Федерации от 18 марта 2025 года № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств»;

- приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости»;

- приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

1.5. Для каждого Помещения назначается лицо, ответственное за доступ в Помещение.

1.6. Сотрудники Учреждения, допущенные в Помещения, обязаны:

- выполнять требования обеспечения безопасности Информации;
- соблюдать режим конфиденциальности при обращении с Информацией, носителями Информации и СКЗИ (в том числе ключевыми документами к ним);

- своевременно выявлять попытки посторонних лиц получить сведения об Информации, об используемых СКЗИ или ключевых документах к ним;

- предусматривать отдельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптографических ключей.

## 2. Общие требования к оборудованию помещений и регламентации доступа в них

2.1. Режим обеспечения безопасности Помещений, в которых осуществляется обработка Информации должен быть организован таким

образом, чтобы препятствовать возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти Помещения.

2.2. Ограждающие конструкции Помещений, должны предполагать существенные трудности для нарушителя по их преодолению (например, металлические решётки на окнах, металлическая дверь, система контроля и управления доступом и так далее).

2.3. Помещения должны быть оснащены надёжными входными дверьми с замками.

2.4. Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, должны быть оборудованы металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

2.5. В Учреждении определяется перечень Помещений, в которых разрешена обработка Информации (форма перечня представлена в приложении № 1 к настоящим Правилам).

2.6. Доступ работников в Помещения Учреждения должен быть организован согласно перечню лиц, допущенных в Помещения обработки Информации (форма перечня представлена в приложении № 2 к настоящим Правилам). Перечень работников, доступ которых разрешён в Помещения, размещается на внутренней стороне двери этого помещения.

2.7. В Помещениях определяются места хранения материальных носителей Информации и лиц, ответственных за их сохранность (форма перечня представлена в приложении № 3 к настоящим Правилам).

2.8. Указанные перечни разрабатываются ответственными за доступ в Помещения лицами и утверждаются директором Учреждения либо лицом его замещающим.

2.9. Доступ посторонних лиц в Помещения, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица из числа работников, допущенных в Помещение. При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с защищаемой Информацией. Такими мерами являются:

- размещение мониторов, исключающее или существенно затрудняющее просмотр отображаемой информации;

- размещение документации на бумажных носителях, содержащих Информацию, исключающее просмотр Информации на них (документация убирается в папки, ящики тумбочек/столов, либо переворачивается лицевой стороной вниз, либо накрывается сверху непрозрачными объектами, закрывающими область текста).

2.10. В нерабочее время все окна и двери в Помещениях (в том числе в смежные помещения), в которых ведётся обработка Информации, должны быть надёжно закрыты, материальные носители должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

2.11. При необходимости повышенного уровня обеспечения безопасности Помещений могут использоваться системы видеонаблюдения и системы контроля и управления доступом.

## 2. Особенности доступа в серверные помещения

2.1. Учёт доступа в серверные помещения третьих лиц (осуществляющих обслуживание, техническое сопровождение, настройку серверного и активного сетевого оборудования) должен отражаться в журнале доступа в серверные помещения (форма журнала приведена в приложении № 4 к настоящим Правилам).

2.2. Двери серверных помещений должны быть оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытие только для санкционированного прохода.

2.3. Уборка серверных помещений должна происходить только под контролем сопровождающего лица из числа работников, допущенных в помещение.

2.4. Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

2.5. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за доступ в помещения лицом.

2.6. Сотрудники органов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (далее – МЧС), аварийных служб, врачи «скорой помощи» допускаются в серверные помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении работника Учреждения, допущенного в помещение.

## 3. Особенности доступа в Спецпомещения

3.1. Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам криптографической защиты информации. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время.

3.2. Расположение Спецпомещений, специальное оборудование и организация режима в Спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

3.3. Двери Спецпомещений должны быть оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытия только для санкционированного прохода.

3.4. При утрате ключа от входной двери в Спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей (с документальным оформлением).

3.5. Доступ работников в Спецпомещения в нерабочее время допускается на основании служебных записок (или иных видов разрешающих документов).

3.6. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в Спецпомещения иных лиц из числа работников Учреждения.

