АДМИНИСТРАЦИЯ
ЗАНЕВСКОГО ГОРОДСКОГО ПОСЕЛЕНИЯ
Всеволожского муниципального района Ленинградской области

ПОСТАНОВЛЕНИЕ

20.04.2026 № 386

д. Заневка

Об организации работы с персональными данными в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» администрация Заневского городского поселения Всеволожского муниципального района Ленинградской области

ПОСТАНОВЛЯЕТ:

1. Утвердить Правила обработки персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области согласно приложению № 1.
2. Утвердить Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области согласно приложению № 2.
3. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области согласно приложению № 3.
4. Утвердить Правила работы с обезличенными персональными данными в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области согласно приложению № 4.
5. Утвердить Перечень персональных данных, обрабатываемых в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием

муниципальных услуг и осуществлением муниципальных функций согласно приложению № 5.

6. Утвердить Перечень должностей служащих администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных согласно приложению № 6.

7. Утвердить Перечень должностей служащих администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным согласно приложению № 7.

8. Утвердить Перечень информационных систем персональных данных, обрабатываемых в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области, согласно приложению № 8.

9. Утвердить должностную инструкцию ответственного за организацию обработки персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области согласно приложению № 9.

10. Утвердить типовое обязательство служащего администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей согласно приложению № 10.

11. Утвердить типовую форму согласия на обработку персональных данных служащих администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области, иных субъектов персональных данных согласно приложению № 11.

12. Утвердить типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные согласно приложению № 12.

13. Утвердить Порядок доступа в помещения, в которых ведётся обработка персональных данных, в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области согласно приложению № 13.

14. Утвердить Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области согласно приложению № 14.

15. Утвердить Инструкцию по организации антивирусной защиты в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области согласно приложению № 15.

16. Утвердить Инструкцию пользователя информационной системы персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области согласно приложению № 16.

17. Утвердить Инструкцию пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области согласно приложению № 17.

18. Утвердить Положение о разрешительной системе допуска пользователей и обслуживающего персонала к информационным ресурсам и системе защиты персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области согласно приложению № 18.

19. Признать утратившими силу:

- постановление администрации МО «Заневское сельское поселение» от 25.09.2013 № 435 «Об утверждении Положения о порядке хранения и использования персональных данных МО «Заневское сельское поселение»;

- постановление администрации МО «Заневское городское поселение» от 20.06.2016 № 324 «О мерах, направленных на реализацию постановления Правительства Российской Федерации от 21.03.2012 № 211»;

- постановление администрации МО «Заневское городское поселение» от 20.06.2016 № 326 «Об утверждении перечня информационных систем персональных данных администрации МО «Заневское городское поселение».

20. Настоящее постановление подлежит опубликованию в сетевом издании «Заневский вестник»: http://www.zanevkasmi.ru и размещению на официальном сайте муниципального образования http://www.zanevkaorg.ru.

21. Настоящее постановление вступает в силу после его официального опубликования в сетевом издании «Заневский вестник»: http://www.zanevkasmi.ru.

22. Контроль за исполнением настоящего постановления возложить на первого заместителя главы администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области Гришко О.В.

Глава администрации А.В. Гердий

Приложение № 1
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Правила
обработки персональных данных в администрации
Заневского городского поселения Всеволожского муниципального района
Ленинградской области

1. Общие положения

1.1. Правила обработки персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – правила, администрация) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, цели обработки персональных данных, а также определяют 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.

1.2. Обработка персональных данных в администрации осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в области персональных данных, а также Правилами.

Лица, допущенные к обработке персональных данных, под роспись знакомятся с настоящими правилами и подписывают обязательство о неразглашении информации, содержащей персональные данные.

2. Цели обработки персональных данных и категории субъектов персональных данных

2.1. В администрации персональные данные могут обрабатываться в целях:

1) обеспечения кадровой работы, в том числе кадрового учета, делопроизводства, содействия в осуществлении служебной (трудовой) деятельности, формирования кадрового резерва, обучения и должностного роста, учета результатов исполнения должностных обязанностей, обеспечения личной безопасности субъектов персональных данных, установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, а также в целях противодействия коррупции;

2) осуществления полномочий по решению вопросов местного значения, предусмотренных Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации»;

3) рассмотрения обращений и заявлений граждан, предоставления муниципальных услуг.

2.2. Категории субъектов персональных данных, персональные данные которых обрабатываются в администрации:

1) муниципальные служащие администрации;

2) работники администрации, замещающие должности, не являющиеся должностями муниципальной службы;

3) граждане, претендующие на замещение должностей муниципальной службы в администрации;

4) работники, замещающие должности на основании трудового договора в подведомственных администрации учреждениях;

5) граждане, претендующие на замещение должностей руководителей в подведомственных администрации учреждениях;

6) лица, состоящие в родстве (свойстве) с субъектами персональных данных, указанными в подпунктах 1 - 5 настоящего пункта: близкие родственники (отец, мать, братья, сестры, дети), а также супруга (супруг), в том числе бывшая (бывший), супруги братьев и сестер, братья и сестры супругов;

7) лица, представляемые к награждению, наградные материалы по которым представлены в администрацию;

8) лица, привлекаемые к административной ответственности в порядке, предусмотренном действующим законодательством;

9) лица, принимающие участие в рассмотрении дел с участием администрации в судах Российской Федерации;

10) лица, в отношении которых осуществляется муниципальный контроль;

11) лица, обратившиеся в администрацию в соответствии с законодательством Российской Федерации, в том числе в соответствии с Федеральными законами от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

12) иные физические лица, с которыми администрация взаимодействует в рамках осуществления полномочий.

3. Процедуры, направленные на выявление и предотвращение нарушений законодательства в сфере персональных данных

3.1. Для выявления и предотвращения нарушений, предусмотренных законодательством Российской Федерации в сфере персональных данных, в администрации используются следующие процедуры:

3.1.1. Назначение ответственного за организацию обработки

персональных данных;

3.1.2. Применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с частями 1 и 2 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ);

3.1.3. Осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, требованиями к обеспечению безопасности персональных данных, нормативным правовым актам администрации в отношении обработки персональных данных;

3.1.4. Оценка вреда, который может быть причинен субъектам персональным данных в случае нарушения законодательства Российской Федерации и настоящих Правил;

3.1.5. Ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных и настоящими правилами;

3.1.6. Запрет на обработку персональных данных лицами, не допущенными к их обработке.

4. Порядок обработки персональных данных

4.1. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации:

Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных».

При эксплуатации автоматизированных систем необходимо соблюдать требования:

к работе допускаются только лица, назначенные распоряжением администрации;

на ПЭВМ, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы);

на период обработки защищаемой информации в помещении должны находиться только лица, допущенные в установленном порядке к обрабатываемой информации; допуск других лиц в указанный период может осуществляться с разрешения главы администрации.

4.2. Порядок обработки персональных данных без использования средств автоматизации:

Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка) может осуществляться в виде документов на бумажных носителях.

При неавтоматизированной обработке различных категорий

персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

При неавтоматизированной обработке персональных данных на бумажных носителях:

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

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

документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

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

типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, наименование администрации, 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 администрацией способов обработки персональных данных;

типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получение письменного согласия на обработку персональных данных;

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;

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

Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с

сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление).

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

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 персональных данных;

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.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5. Сроки обработки и хранения обрабатываемых персональных данных

5.1. Сроки обработки и хранения персональных данных определяются:

приказ Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»;

сроком исковой давности;

иными требованиями законодательства Российской Федерации и муниципальными правовыми актами администрации.

5.2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

5.3. Сроки хранения персональных данных, обрабатываемых в информационных системах, должны соответствовать срокам хранения документов на бумажных носителях, содержащих персональные данные.