3.7. Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в Спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении лица, ответственного за доступ в Спецпомещение.

3.8. Нахождение в Спецпомещениях посторонних лиц в нерабочее время запрещается.



Приложение № 2

к Правилам доступа в помещения муниципального казенного учреждения «Цифра.ФТ» в которых ведётся обработка защищаемой информации, в том числе персональных данных

**Форма**

**ПЕРЕЧЕНЬ**

**лиц, допущенных в помещения обработки конфиденциальной информации (в том числе персональных данных)**

№ п/п	Наименование структурного подразделения	№ кабинета	Ф.И.О. работника	Должность





Приложение № 4 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № 101/02-23/17

УТВЕРЖДЕНЫ  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № 101/02-23/17

## Правила работы с обезличенными персональными данными в муниципальном казенном учреждении «Цифра.ФТ»

### 1. Общие положения

1. Настоящие Правила работы с обезличенными персональными данными в муниципальном казенном учреждении «Цифра.ФТ» (далее соответственно – Правила, Учреждение) разработаны с учетом требований Федерального закона от 27 июля 2006 № 152-ФЗ «О персональных данных».

2. Настоящие Правила определяют порядок работы с обезличенными данными в Учреждении.

### 2. Термины и определения

Персональные данные – 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.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

### 3. Условия обезличивания

3.1. Обезличивание персональных данных в Учреждении может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных в Учреждении:

- замена части сведений идентификаторами;

- обобщение – понижение точности некоторых сведений (например, «место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город).

3.3. Перечень должностей Учреждения, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных утверждается приказом директора Учреждения.

Решение о необходимости обезличивания персональных данных принимаются директором Учреждения, либо уполномоченным сотрудником Учреждения.

Работники Учреждения, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

Сотрудники структурных подразделений, обслуживающие базы данных содержащие персональные данные, совместно с ответственным за организацию обработки персональных данных в Учреждении, осуществляют непосредственное обезличивание персональных данных выбранным способом.

#### 4. Правила работы с обезличенными персональными данными

4.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

4.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

4.3. При обработке обезличенных персональных данных с использованием и без использования средств автоматизации, необходимо руководствоваться требованиями к защите персональных данных, установленными Правительством Российской Федерации.

4.4. Обрабатываемые персональные данные подлежат обезличиванию по достижению целей их обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

Приложение № 5 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № У.101102.23/11

УТВЕРЖДЕНЫ  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № У.101102.23/11

## Правила рассмотрения запросов субъектов персональных данных или их представителей в муниципальном казенном учреждении «Цифра.ФТ»

### 1. Общие положения

1.1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей в муниципальном казенном учреждении «Цифра.ФТ» (далее соответственно – Правила, Учреждение) определяют порядок рассмотрения запросов субъектов персональных данных или их представителей (далее – запросы), поступающих в Учреждение.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

### 2. Права субъектов персональных данных

2.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных в соответствии с частью 7 статьи 14 Федерального закона «О персональных данных», в том числе содержащей:

- подтверждение факта обработки персональных данных Учреждением;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Учреждением способы обработки персональных данных;
- наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные субъекта персональных данных на основании договора с Учреждением или на основании федерального закона, в соответствии с которым осуществляется предоставление персональных данных;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществлённой или о предполагаемой трансграничной передаче данных;

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

- информацию о способах исполнения Учреждением обязанностей, установленных статьей 18.1 Федерального закона «О персональных данных»;

- иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

2.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона «О персональных данных».

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

2.4. Сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», должны быть предоставлены субъекту персональных данных в доступной форме и в них не должно содержаться персональных данных, относящихся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

2.5. Сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», предоставляются субъекту персональных данных или его представителю при обращении субъекта персональных данных, либо при получении запроса от субъекта персональных данных или его представителя.

### 3. Правила рассмотрения запросов субъектов персональных данных

3.1. Запрос субъекта персональных данных должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;

- сведения о дате выдачи указанного документа и выдавшем его органе;

- сведения, подтверждающие факт обработки Учреждением персональных данных субъекта персональных данных, подпись субъекта персональных данных или его представителя.

3.2. Запрос может быть направлен в форме электронного документа.