5.4. Обработка персональных данных прекращается в случаях:

1) выявления факта неправомерной обработки персональных данных;

2) достижения цели обработки персональных данных или утраты необходимости в её достижении;

3) отзыва субъектом персональных данных согласия на обработку его персональных данных, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами;

4) обращения субъекта персональных данных с требованием о прекращении обработки его персональных данных, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

5.5. В случае прекращения обработки персональных данных предпринимаются меры, предусмотренные статьей 21 Федерального закона № 152-ФЗ.

6. Порядок уничтожения обработанных персональных данных

6.1. Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

6.2. Уничтожение обработанных персональных данных производится комиссией администрации с составлением соответствующего акта.

Приложение № 2
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от _____ № _____

Правила
рассмотрения запросов субъектов персональных данных
или их представителей в администрации Заневского городского поселения
Всеволожского муниципального района Ленинградской области

1. Настоящие Правила определяют порядок рассмотрения запросов субъектов персональных данных или их представителей в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – администрация).

2. В соответствии с частью 1 и 7 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (далее – сведения), в том числе содержащей:

подтверждение факта обработки персональных данных в администрации;

правовые основания и цели обработки персональных данных;

цели и применяемые в администрации способы обработки персональных данных;

полное наименование и место нахождения администрации, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с администрацией или на основании федерального закона;

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 в администрации;

порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;

информацию об осуществленной или предполагаемой трансграничной передаче персональных данных;

полное наименование организации или фамилию, имя, отчество (при наличии) и адрес лица, осуществляющего обработку персональных данных по поручению администрации, если обработка поручена или будет поручена такой организации или лицу;

информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 Федерального закона № 152-ФЗ;

иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

3. Субъект персональных данных вправе требовать от администрации, являющейся оператором, уточнения его персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме. 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.

5. Сведения предоставляются субъекту персональных данных (его представителю) при его обращении либо при получении от него или его представителя запроса. Запрос должен содержать:

номер основного документа, удостоверяющего личность субъекта персональных данных (его представителя);

сведения о дате выдачи указанного документа и выдавшем его органе;

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

подпись субъекта персональных данных (его представителя).

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона № 152-ФЗ, а также в целях ознакомления с обрабатываемыми персональными данными 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 должен содержать обоснование направления повторного запроса.

7. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего требованиям, предусмотренным пунктом 5 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

8. Сведения, указанные в пункте 2 настоящих Правил, предоставляются субъекту персональных данных или его представителю лицом, уполномоченным осуществлять обработку персональных данных в

администрации, в течение десяти рабочих дней с момента обращения либо получения запроса субъекта персональных данных или его представителя.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Приложение № 3
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области

1. Цель внутреннего контроля

1.1. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных осуществляется в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – администрация) с целью проверки соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ).

2. Виды и периодичность внутреннего контроля

2.1. Внутренний контроль соответствия обработки персональных данных осуществляется в администрации в форме плановых и внеплановых проверок.

2.2. Проверки проводятся комиссией по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям, предусмотренным Федеральным законом № 152-ФЗ (далее – Комиссия).

2.3. Плановые проверки проводятся в соответствии с поручением главы администрации не реже одного раза в два года.

2.4. Внеплановые проверки проводятся на основании поступившего в администрацию письменного обращения субъекта персональных данных или его представителя о нарушении правил обработки персональных данных данного субъекта персональных данных (далее – заявитель).

Проведение внеплановой проверки организуется в течение 5 рабочих дней со дня поступления обращения заявителя и не может превышать 30 календарных дней со дня принятия решения о её проведении.

3. Порядок создания Комиссии для осуществления внутреннего контроля

3.1. Комиссия создаётся постановлением администрации из числа сотрудников администрации, допущенных к обработке персональных данных.

3.2. В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.

4. Порядок проведения проверок

4.1. При проведении проверки Комиссией должны быть полностью, объективно и всесторонне установлены:

порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

порядок и условия применения средств защиты информации;

эффективность принимаемых мер по обеспечению безопасности персональных данных;

состояние учёта бумажных и машинных носителей персональных данных;

соблюдение правил доступа к персональным данным;

наличие (отсутствие) фактов несанкционированного доступа к персональным данным;

мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

осуществление мероприятий по обеспечению целостности персональных данных.

4.2. По результатам каждой проверки Комиссией проводится заседание. Решение, принятое на заседании Комиссии, оформляется протоколом по форме согласно приложению к настоящим Правилам.

4.3. При проведении внеплановой проверки Комиссия в течение 5 рабочих дней со дня её окончания направляет заявителю письменный ответ по существу поставленных в его обращении вопросов.

4.4. Протоколы хранятся у председателя Комиссии в течение текущего года, после чего подлежат уничтожению.

4.5. О результатах проверки и мерах, необходимых для устранения нарушений, председатель Комиссии докладывает главе администрации.

Приложение
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области

Протокол
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

«__» _____ 20__ г. комиссией по внутреннему контролю соответствия обработки персональных данных требованиям, предусмотренным Федеральным законом № 152-ФЗ, проведена проверка_____
_____
тема проверки

Проверка осуществлялась в соответствии с требованиями _____
_____

В ходе проверки проверено: _____
_____

Выявленные нарушения: _____
_____

Меры по устранению нарушений: _____
_____

Срок устранения нарушений: _____

Председатель комиссии И.О. Фамилия

Члены комиссии:
Должность _____ И.О. Фамилия
Должность _____ И.О. Фамилия
Должность _____ И.О. Фамилия

Должность руководителя проверяемого подразделения _____ И.О. Фамилия

Приложение № 4
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Правила
работы с обезличенными персональными данными
в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области

1. Условия обезличивания

1.1. Настоящие Правила определяют порядок работы в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – администрация) с обезличенными данными в случае обезличивания персональных данных.

1.2. Обезличивание персональных данных проводится в целях снижения ущерба от разглашения персональных данных, по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении, а также в статистических или иных исследовательских целях.

1.3. При обезличивании персональных данных администрация должна обеспечить:

а) соблюдение Правил обезличивания персональных данных и методов обезличивания персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.08.2025 № 1154 «Об утверждении требований к обезличиванию персональных данных, методов обезличивания персональных данных и Правил обезличивания персональных данных», с учетом требования о предоставлении обезличенных данных;

б) раздельное хранение персональных данных и обезличенных данных;

в) принятие мер по обеспечению безопасности обезличенных данных в соответствии с Федеральным законом «О персональных данных»;

г) исключение из обезличенных данных информации, доступ к которой ограничен федеральными законами;

д) использование алгоритмов и программы для электронных вычислительных машин для обезличивания персональных данных, обеспечивающих возможность предоставления обезличенных данных из информационной системы оператора в государственную информационную систему Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, указанную в статье 13.1 Федерального закона «О персональных данных», без потери таких данных и (или) их изменения;

е) возможность внесения изменений и дополнений в обезличенные данные, поддержку актуальности обезличенных данных и возможность повторного применения методов обезличивания персональных данных,

утвержденных постановлением Правительства Российской Федерации от 01.08.2025 № 1154 «Об утверждении требований к обезличиванию персональных данных, методов обезличивания персональных данных и Правил обезличивания персональных данных», без возможности преобразования обезличенных данных к исходному виду, позволяющему определить их принадлежность конкретному субъекту персональных данных, а также целостность массива обезличенных данных и их соответствие требованию о предоставлении обезличенных данных.

2. Способы обезличивания

2.1. К способам обезличивания персональных данных при условии дальнейшей обработки персональных данных относятся:

1) замена части сведений идентификаторами;

2) обобщение (понижение) точности некоторых сведений;

3) деление сведений на части и обработка их в разных информационных системах;

4) другие способы.

2.2. К способам обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

3. Правила работы с обезличенными данными

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

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

3.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо:

1) использование средств защиты информации;

2) использование антивирусных программ;

3) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных;

4) соблюдение правил работы со съемными носителями (в случае их использования), правил резервного копирования.

3.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо:

1) хранение бумажных носителей в условиях, исключающих доступ к ним посторонних лиц;

2) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных.

Приложение № 5
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от _____ № _____

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций

1. Фамилия, имя, отчество (при наличии), в том числе прежние (в случае их изменения), причины их изменения, дата и место рождения, пол.

2. Сведения о гражданстве (в том числе о предыдущих гражданствах, иных гражданствах).

3. Фотография.

4. Адрес и дата регистрации по месту жительства (месту пребывания), адрес места фактического проживания.

5. Почтовый адрес.

6. Адрес электронной почты (при наличии).

7. Номер телефона (домашний, служебный, мобильный).

8. Вид, серия, номер документа, удостоверяющего личность, наименование подразделения и код подразделения (при наличии), выдавшего его, дата выдачи.

9. Идентификационный номер налогоплательщика.

10. Реквизиты страхового свидетельства обязательного пенсионного страхования, сведения, содержащиеся в нем или документе (электронном документе), подтверждающем регистрацию в системе индивидуального (персонифицированного) учета.

11. Реквизиты страхового медицинского полиса обязательного медицинского страхования, сведения, содержащиеся в нем.

12. Реквизиты свидетельств государственной регистрации актов гражданского состояния.

13. Сведения о владении иностранными языками и языками народов Российской Федерации, степень владения.

14. Сведения об образовании, в том числе о послевузовском профессиональном образовании (полное наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании).

15. Сведения об ученой степени.

16. Сведения о профессиональной переподготовке и (или) повышении квалификации.

17. Сведения о трудовой деятельности, в том числе сведения о трудовой деятельности на условиях совместительства, совмещения, предпринимательской и иной деятельности (включая даты заключения и прекращения трудового договора, даты перевода, перемещения на иную должность, наименование замещаемых должностей с указанием структурных подразделений, размер заработной платы).

18. Сведения о классном чине федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации и (или) муниципальной службы, дипломатическом ранге, воинском и (или) специальном звании, классном чине правоохранительной службы, классном чине юстиции (кем и когда присвоены).

19. Сведения о государственных наградах, иных наградах и знаках отличия (кем награжден(а) и когда).

20. Сведения о семейном положении, составе семьи, близких родственниках (отец, мать, братья, сестры, дети), супругах (в том числе бывших), супругах братьев и сестер, братьях и сестрах супругов: степень родства, фамилия, имя, отчество (при наличии), дата рождения, место рождения, место работы (полное и (если имеется) сокращенное наименование и адрес юридического лица в пределах места нахождения), должность, адрес регистрации по месту жительства (месту пребывания), адрес фактического проживания.

21. Сведения о пребывании за границей (время, место, цель пребывания).

22. Реквизиты документа, удостоверяющего личность гражданина Российской Федерации за пределами территории Российской Федерации (серия, номер, когда и кем выдан).

23. Сведения о близких родственниках (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывших, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей).

24. Сведения о воинском учете, реквизиты документов воинского учета, а также сведения, содержащиеся в них (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу).

25. Сведения о наличии (отсутствии) судимости, в том числе снятой или погашенной.

26. Сведения об оформлении допуска к государственной тайне (имеющемся и (или) имевшихся ранее (форма, реквизиты).

27. Сведения о наличии (отсутствии) заболевания, препятствующего поступлению на муниципальную службу или ее прохождению.

28. Сведения об инвалидности, сроке действия установленной инвалидности.

29. Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и

обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей.

30. Сведения о счетах в банках и кредитных организациях (полное наименование банка или кредитной организации, номер счета и дата открытия).

31. Реквизиты банковских карт (номер карты).

32. Сведения, содержащиеся в трудовом договоре, дополнительных соглашениях к трудовому договору.

33. Сведения об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети «Интернет», на которых муниципальный служащий, гражданин Российской Федерации, претендующий на замещение должности муниципальной службы, размещали общедоступную информацию, а также данные, позволяющие их идентифицировать.

34. Иные персональные данные, соответствующие целям их обработки, которые субъект персональных данных пожелает сообщить о себе.

Приложение № 6
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Перечень
должностей служащих администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

1. Первый заместитель главы администрации.
2. Заместитель главы администрации по экономике и финансам.
3. Начальник отдела бухгалтерского учета и отчетности – централизованной бухгалтерии.
4. Главный специалист отдела бухгалтерского учета и отчетности – централизованной бухгалтерии.
5. Ведущий специалист отдела бухгалтерского учета и отчетности – централизованной бухгалтерии.
6. Начальник сектора муниципальной службы и кадровой работы.
7. Главный специалист сектора муниципальной службы и кадровой работы.
8. Ведущий специалист сектора муниципальной службы и кадровой работы.
9. Инспектор военно-учетного стола.

Приложение № 7
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Перечень
должностей служащих администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

1. Глава администрации.
2. Первый заместитель главы администрации.
3. Заместитель главы администрации по экономике и финансам.
4. Заместитель главы администрации по архитектуре и земельным вопросам.
5. Заместитель главы администрации по безопасности и социальному развитию.
6. Заместитель главы администрации по ЖКХ и благоустройству.
7. Начальник отдела бухгалтерского учета и отчетности – централизованной бухгалтерии.
8. Начальник сектора муниципальной службы и кадровой работы.
9. Начальник отдела по организационным и общим вопросам.
10. Начальник юридического отдела.
11. Начальник отдела муниципального заказа.
12. Начальник сектора бюджетного планирования и социально-экономического развития.
13. Начальник сектора по управлению муниципальным имуществом, учёта и распределения муниципального жилищного фонда.
14. Начальник отдела архитектуры, градостроительства и территориального планирования.
15. Начальник сектора землеустройства и муниципального земельного контроля.
16. Начальник отдела ГОЧС и безопасности.
17. Начальник отдела культуры, спорта, молодёжной политики и туризма.
18. Начальник сектора по взаимодействию с общественностью, организациями и населением.
19. Начальник сектора архивной работы.
20. Начальник сектора делопроизводства.
21. Начальник сектора дорожного хозяйства.
22. Начальник сектора благоустройства.

23. Начальник отдела ЖКХ.

24. Заместитель начальника юридического отдела.

25. Заместитель начальника отдела муниципального заказа.

26. Главный специалист отдела бухгалтерского учета и отчетности – централизованной бухгалтерии.

27. Ведущий специалист отдела бухгалтерского учета и отчетности – централизованной бухгалтерии.

28. Главный специалист сектора муниципальной службы и кадровой работы.

29. Ведущий специалист сектора муниципальной службы и кадровой работы.

30. Главный специалист отдела по организационным и общим вопросам.

31. Ведущий специалист отдела по организационным и общим вопросам.

32. Главный специалист сектора архивной работы.

33. Ведущий специалист сектора архивной работы.

34. Главный специалист сектора делопроизводства.

35. Ведущий специалист сектора делопроизводства.

36. Главный специалист юридического отдела.

37. Ведущий специалист юридического отдела.

38. Главный специалист отдела муниципального заказа.

39. Ведущий специалист отдела муниципального заказа.

40. Главный специалист сектора бюджетного планирования и социально-экономического развития.

41. Ведущий специалист сектора бюджетного планирования и социально-экономического развития.

42. Главный специалист сектора по управлению муниципальным имуществом, учёта и распределения муниципального жилищного фонда.

43. Ведущий специалист сектора по управлению муниципальным имуществом, учёта и распределения муниципального жилищного фонда.

44. Главный специалист отдела архитектуры, градостроительства и территориального планирования.

45. Ведущий специалист отдела архитектуры, градостроительства и территориального планирования.

46. Главный специалист сектора землеустройства и муниципального земельного контроля.

47. Ведущий специалист сектора землеустройства и муниципального земельного контроля.