3.3. Рассмотрение запросов является обязанностью уполномоченных работников Учреждения.

3.4. Работники Учреждения обеспечивают:

- проверку достоверности сведений, указанных в запросе;

- объективное, всестороннее и своевременное рассмотрение запроса;

- принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

- направление письменных ответов по существу запроса.

3.5. Запрос прочитывается и проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться к Учреждению повторно или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона «О персональных данных», и ознакомления с такими персональными данными в соответствии с частью 4 статьи 14 Федерального закона «О персональных данных» не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен предусмотренным Федеральным законом «О персональных данных».

3.6. Срок предоставления ответов на поступившие запросы от субъектов персональных данных или их представителей в соответствии с частью 1 статьи 20 Федерального закона «О персональных данных» составляет десять рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Учреждением в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

3.7. Субъект персональных данных вправе обратиться в Учреждение повторно или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона «О персональных данных», а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 статьи 14 Федерального закона «О персональных данных», в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объёме по результатам рассмотрения первоначального обращения. Повторный запрос, наряду с необходимыми сведениями, должен содержать обоснование направления повторного запроса.

3.8. Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона «О персональных данных». Такой отказ должен быть мотивированным, обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Учреждении.

3.9. Учреждение обязано сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя, либо дать письменный ответ в сроки, предусмотренные Федеральным законом «О персональных данных».

3.10. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении, либо при получении запроса субъекта персональных данных или его представителя, уполномоченные должностные лица Учреждения обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного Федерального закона, являющегося основанием для такого отказа. Ответ на запрос должен быть предоставлен в срок не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Учреждением в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

3.11. В соответствии с частью 3 статьи 20 Федерального закона «О персональных данных» Учреждение обязано безвозмездно предоставлять субъекту персональных данных, либо его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных:

- в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, работники Учреждения обязаны внести в них необходимые изменения;

- в срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, работники Учреждения обязаны уничтожить такие персональные данные.

3.12. Учреждение обязано уведомить субъекта персональных данных или его представителя о внесённых изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы, в случае их неактуальности, неполноты, неточности персональных данных и (или) если такие персональные данные были получены незаконно.

3.13. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных, работники Учреждения обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

3.14. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, работники Учреждения обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.15. В случае подтверждения факта неточности персональных данных работники Учреждения на основании сведений, представленных субъектом персональных данных или его представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в соответствии с частью 2 статьи 20 Федерального закона «О персональных данных» в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.16. В случае выявления неправомерной обработки персональных данных работники Учреждения в срок, в соответствии с частью 3 статьи 20 Федерального закона «О персональных данных», не превышающий трёх рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных, а в случае, если обеспечить правомерность обработки персональных данных невозможно, работники Учреждения в срок не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждения обязан уведомить субъекта персональных данных или его представителя. В случае, если обращение субъекта персональных данных или его представителя, либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также в указанный орган.

3.17. Для проверки фактов, изложенных в запросах, при необходимости Учреждением организуются служебные (внутренние) проверки.

3.18. По результатам служебной (внутренней) проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения работниками Учреждения действия (бездействия), содержащего признаки административного правонарушения или состава преступления, информация передается незамедлительно в правоохранительные органы.

Приложение № 6 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № 4/01/02-23/17

УТВЕРЖДЕН  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № 4/01/02-23-17

Перечень должностей в муниципальном казенном учреждении  
«Цифра.ФТ», замещение которых предусматривает осуществление  
обработки, хранения, либо доступа к персональным данным