48. Главный специалист отдела ГОЧС и безопасности.

49. Ведущий специалист отдела ГОЧС и безопасности.

50. Главный специалист отдела культуры, спорта, молодёжной политики и туризма.

51. Ведущий специалист отдела культуры, спорта, молодёжной политики и туризма.

52. Главный специалист сектора по взаимодействию с общественностью, организациями и населением.

53. Ведущий специалист сектора по взаимодействию с общественностью.

54. Главный специалист сектора дорожного хозяйства.

55. Ведущий специалист сектора дорожного хозяйства.

56. Главный специалист сектора благоустройства.

57. Ведущий специалист сектора благоустройства.

58. Главный специалист отдела ЖКХ.

59. Ведущий специалист отдела ЖКХ.

60. Инспектор военно-учетного стола.

Приложение № 8
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Перечень информационных систем персональных данных, обрабатываемых в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области

1. Информационная система «1С: Предприятие»
2. Система электронного документооборота Ленинградской области
3. Прикладное программное обеспечение автоматизированной системы Федерального казначейства «Система удаленного финансового документооборота» (ППО «СУФД»)
4. Государственная информационная система о государственных и муниципальных платежах
5. ССТУ РФ «Результаты рассмотрения обращений граждан»
6. Автоматизированная информационная система Межведомственного электронного взаимодействия Ленинградской области (АИС «Межвед ЛО»)
7. Государственная информационная система Ленинградской области «Единая информационная система учёта граждан, проживающих в Ленинградской области, нуждающихся в улучшении жилищных условий» (ГИС ЛО «Жильё»)
8. Государственная информационная система «АИС Управления имуществом Ленинградской области»
9. Федеральная государственная информационная система «Единая система предоставления государственных и муниципальных услуг (сервисов)» (Платформа государственных сервисов, ПГС)
10. Государственная информационная система «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» (ГИС ТОР КНД»)
11. Государственная информационная система «Единый реестр видов федерального государственного контроля (надзора), регионального государственного контроля (надзора), муниципального контроля» (ЕРВК)
12. Информационная система «ТехноКад-Муниципалитет»
13. Федеральная информационная адресная система (ФИАС)
14. Автоматизированная информационная система «Государственный заказ Ленинградской области» (АИС «ГосЗаказ»)
15. Единая информационная система (ЕИС) в сфере закупок
16. Государственная информационная система жилищно-коммунального хозяйства (ГИС ЖКХ)
17. Автоматизированная информационная система «Мониторинг МСП»

Приложение № 9
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Должностная инструкция
ответственного за организацию обработки персональных данных
в администрации Заневского городского поселения Всеволожского
муниципального района Ленинградской области

1. Ответственный за организацию обработки персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – администрация) назначается распоряжением администрации.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Правилами обработки персональных данных в администрации, настоящей должностной инструкцией.

2. Ответственный за организацию обработки персональных данных обязан:

2.1. Организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в администрации, от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий.

2.2. Получать от сотрудников администрации, осуществляющих обработку персональных данных, обязательство о неразглашении информации, содержащей персональные данные.

2.3. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов в администрации.

2.4. Предоставлять субъекту персональных данных либо его представителю по запросу информацию об обработке его персональных данных.

2.5. Осуществлять внутренний контроль за соблюдением требований законодательства Российской Федерации и Правил обработки персональных данных, в том числе требований к защите персональных данных.

2.6. Доводить до сведения лиц, допущенных к обработке персональных данных, положения федерального законодательства Российской Федерации о персональных данных, нормативных правовых актов администрации по

вопросам обработки персональных данных, требований к защите персональных данных.

3. Ответственный за организацию обработки персональных данных вправе:

3.1. Иметь доступ к информации, касающейся обработки персональных данных в администрации, и включающей:

цели обработки персональных данных;

категории обрабатываемых персональных данных;

категории субъектов персональных данных, персональные данные которых обрабатываются;

правовые основания обработки персональных данных;

перечень действий с персональными данными, общее описание используемых в администрации способов обработки персональных данных;

описание мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27.07.2006 № 152-ФЗ «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 при их обработке в информационных системах персональных данных.

3.2. Привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в администрации, иных муниципальных служащих администрации с возложением на них соответствующих обязанностей и закреплением ответственности.

Приложение № 10
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Типовое обязательство
служащего администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора (контракта) прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я, _____,
(фамилия, имя, отчество (при наличии)

замещающий (замещающая) должность: _____ _
_____,
(указывается замещаемая должность)

обязуюсь прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен (уведомлена) о том, что персональные данные являются конфиденциальной информацией и обязан (обязана) не раскрывать третьим лицам и не распространять их без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Положения законодательства Российской Федерации, предусматривающие ответственность за нарушение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», мне разъяснены.

Приложение № 11
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Типовая форма согласия на обработку персональных данных служащих администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области, иных субъектов персональных данных

г. _____ «__» _____ 20__ г.

Я, _____,
(фамилия, имя, отчество)
зарегистрированный(ая) по адресу: _____
_____,
паспорт серия _____ № _____, выдан _____, _____
(дата) (кем выдан)
_____,
свободно, своей волей и в своем интересе даю согласие уполномоченным должностным лицам администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – администрация), расположенной по адресу:
_____,
на обработку (любое действие (операцию) 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) следующих персональных данных:

1. Фамилия, имя, отчество (при наличии), в том числе прежние (в случае их изменения), причины их изменения.
2. Пол.
3. Дата рождения (число, месяц, год).
4. Место рождения.
5. Сведения о гражданстве (в том числе о предыдущих гражданствах, иных гражданствах).

6. Вид, серия, номер документа, удостоверяющего личность, наименование подразделения и код подразделения (при наличии), выдавшего его, дата выдачи.

7. Фотография.

8. Адрес и дата регистрации по месту жительства (месту пребывания), адрес места фактического проживания.

9. Номер телефона (домашний, служебный, мобильный).

10. Почтовый адрес.

11. Адрес электронной почты (при наличии).

12. Идентификационный номер налогоплательщика.

13. Реквизиты страхового медицинского полиса обязательного медицинского страхования, сведения, содержащиеся в нем.

14. Реквизиты страхового свидетельства обязательного пенсионного страхования, сведения, содержащиеся в нем или документе (электронном документе), подтверждающем регистрацию в системе индивидуального (персонифицированного) учета.

15. Реквизиты свидетельств государственной регистрации актов гражданского состояния.

16. Сведения о воинском учете, реквизиты документов воинского учета, а также сведения, содержащиеся в них.

17. Сведения о семейном положении, составе семьи, близких родственниках (отец, мать, братья, сестры, дети), супругах (в том числе бывших), супругах братьев и сестер, братьях и сестрах супругов: степень родства, фамилия, имя, отчество (при наличии), дата рождения, место рождения, место работы (полное и (если имеется) сокращенное наименование и адрес юридического лица в пределах места нахождения), должность, адрес регистрации по месту жительства (месту пребывания), адрес места фактического проживания.

18. Сведения об образовании, в том числе о послевузовском профессиональном образовании (полное наименование и год окончания образовательной организации, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании).

19. Сведения об ученой степени.

20. Сведения о профессиональной переподготовке и (или) повышении квалификации.

21. Сведения о владении иностранными языками и языками народов Российской Федерации, степень владения.

22. Сведения о наличии (отсутствии) заболевания, препятствующего поступлению на федеральную государственную гражданскую службу или ее прохождению, а также медицинское заключение об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну (в случае оформления допуска к сведениям, составляющим государственную и иную охраняемую законом тайну).

23. Сведения об инвалидности, сроке действия установленной инвалидности.

24. Сведения о трудовой деятельности (в том числе о прохождении государственной гражданской службы, включая дату, основания поступления на государственную гражданскую службу и назначения на должность государственной гражданской службы, дату, основания назначения, перевода, перемещения на иную должность государственной гражданской службы, наименование замещаемых должностей государственной гражданской службы с указанием структурных подразделений, размер денежного содержания (заработной платы), результаты аттестации на соответствие замещаемой должности государственной гражданской службы (работы), в том числе сведения о трудовой деятельности на условиях совместительства, совмещения, предпринимательской и иной деятельности).

25. Сведения о классном чине федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации и (или) муниципальной службы, дипломатическом ранге, воинском и (или) специальном звании, классном чине правоохранительной службы, классном чине юстиции (кем и когда присвоены).

26. Сведения о пребывании за границей (время, место, цель пребывания).

27. Реквизиты документа, удостоверяющего личность гражданина Российской Федерации за пределами территории Российской Федерации (серия, номер, когда и кем выдан).

28. Сведения о наличии (отсутствии) судимости, в том числе снятой или погашенной.

29. Сведения об оформлении допуска к государственной тайне (имеющемся и или) имевшихся ранее (форма, реквизиты).

30. Сведения о государственных наградах, иных наградах и знаках отличия.

31. Сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания.

32. Сведения о своих доходах, расходах, об имуществе и обязательствах имущественного характера, а также сведения о доходах, расходах, об имуществе и обязательствах имущественного характера своих супруга (супруги) и несовершеннолетних детей.

33. Сведения о счетах в банках и кредитных организациях (полное наименование банка или кредитной организации, номер счета и дата открытия).

34. Реквизиты банковских карт (номер карты).

35. Сведения, содержащиеся в служебном контракте, трудовом договоре, дополнительных соглашениях к служебному контракту, трудовому договору.

36. Сведения о близких родственниках (отец, мать, братья, сестры, дети), супругах (в том числе бывших), супругах братьев и сестер, братьях и сестрах супругов, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство: фамилия, имя, отчество (при наличии), с какого времени проживают за границей.

37. Сведения об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети «Интернет», на которых муниципальный служащий, гражданин Российской Федерации, претендующий на замещение должности муниципальной службы, размещали общедоступную информацию, а также данные, позволяющие их идентифицировать.

38. Персональный идентификатор.

39. Иные персональные данные, соответствующие целям их обработки, которые я пожелаю сообщить о себе.

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с поступлением на муниципальную службу Российской Федерации (работу), ее прохождением и прекращением (трудовых и непосредственно связанных с ними отношений) для реализации функций, возложенных на администрацию действующим законодательством.

Персональные данные, а именно: фамилию, имя, отчество (при наличии) разрешаю использовать в качестве общедоступных в электронной почте и системе электронного документооборота администрации, а также в иных случаях, предусмотренных законодательством Российской Федерации об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления.

Я ознакомлен(а), что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока муниципальной службы (работы) в администрации;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных администрация вправе продолжить обработку 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 от 27.07.2006 № 152-ФЗ «О персональных данных»;

4) после увольнения с муниципальной службы (прекращения трудовых отношений) персональные данные хранятся в администрации в течение срока хранения документов, предусмотренного действующим законодательством Российской Федерации;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения функций, возложенных законодательством Российской Федерации на администрацию.

Дата начала обработки персональных данных:

_____ _____

(число, месяц, год) (подпись)

Приложение № 12
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Типовая форма разъяснения
субъекту персональных данных юридических последствий отказа
предоставить свои персональные данные

В соответствии с Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», статьями 65, 86 Трудового кодекса Российской Федерации определен перечень персональных данных, который субъект персональных данных обязан предоставить в связи с поступлением или прохождением муниципальной службы (работы). Без представления субъектом персональных данных обязательных для заключения служебного контракта (трудового договора) сведений служебный контракт (трудовой договор) не может быть заключен.

На основании пункта 11 статьи 77 Трудового кодекса Российской Федерации служебный контракт (трудовой договор) прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности (продолжения работы).

Мне, _____,
(фамилия, имя, отчество)
разъяснены юридические последствия отказа предоставить свои персональные данные.

_____ _____
(число, месяц, год) (подпись)

Приложение № 13
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Порядок доступа в помещения,
в которых ведётся обработка персональных данных, в администрации
Заневского городского поселения Всеволожского муниципального района
Ленинградской области

1. Порядок доступа служащих администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – администрация) в помещения, в которых ведется обработка персональных данных (далее – Порядок) определяет правила доступа в помещения, в которых хранятся и обрабатываются персональные данные, в целях исключения несанкционированного доступа к персональным данным, а также обеспечения безопасности персональных данных от уничтожения, изменения, блокирования, копирования, распространения, а также от неправомерных действий в отношении персональных данных.

2. К помещениям, в которых ведется обработка персональных данных, относятся помещения, в которых происходит обработка персональных данных, как с использованием средств автоматизации, так и без таковых, а также хранятся резервные копии персональных данных и ключевые документы к ним.

3. Доступ в помещения администрации, в которых ведется обработка персональных данных, осуществляется в соответствии с Перечнем должностей служащих администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, указанным в приложении № 7 к настоящему постановлению (далее – Перечень).

4. Для помещений, в которых ведется обработка персональных данных, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащих персональные данные, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Данный режим должен обеспечиваться в том числе:

запиранием помещения на ключ, в том числе при выходе из него в рабочее время;

закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие персональные данные, во время отсутствия в помещении служащих администрации, замещающих должности, предусмотренные Перечнем.

5. Доступ посторонних лиц в помещения, в которых ведется обработка персональных данных, возможен только ввиду служебной необходимости.

На момент присутствия посторонних лиц в помещении, в котором ведется обработка персональных данных, должны быть приняты меры по недопущению ознакомления посторонних лиц с персональными данными.

6. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на ответственного за организацию обработки персональных данных в администрации.

Приложение № 14
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Порядок
резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области

1. Общие положения

1.1. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты персональных данных (далее – Порядок) определяет порядок действий, направленных на восстановление работоспособности информационной системы персональных данных (далее – ИСПДн) администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – администрация), а также меры защиты от потери информации и действия по восстановлению информации в случае её потери.

1.2. Действие настоящего Порядка распространяется на все информационные системы администрации, в которых осуществляется обработка персональных данных, и всех пользователей ИСПДн.

2. Порядок действий, направленных на восстановление работоспособности ИСПДн

2.1. Нарушение работоспособности ИСПДн, потеря информации могут произойти в результате:

- непреднамеренных действий пользователей;
- преднамеренных действий пользователей и третьих лиц;
- нарушения правил эксплуатации технических средств ИСПДн;
- возникновения нештатных ситуаций и обстоятельств непреодолимой силы (далее – инциденты).

Ответственный за организацию обработки персональных данных в администрации и администратор ИСПДн обеспечивают своевременное реагирование на инциденты, приводящие к нарушению работоспособности ИСПДн, потере защищаемой информации, обеспечивают проведение мероприятий по предотвращению инцидентов, приводящих к нарушению работоспособности ИСПДн, потере защищаемой информации.

2.2. В кратчайший срок, не превышающий одного рабочего дня, ответственный за организацию обработки персональных данных в администрации и администратор ИСПДн предпринимают меры по восстановлению работоспособности ИСПДн.

2.3. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

2.4. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов.

2.5. При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы и по согласованию с администратором ИСПДн оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации.

Работа с использованием неисправных технических средств запрещается.

2.6. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты.

2.7. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

3. Меры защиты от потери информации и действия по восстановлению информации

3.1. К мерам защиты от потери информации и действиям по восстановлению информации в случае её потери, относятся:

- резервное копирование;
- контроль резервного копирования;
- хранение резервных копий;
- полное или частичное восстановление данных и приложений.