1. Директор муниципального казенного учреждения «Цифра.ФТ»  
(далее – МКУ «Цифра.ФТ»).
2. Заместитель директора – директор по экономическому развитию  
и правовому обеспечению МКУ «Цифра.ФТ».
3. Заместитель директора – директор дирекции по проектам МКУ  
«Цифра.ФТ».
4. Директор технический МКУ «Цифра.ФТ».
5. Главный бухгалтер МКУ «Цифра.ФТ».
6. Бухгалтер МКУ «Цифра.ФТ».
7. Главный экономист МКУ «Цифра.ФТ».
8. Специалист по управлению персоналом МКУ «Цифра.ФТ».
9. Главный специалист по защите информации МКУ «Цифра.ФТ».
10. Специалист по защите информации МКУ «Цифра.ФТ».
11. Специалист по организационному и документационному обеспечению  
управления организацией МКУ «Цифра.ФТ».
12. Ведущий юрисконсульт МКУ «Цифра.ФТ».
13. Юрисконсульт МКУ «Цифра.ФТ».
14. Ведущий руководитель проектов в области информационных технологий  
МКУ «Цифра.ФТ».
15. Руководитель службы эксплуатации информационных систем МКУ  
«Цифра.ФТ».
16. Руководитель группы сопровождения информационных систем МКУ  
«Цифра.ФТ».
17. Руководитель группы технической поддержки технического отдела МКУ  
«Цифра.ФТ».

Приложение № 7 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № 10/102-23/1

УТВЕРЖДЕН  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № 10/102-23/1

Перечень должностей в муниципальном казенном учреждении «Цифра.ФТ»  
ответственных за проведение мероприятий по обезличиванию обрабатываемых  
персональных данных

1. Директор муниципального казенного учреждения «Цифра.ФТ»  
(далее – МКУ «Цифра.ФТ»).
2. Главный бухгалтер МКУ «Цифра.ФТ».
3. Специалист по управлению персоналом МКУ «Цифра.ФТ».
4. Директор технический МКУ «Цифра.ФТ».
5. Главный специалист по защите информации МКУ «Цифра.ФТ».

Приложение № 8 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № Ц/01/02-23/11

УТВЕРЖДЕНА  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № Ц/01/02-23/11

## Форма

### ОБЯЗАТЕЛЬСТВО

**работника муниципального казенного учреждения «Цифра.ФТ»,  
непосредственно осуществляющего обработку персональных данных**

Я, \_\_\_\_\_  
(фамилия, имя, отчество, должность)

обязуюсь:

- знать и выполнять требования законодательства в области персональных данных;

- хранить в тайне известные мне персональные данные, информировать лицо, ответственное за организацию обработки персональных данных, о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;

- обрабатывать только те персональные данные, к которым получен доступ в силу исполнения своих служебных обязанностей;

- прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора, освобождения меня от замещаемой должности или увольнения.

В соответствии со статьёй 7 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются информацией ограниченного доступа, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная законодательством Российской Федерации, за разглашение информации ограниченного доступа, мне разъяснена.

\_\_\_\_\_  
(дата)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(расшифровка подписи)

Приложение № 9 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № 4/01/02-23/17

УТВЕРЖДЕНА  
Приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № 4/01/02-23/17

## Форма

### СОГЛАСИЕ

#### субъекта персональных данных на обработку персональных данных

Я, \_\_\_\_\_,  
(фамилия, имя, отчество субъекта персональных данных)

зарегистрированный(ая) по адресу: \_\_\_\_\_

документ, удостоверяющий личность: \_\_\_\_\_, серия \_\_\_\_\_, № \_\_\_\_\_,  
выдан \_\_\_\_\_

свободно, своей волей и в своем интересе даю свое согласие уполномоченным должностным лицам муниципального казенного учреждения «Цифра.ФТ» (ИНН 2367026222, ОГРН1222300037981) (далее – Учреждение), расположенного по адресу: \_\_\_\_\_, на обработку как \_\_\_\_\_ с использованием \_\_\_\_\_ средств автоматизации, так и без использования таких средств, включая (сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение) следующих моих персональных данных: \_\_\_\_\_  
(перечисление сведений, относящихся к персональным данным)

- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;

с целью: \_\_\_\_\_  
(наименование цели обработки персональных данных)

- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;
- \_\_\_\_\_;

Срок действия настоящего согласия – с даты подписания до достижения целей обработки персональных данных и (или) до дня отзыва персональных данных по просьбе субъекта персональных данных.

Я проинформирован(а), что под обработкой персональных данных понимаются действия (операции) с персональными данными в рамках выполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», конфиденциальность персональных данных соблюдается в рамках исполнения Учреждением законодательства Российской Федерации.