3.2. Резервному копированию подлежит информация следующих основных категорий:

- персональная информация субъектов персональных данных;
- групповая информация пользователей;
- информация, необходимая для восстановления серверов и систем управления базами данных;
- персональные профили пользователей сети;
- информация автоматизированных систем, в т.ч. базы данных;

- рабочие копии установочных компонентов программного обеспечения рабочих станций;

- регистрационная информация системы информационной безопасности автоматизированных систем.

3.3. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на твердом носителе (жесткий диск и т.п.).

3.4. Администратор ИСПДн производит резервное копирование вручную и/или настраивает задания для ПО, осуществляющего резервное копирование, на автоматическое выполнение в соответствии с перечнем информационных ресурсов, подлежащих резервному копированию, и графиком резервного копирования.

Перед выполнением задания резервного копирования администратор ИСПДн проверяет доступность резервного носителя, а также наличие на нем свободного места для записи данных.

После завершения выполнения задачи резервного копирования администратор ИСПДн должен извлечь резервный носитель (если используется съемный носитель), подписать его по формату «число, месяц, год, номер» и поместить в сейф (запираемый шкаф, ящик).

При создании резервных копий на сетевые хранилища – доступ к сетевым хранилищам должен быть ограничен. Доступ должен иметь только администратор ИСПДн.

Резервные копии должны храниться не менее года, для возможности восстановления данных.

3.5. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже одного раза в неделю;

- для технологической информации – не реже одного раза в месяц;

- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже одного раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в журнале учета.

3.6. В случае необходимости восстановление данных из резервных копий производится на основании заявки сотрудника администрации – пользователя ИСПДн.

После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

3.7. Процедура восстановления информации из резервной копии осуществляется администратором ИСПДн.

Приложение № 15
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Инструкция
по организации антивирусной защиты в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области

1.1. Настоящая инструкция по организации антивирусной защиты в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – Инструкция, администрация) определяет порядок организации антивирусной защиты в информационных системах персональных данных (далее – ИСПДн) администрации.

1.2. Контроль за соблюдением настоящей Инструкции сотрудниками администрации, имеющими доступ к персональным данным, осуществляет администратор ИСПДн.

2. Основы организации антивирусной защиты

2.1. Для защиты ИСПДн в администрации на компьютерах всех сотрудников администрации, имеющих доступ к персональным данным, устанавливается антивирусное программное обеспечение.

Антивирусное программное обеспечение должно обеспечивать обнаружение в информационных системах администрации компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

2.2. Антивирусное программное обеспечение устанавливается администратор ИСПДн в соответствии с документацией разработчика (поставщика) антивирусного программного обеспечения.

Администратор ИСПДн обязан поддерживать в актуальном состоянии и регулярно обновлять модули и базы данных антивирусного программного обеспечения.

2.3. Администратор ИСПДн обязан устанавливать только сертифицированное в Российской Федерации антивирусное программное обеспечение, имеющее соответствующую лицензию.

Устанавливаемое антивирусное программное обеспечение должно иметь соответствующие сертификаты безопасности и быть разрешено для работы с информационными системами персональных данных в Российской Федерации.

При использовании антивирусного программного обеспечения необходимо использовать в первую очередь то антивирусное программное обеспечение, которое рассчитано на наиболее широкий диапазон вредоносного программного обеспечения или на вредоносное программное обеспечение, которое не выявляется другими программами.

2.4. Для используемого антивирусного программного обеспечения рекомендуется настроить обновление антивирусных баз и проведение антивирусного контроля в автоматическом режиме без участия сотрудников администрации.

Используемое антивирусное программное обеспечение должно предоставлять возможность автоматического распространения обновлений антивирусных баз на каждое автоматизированное рабочее место (сервер).

Антивирусное программное обеспечение должно быть настроено таким образом, чтобы объекты, подозреваемые на заражение вирусами и их модификациями, помещались в карантин для дальнейшего принятия решения об их лечении либо удалении.

2.5. При каждой загрузке автоматизированного рабочего места (для серверов – при перезапуске) должна проводиться проверка объектов, загрузка которых осуществляется при старте операционной системы, а также проверка системной памяти и загрузочных секторов диска (быстрая проверка).

Обязательно, не реже одного раза в месяц, в автоматическом режиме должен проводиться полный антивирусный контроль всех дисков и файлов в соответствии с документацией разработчика (поставщика) антивирусного программного обеспечения.

2.6. Внеплановый антивирусный контроль должен проводиться в следующих случаях:

- непосредственно после установки (изменения) программного обеспечения;

- при возникновении подозрения на наличие вредоносного программного обеспечения (наличие лишних файлов, нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

2.7. Сотрудник администрации, имеющий доступ к персональным данным, не имеет права:

2.7.1. Устанавливать свои программы на автоматизированное рабочее место, содержащее доступ к информационным системам персональных данных, а также отключать или удалять программы, установленные администратор ИСПДн, самостоятельно изменять настройки и параметры антивирусного программного обеспечения.

2.7.2. Загружать файлы из неизвестных источников, расположенных в информационно-телекоммуникационной сети «Интернет». В случае возникновения сомнений в благонадежности источника сообщать администратор ИСПДн о необходимости проведения проверки.

2.7.3. Загружать и открывать вложения из писем электронной почты, полученных от сомнительных отправителей, или писем с массовой рассылкой многим адресатам. В случае возникновения сомнений в благонадежности источника сообщать администратор ИСПДн о необходимости проведения проверки.

2.7.4. Использовать на автоматизированных рабочих местах неучтенные (личные) съемные носители информации.

2.7.5. Использовать съемные носители информации без служебной необходимости (в личных целях).

2.7.6. Допускать к работе на своем автоматизированном рабочем месте посторонних лиц.

2.8. Администратор ИСПДн обязан проводить инструктаж для сотрудников администрации по использованию антивирусного программного обеспечения, в том числе объяснить порядок действий при использовании съемных носителей и при обнаружении вирусов.

2.9. При использовании съемных носителей информации сотрудник администрации должен сначала проверить их на наличие вирусов, используя антивирусное программное обеспечение.

2.10. Для полученных или разработанных электронного документа или программы сотрудникам администрации рекомендуется создавать резервную копию, с помощью которой можно было бы легко восстановить эти файлы в случае вирусного заражения.

2.11. В случае получения оповещений от антивирусного программного обеспечения о возможном заражении файлов вирусом сотрудник администрации обязан:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных файлов администратора ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

- совместно с владельцем зараженных файлов провести анализ необходимости дальнейшего их использования.

Решение о действиях над объектами, помещенными в карантин антивирусного программного обеспечения (лечение или уничтожение зараженных файлов), принимается администратором ИСПДн.

2.12. Администратор ИСПДн принимает все возможные меры для лечения или уничтожения зараженных файлов, уничтожения вируса, после чего представляет главе администрации отчет о результатах проведенных действий, возможных причинах проникновения вирусов в информационную систему и о мерах, которые необходимо принять, чтобы избежать подобных ситуаций.

2.13. В случае обнаружения заражения автоматизированных рабочих мест (серверов) вирусом администратор ИСПДн выполняет следующие действия:

- централизованно обновляет антивирусные базы сервера администрирования и всех информационных систем;

- проверяет состояние всех информационных систем, наличие зараженных автоматизированных рабочих мест в случае обнаружения пораженных узлов;

- оперативно принимает меры по предотвращению распространения заражения вирусом и при необходимости отключает от сети зараженное автоматизированное рабочее место (сервер);

- проводит действия, направленные на устранение вируса на всех пораженных узлах информационных систем;

- по завершении мероприятий по устранению последствий заражения восстанавливает работоспособность автоматизированного рабочего места и передает его ответственному сотруднику администрации.

2.14. По умолчанию файлы, подозреваемые на заражение вирусами и их модификациями, помещаются антивирусным программным обеспечением в карантин для дальнейшего принятия решения об их лечении либо удалении.

В общем случае зараженные файлы подлежат удалению путем уничтожения файлов на жестком диске либо ином носителе информации. После уничтожения зараженных файлов восстанавливают файлы, используя их резервные копии.

В тех случаях, когда отсутствуют резервные копии зараженных файлов либо восстановление с помощью резервных копий очень трудоемко, к зараженным объектам применяется специальный «лечащий» режим антивирусного программного обеспечения. Использование «лечащего» режима не дает полной гарантии восстановления файла, поэтому после лечения необходима проверка корректности восстановления данного файла.

В любом случае после уничтожения или лечения зараженных файлов и восстановления файлов из резервных копий производится перезагрузка автоматизированного рабочего места через выключение и последующее включение и еще раз выполняется антивирусная проверка с использованием антивирусного программного обеспечения с установленными последними обновлениями.

2.15. Администратор ИСПДн:

2.15.1. Проводит профилактические мероприятия по предотвращению и ограничению вирусных эпидемий, включающие загрузку и развертывание специальных правил нейтрализации (отражения, изоляции и ликвидации) вредоносного программного обеспечения на основе рекомендаций по контролю атак, подготавливаемых разработчиком антивирусного программного обеспечения, до того как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.

2.15.2. Предварительно проверяет устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусного заражения.

2.15.3. Осуществляет уничтожение вирусов на автоматизированных рабочих местах сотрудников и серверах.

2.15.4. Анализирует ситуации появления вирусов и причины их появления.

2.15.5. Принимает меры по предотвращению причин появления вирусов.

2.15.6. Осуществляет непрерывный контроль над всеми возможными путями проникновения вирусов, мониторинг антивирусной безопасности и обнаружение активности вирусов на всех объектах информационных систем.

2.15.7. Проводит регулярные проверки целостности критически важных программ и данных. Для обеспечения бесперебойной работы администрации в случаях вирусного заражения осуществляет регулярное резервное копирование всех необходимых данных и программ.

2.15.8. Проводит периодический контроль работы антивирусного программного обеспечения.

2.15.9. Осуществляет периодический контроль за соблюдением сотрудниками администрации требований настоящей Инструкции.

2.16. Ответственность сотрудников за несоблюдение требований настоящей Инструкции определяется законодательством Российской Федерации, локальными нормативными актами администрации, а также должностными инструкциями сотрудников администрации.

Приложение № 16
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Инструкция
пользователя информационной системы персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области

1. Общие требования по обеспечению безопасности обработки информации в ИСПДн

1.1. К защищаемой информации, обрабатываемой в информационных системах персональных данных администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – ИСПДн, администрация), относятся персональные данные, служебная (технологическая) информация системы защиты, другая информация конфиденциального характера.

1.2. Пользователем является каждый сотрудник администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. К самостоятельной работе на автоматизированных рабочих местах (далее – АРМ), входящих в состав ИСПДн администрации, допускаются лица, изучившие требования настоящей Инструкции и освоившие правила эксплуатации АРМ и технических средств защиты. Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

1.4. Методическое руководство работой пользователя осуществляется администратором ИСПДн и ответственным за организацию обработки персональных данных.

1.5. Вход в помещения, в которых производится автоматизированная обработка защищаемой информации, разрешается постоянно работающим в нем сотрудникам администрации, а также лицам, привлекаемым к проведению ремонтных, наладочных и других работ и посетителей в сопровождении сотрудников администрации.

1.6. Техническое обслуживание АРМ, уборка помещения и т.п. проводятся только под контролем уполномоченного сотрудника

администрации. При проведении этих работ обработка защищаемой информации (персональных данных) запрещается.

2. Обязанности пользователя

2.1. При первичном допуске к работе в ИСПДн администрации пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных (регламентирующих) документов по вопросам безопасности при автоматизированной обработке информации, изучает настоящую Инструкцию.

2.2. Каждый сотрудник администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн администрации, несет персональную ответственность за свои действия и обязан:

2.2.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн администрации.

2.2.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн администрации.

2.2.3. Хранить в тайне свой пароль.

2.2.4. Выполнять требования по антивирусной защите в части, касающейся действий пользователей.

2.2.5. Немедленно ставить в известность администратора ИСПДн в следующих случаях:

- при подозрении компрометации личного пароля;
- обнаружения фактов совершения в отсутствие пользователя попыток несанкционированного доступа (НСД) к ресурсам ИСПДн администрации;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн администрации;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн администрации, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных средств защиты;
- обнаружения непредусмотренных отводов кабелей и подключенных устройств;
- обнаружения фактов и попыток НСД и случаев нарушения установленного порядка обработки защищаемой информации.

2.3. Пользователю категорически запрещается:

2.3.1. Использовать компоненты программного и аппаратного обеспечения ИСПДн администрации в неслужебных целях.

2.3.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн администрации или устанавливать дополнительно любые программные и аппаратные средства.

2.3.3. Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.

2.3.4. Записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.).

2.3.5. Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД.

2.3.6. Оставлять без личного присмотра на АРМ или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие защищаемую информацию.

2.3.7. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц. Об обнаружении такого рода ошибок ставить в известность администратора ИСПДн.

2.3.8. Производить перемещения технических средств АРМ без согласования с администратором ИСПДн.

2.3.9. Вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств, производить техническое обслуживание (ремонт) средств вычислительной техники без согласования с администратором ИСПДн.

2.3.10. Подключать к АРМ нештатные устройства и самостоятельно вносить изменения в состав и конфигурацию.

2.3.11. Осуществлять ввод пароля в присутствии посторонних лиц.

2.3.12. Оставлять без контроля АРМ в процессе обработки конфиденциальной информации.

2.3.13. Привлекать посторонних лиц для производства ремонта (технического обслуживания) технических средств АРМ.

Приложение № 17
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Инструкция
пользователя по обеспечению безопасности обработки персональных данных при возникновении нештатных ситуаций в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области

1. Назначение и область действия

1.1. Настоящая Инструкция определяет порядок действий в случае возникновения нештатных ситуаций, связанных с функционированием информационной системы персональных данных (далее – ИСПДн) администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – администрация), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Действие настоящей Инструкции распространяется на всех сотрудников администрации, имеющих доступ к ресурсам ИСПДн (далее – Пользователи).

2. Общие положения

2.1. В настоящем Инструкции под нештатной ситуацией понимается происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также с вероятностью потери защищаемой информации.

В кратчайший срок, не превышающий одного рабочего дня, ответственный за организацию обработки персональных данных в администрации и администратор ИСПДн предпринимают меры по восстановлению работоспособности ИСПДн.

2.2. При реагировании на ситуацию, важно, чтобы пользователь правильно классифицировал критичность ситуации. Критичность ситуации оценивается на основе следующей классификации:

1) Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты.

2) Авария. Любое событие, которое приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты (отключение электроэнергии, техническая неисправность

сервера, прорыв системы водоснабжения и т.п.)

3) Катастрофа. Любое событие, приводящее к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв, массовые беспорядки и т.п.), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

2.3. К нештатным ситуациям относятся:

- отключение электричества;
- сбой в локальной вычислительной сети (отсутствие доступа в локальную сеть, отсутствие доступа в интернет, отсутствие связи с сервером и т.п.);
- выход из строя сервера;
- потеря данных (отсутствие возможности сохранить внесенные данные, отсутствие связи с сервером, повреждение файлов и т.п.);
- обнаружение вредоносной программы (вируса);
- обнаружение утечки информации (взлом учетной записи пользователя, обнаружение посторонних устройств в системном блоке, попытка распечатывания или сканирования документов на принтере и т.п.);
- взлом системы (web-сервера и др.) или несанкционированный доступ;
- попытка несанкционированного доступа (обнаружены попытки подбора пароля, доступ постороннего лица в помещение и т.п.);
- компрометация ключей (утеря носителя ключевой информации и т.п.), несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации, визуальный осмотр носителя информации посторонним лицом или подозрение, что данные факты имели место; взлом учетной записи пользователя;
- компрометация пароля (взлом учетной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т.п.)
- физическое повреждение локально-вычислительной сети (далее – ЛВС) или персонального компьютера (далее – ПК) (не включается ПК, при попытке включения отображается синий или черный экран, повреждены провода и т.п.);
- стихийное бедствие;
- иные нештатные ситуации, не включенные в данный список, но влекущие за собой повреждение элементов ИСПДн и возможность потери защищаемой информации, и названные таковыми пользователем ИСПДн или ответственным за ИСПДн.