Подтверждаю ознакомление с Правилами обработки персональных данных в Учреждении, правами и обязанностями в области защиты персональных данных.

Мне разъяснены юридические последствия отказа от предоставления персональных данных.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Учреждения.

Я осведомлен(а), что в случае отзыва согласия на обработку персональных данных, Учреждение вправе продолжить обработку персональных данных при наличии оснований, указанных в статьях 6, 10 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Субъект персональных данных: \_\_\_\_\_ / \_\_\_\_\_

(подпись)

(ФИО)

«\_\_» \_\_\_\_\_ 20\_\_ г.

Приложение № 10 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № 410/102-23/17

УТВЕРЖДЕНА  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № 410/102-23/17

## Форма

### СОГЛАСИЕ субъекта персональных данных на распространение (предоставление, передачу) персональных данных третьим лицам

Я, \_\_\_\_\_,  
(фамилия, имя, отчество субъекта персональных данных)

зарегистрированный(ая) по адресу: \_\_\_\_\_

документ, удостоверяющий личность: \_\_\_\_\_, серия: \_\_\_\_\_, № \_\_\_\_\_,  
выдан \_\_\_\_\_

свободно, своей волей и в своем интересе даю свое согласие уполномоченным  
должностным лицам муниципального казенного учреждения «Цифра.ФТ» (ИНН  
2367026222, ОГРН1222300037981) (далее – Учреждение), расположенного  
по адресу: \_\_\_\_\_

на распространение (предоставление, передачу) моих персональных данных.

\*РАЗРЕШАЮ /  НЕ РАЗРЕШАЮ Учреждению осуществлять  
распространение следующих моих персональных данных:

\_\_\_\_\_ с целью: \_\_\_\_\_

реализуемое посредством: \_\_\_\_\_

\*РАЗРЕШАЮ /  НЕ РАЗРЕШАЮ Учреждению предоставлять следующие  
мои персональные данные: \_\_\_\_\_

\_\_\_\_\_ с целью: \_\_\_\_\_

посредством: \_\_\_\_\_

\_\_\_\_\_ следующим лицам: \_\_\_\_\_

\*РАЗРЕШАЮ /  НЕ РАЗРЕШАЮ Учреждению передачу следующих моих  
персональных данных: \_\_\_\_\_

с целью: \_\_\_\_\_,  
посредством: \_\_\_\_\_,  
\_\_\_\_\_,  
следующим лицам: \_\_\_\_\_.

Подтверждаю ознакомление с Правилами обработки персональных данных в Учреждении, правами и обязанностями в области защиты персональных данных.

Мне разъяснены юридические последствия отказа от предоставления персональных данных.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Учреждения.

Срок действия настоящего согласия – с даты подписания до достижения целей обработки персональных данных и (или) до дня отзыва персональных данных по просьбе субъекта персональных данных.

Я осведомлен(а), что в случае отзыва согласия на обработку и (или) распространение (предоставление, передачу) персональных данных, Учреждение вправе продолжить обработку персональных данных при наличии оснований, указанных в статьях 6, 10 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Субъект персональных данных: \_\_\_\_\_  
(подпись) (ФИО)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.



Приложение № 12 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.05.2026 № 4/10/102-23/17

УТВЕРЖДЕН  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.07.2026 № 4/10/102-23/17

### Форма

Директору муниципального казенного  
учреждения «Цифра.ФТ» (МКУ «Цифра.ФТ»)

адрес местонахождения: \_\_\_\_\_

ОГРН: 1222300037981, ИНН: 2367026222

от

\_\_\_\_\_ (фамилия, имя, отчество субъекта персональных данных)

паспорт серии \_\_\_\_\_ № \_\_\_\_\_, выдан  
« \_\_\_\_ » \_\_\_\_\_ 202 \_\_\_\_ года

\_\_\_\_\_ (кем выдан)

зарегистрированного (ой)

по адресу: \_\_\_\_\_

адрес электронной почты \_\_\_\_\_

номер телефона: \_\_\_\_\_

### СОГЛАСИЕ

**на обработку персональных данных,  
разрешенных субъектом персональных данных для распространения**

Настоящим я, \_\_\_\_\_,  
(фамилия, имя, отчество субъекта персональных данных)

руководствуясь статьей 10.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», заявляю о согласии на распространение МКУ «Цифра.ФТ» моих персональных данных с целью размещения информации обо мне на информационном (ых) ресурсе (ах) в следующем порядке:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да/нет)	Разрешаю к распространению неограниченному кругу	Условия и запреты	Дополнительные условия
-------------------------------	------------------------------	-------------------------------------	--	-------------------	------------------------

			лиц (да/нет)		
общие персональные данные	фамилия				
	имя				
	отчество				
	год рождения				
	месяц рождения				
	дата рождения				
	место рождения				
	адрес				
	семейное положение				
	образование				
	профессия				
	ИНН				
	СНИЛС				
	контактный телефон				
	паспортные данные				
сведения о трудовом стаже					
отношение к воинской обязанности					

биометрические персональные данные	цветное, цифровое, фотографическое изображение лица				
	видеоматериалы с моим изображением				

Сведения об информационных ресурсах МКУ «Цифра.ФТ», посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными

Данное согласие действует до достижения целей обработки персональных данных или в течение установленного нормативными правовыми актами срока хранения информации. Данное согласие может быть отозвано в любой момент по моему письменному заявлению в произвольной форме.

В случае получения требования МКУ «Цифра.ФТ» обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

Субъект персональных данных: \_\_\_\_\_

(подпись)

(ФИО)

«\_\_» \_\_\_\_\_ 20\_\_ г.

Приложение № 13 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № 10/102-23/17

УТВЕРЖДЕН  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № 10/102-23/17

Перечень информационных систем, в которых осуществляется  
обработка персональных данных в муниципальном казенном  
учреждении «Цифра.ФТ»

1. Сервис для управления задачами и проектами «Яндекс Трекер».
2. Корпоративная почта.
3. Программный комплекс «1С:Бухгалтерия 8».
4. Программный комплекс «1С:Зарплаты и кадры государственного учреждения 8».
5. Информационная платформа «Nextcloud».
6. Официальный сайт учреждения (<https://cifra.sirius-ft.ru>).
7. Система электронного документооборота администрации федеральной территории «Сириус» (ГИС СЭД Сириус»).
8. Государственная информационная система «Единый цифровой профиль жителя и гостя федеральной территории «Сириус» (ГИС ЕЦП).
9. Государственная информационная система «Единая цифровая образовательная среда федеральной территории «Сириус» (ГИС ЕЦОС).
10. Государственная информационная система «Цифровая спортивная платформа федеральной территории «Сириус» (ГИС ЦСП).
11. Информационная система «Цифровой двойник» федеральной территории «Сириус».
12. Система видеонаблюдения в федеральной территории «Сириус».
13. Аппаратно-программный комплекс «Ситуационный центр главы администрации федеральной территории «Сириус».
14. Система оповещения населения федеральной территории «Сириус».
15. Интеллектуальная транспортная система. Автоматизированная система управления дорожным движением и светофорным хозяйством федеральной территории «Сириус».
16. Программное обеспечение спутникового мониторинга средств индивидуальной мобильности в границах федеральной территории «Сириус».
17. Программное решение, автоматизирующее деятельность Административной комиссии федеральной территории «Сириус».
18. Информационная система обеспечения учета и управления имуществом - земельным комплексом федеральной территории «Сириус».
19. Государственная информационная система обеспечения градостроительной деятельности с функциями автоматизированной информационно-аналитической поддержки осуществления полномочий в области градостроительной деятельности и адаптированными возможностями

территориальной геоинформационной системы федеральной территории «Сириус».

20. Информационная система многофункционального центра предоставления государственных и муниципальных услуг в федеральной территории «Сириус».

21. Программно-аппаратный комплекс оценки качества обслуживания заявителей в муниципальном казенном учреждении «Центр социальной поддержки федеральной территории «Сириус».

22. Программный комплекс «Региональный электронный бюджет. Бюджетное планирование» (ПК «Web-Планирование») в части формирования и ведения государственных программ федеральной территории «Сириус».

23. Программный комплекс «Катарсис: Соцзащита» для автоматизации функций в сфере социальной защиты населения в администрации федеральной территории «Сириус».

24. Система электронных библиотек «Ирбис».

25. Информационные системы (подсистемы) АПК «Безопасный город».

Приложение № 14 к приказу  
директора МКУ «Цифра.ФТ»  
от 26.03.2026 № 4/10/102-23/17

УТВЕРЖДЕН  
приказом директора  
МКУ «Цифра.ФТ»  
от 26.03.2026 № 4/10/102-23/17

## Перечень персональных данных, обрабатываемых в муниципальном казенном учреждении «Цифра.ФТ»

1. В целях ведения кадрового и бухгалтерского учета, в муниципальном казенном учреждении «Цифра.ФТ» (далее – Учреждение) обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- год рождения;
- месяц рождения;
- дата рождения;
- место рождения;
- семейное положение;
- доходы работников;
- адрес электронной почты;
- адрес места жительства;
- адрес регистрации;
- номер телефона;
- СНИЛС;
- ИНН;
- гражданство;
- данные документа, удостоверяющего личность;
- реквизиты банковской карты;
- номер расчетного счета;
- номер лицевого счета;
- профессия;
- должность;
- сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);
- отношение к воинской обязанности, сведения о воинском учете; сведения об образовании;
- фотография для карточки Т2;
- сведения о составе семьи;
- реквизиты свидетельств государственной регистрации актов гражданского состояния и содержащиеся в них сведения;
- сведения об образовании (наименование образовательной и (или) иной организации, год окончания, уровень профессионального образования, реквизиты документов об образовании, направление подготовки,

специальность

и квалификация по документу об образовании, ученая степень, ученое звание (дата присвоения, реквизиты диплома, аттестата);

- сведения о дополнительном профессиональном образовании (профессиональной переподготовке, повышении квалификации) (наименование образовательной и (или) научной организации, год окончания, реквизиты документа о переподготовке (повышении квалификации), квалификация и специальность по документу о переподготовке (повышении квалификации), наименование программы обучения, количество часов обучения).

2. В целях осуществления подбора сотрудников Учреждения (соискание вакантных должностей), в Учреждении обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- год рождения;
- месяц рождения;
- дата рождения;
- место рождения;
- семейное положение;
- адрес электронной почты;
- адрес места жительства;
- адрес регистрации;
- номер телефона;
- гражданство;
- данные документа, удостоверяющего личность;
- сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);
- отношение к воинской обязанности, сведения о воинском учете; сведения об образовании;
- сведения об образовании (наименование образовательной и (или) иной организации, год окончания, уровень профессионального образования, реквизиты документов об образовании, направление подготовки, специальность и квалификация по документу об образовании, ученая степень, ученое звание (дата присвоения, реквизиты диплома, аттестата);

- сведения о дополнительном профессиональном образовании (профессиональной переподготовке, повышении квалификации) (наименование образовательной и (или) научной организации, год окончания, реквизиты документа о переподготовке (повышении квалификации), квалификация и специальность по документу о переподготовке (повышении квалификации), наименование программы обучения, количество часов обучения).

3. В целях рассмотрения поступающих обращений граждан, в Учреждении обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- адрес электронной почты;
- адрес места жительства;

- адрес регистрации;
- номер телефона;
- иные, указанные субъектом персональных данных в обращении сведения.

4. В информационных системах, оператором которых является Учреждение могут обрабатываться следующие персональные данные:

- фамилия, имя, отчество;
- год рождения;
- месяц рождения;
- дата рождения;
- место рождения;
- социальное положение;
- пол;
- адрес электронной почты;
- адрес места жительства;
- адрес регистрации;
- номер телефона;
- СНИЛС;
- ИНН;
- гражданство;
- данные документа, удостоверяющего личность;
- данные документа, содержащиеся в свидетельстве о рождении;
- реквизиты банковской карты;
- номер расчетного счета; номер лицевого счета;
- профессия;
- сведения об образовании;
- биометрические данные, характеризующие внешний облик человека;
- иные персональные данные, вносимые пользователями информационных систем в рамках обработки информации.

5. В целях обеспечения пропускного режима в Учреждении обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- данные документа, удостоверяющего личность.