3. Порядок реагирования на нештатную ситуацию

3.1. В общем случае для предотвращения нештатных ситуаций необходимо чёткое соблюдение требований нормативных документов и

инструкций по эксплуатации оборудования и программного обеспечения.

3.2. Рекомендации в случае возникновения нештатных ситуаций:

- сбой в системе жизнеобеспечение здания (электро-, тепло-, водоснабжение, водоотведение):

при сбоях в системе жизнеобеспечения здания, повлекших нарушения в функционировании элементов ИСПДн, администратор ИСПДн проверяет работоспособность соответствующего оборудования, программного обеспечения и устраняют неисправность. Администратор ИСПДн и пользователь, у которого произошёл сбой в работе ИСПДн, проводят анализ на наличие потерь и (или) разрушения данных и программного обеспечения (далее – ПО). В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

- сбой программного обеспечения:

администратор ИСПДн выясняет причину и последствия сбоя, проводится антивирусная проверка, целостность и работоспособность ПО, проверяется наличие обновлений для ПО, их установка, если они доступны и др. При необходимости производится восстановление ПО и данных из последней резервной копии.

- сбой в ЛВС, выход из строя сервера:

администратор ИСПДн проводит меры по немедленному устранению причин сбоя и восстановлению работоспособности ЛВС, сервера, в том числе с помощью специалистов технической поддержки, устанавливаются причины сбоя в ЛВС и выхода из строя сервера, принимаются меры, направленные на устранение указанных причин и предотвращение их возникновения. В случае необходимости производится восстановление ПО и данных из последней резервной копии.

- потеря, уничтожение, модифицирование, блокирование, копирование данных:

при обнаружении потери данных, администратор ИСПДн проводит мероприятия по поиску и устранению причин потери данных, предотвращению потери, уничтожения, модифицирования, блокирования, копирования данных. При необходимости производится восстановление ПО и данных из последней резервной копии.

- заражение вредоносными программами (вирусами):

при заражении вредоносными программами производится локализация вредоносной программы с целью предотвращения её дальнейшего распространения и анализ состояния компьютера. Анализ проводится администратором ИСПДн. Осуществляется удаление вредоносной программы, устанавливаются причины и источник заражения. После успешной ликвидации вредоносной программы, сохранённые данные также необходимо подвергнуть проверке на наличие вредоносных файлов. Проводится полная антивирусная проверка всех программно-аппаратных компонентов ИС. При необходимости производится восстановление ПО и данных из резервных копий. Возобновление работы с компонентом ИС, подвергшимся заражению, осуществляется только после окончания работ по

удалению вредоносных программ и проведения антивирусной проверки прочих компонентов ИСПДн.

- утечка информации (уязвимость в системе защиты):

при обнаружении утечки информации необходимо сообщить администратору ИСПДн, а также ответственному за организацию обработки персональных данных в администрации. Устанавливаются причины утечки информации. Осуществляется сброс паролей и отзыв сертификатов, все потенциально скомпрометированные учётные записи должны быть немедленно сброшены. Если использовались цифровые сертификаты или ключи доступа, их необходимо отозвать и заменить. Осуществляется обновление и настройка ПО, установка актуальных патчей и обновлений безопасности. Если утечка информации произошла по техническим причинам, проводится анализ защищённости системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

- взлом системы или несанкционированный доступ:

при обнаружении взлома сервера проводится, по возможности, временное отключение сервера от сети для проверки на вредоносные программы, проводится проверка целостности файлов в соответствии с хэш-функциями эталонного программного обеспечения, а также проводится анализ состояния файлов-скриптов и журналы сервера. Необходимо сменить все пароли, которые имели отношение к данному серверу. В случае необходимости производится восстановление ПО и данных из эталонного архива и резервных копий.

- попытка несанкционированного доступа:

при обнаружении попытки несанкционированного доступа необходимо поставить в известность администратора ИСПДн, а также ответственного за организацию обработки персональных данных в администрации. При необходимости блокируется доступ к ИСПДн. Рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует установить такое обновление.

- компрометация ключей:

при компрометации ключей необходимо сообщить о факте компрометации (или предполагаемом факте компрометации) администратору ИСПДн, обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдать их администратору ИСПДн, в течение 3 рабочих дней. Зарегистрировать вновь изготовленные (или резервные) ключи для восстановления конфиденциальной связи.

- компрометация пароля:

при компрометации пароля необходимо сообщить о факте компрометации (или предполагаемом факте компрометации) администратору ИСПДн, незамедлительно сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять меры по минимизации возможного (или нанесенного) ущерба.

- физическое повреждение ЛВС или ПК:

при повреждении ЛВС или ПК необходимо сообщить администратору ИСПДн, который определяет причины повреждения ЛВС или ПК и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод из строя оборудования, проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ, целостность ПО и данных. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий.

В случае ошибки пользователей при эксплуатации технических средств, программных средств и систем защиты информации, повлекших нарушение работоспособности, проводится анализ и идентификация причин инцидента, определяется ущерб, нанесенный нештатной ситуацией, восстанавливается работоспособность системы.

- стихийное бедствие:

при возникновении стихийных бедствий следует руководствоваться документами, регламентирующими действия при чрезвычайных ситуациях. Необходимо выключить персональные компьютеры. Администратор ИСПДн и ответственный за обработку персональных данных в администрации принимают решение о выключении серверов, сетевого оборудования и принимают меры к эвакуации резервных копий с информацией, системных блоков компьютеров, содержащих особо ценную информацию, документов и другого имущества.

3.3. Все сотрудники администрации, имеющие доступ к ресурсам ИСПДн, знакомятся с настоящей Инструкцией под роспись. Новый сотрудник должен быть ознакомлен с настоящей Инструкцией в срок, не превышающий 3-х рабочих дней с момента выхода на работу.

Все сотрудники администрации, имеющие доступ к ресурсам ИСПДн, должны пройти обучение порядку действий при возникновении нештатных ситуаций.

Администратор ИСПДн и ответственный за организацию обработки персональных данных должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания сотрудников, имеющих доступ к ресурсам ИСПДн, по реагированию на нештатные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение порядку действий при возникновении нештатных ситуации.

Приложение № 18
к постановлению администрации
Заневского городского поселения
Всеволожского муниципального
района Ленинградской области
от 20.04.2026 № 386

Положение
о разрешительной системе допуска пользователей и обслуживающего персонала к информационным ресурсам и системе защиты персональных данных в администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области

Настоящее Положение о разрешительной системе допуска определяет порядок и правила доступа работников администрации Заневского городского поселения Всеволожского муниципального района Ленинградской области (далее – администрация) к информационным ресурсам информационной системы персональных данных (ИСПДн) администрации.

К работе в ИСПДн допускаются работники, ознакомившиеся с настоящим Положением, Положением об организации и обеспечении защиты персональных данных, Правилами о порядке обработки персональных данных, Перечнем персональных данных, обрабатываемых в администрации.

Учетная запись нового сотрудника (пользователя) с соответствующими правами доступа создается администратором ИСПДн по представлению начальника структурного подразделения данного работника, согласованного с курирующим данное структурное подразделение заместителем главы администрации или главой администрации.

После получения заявки администратор ИСПДн производит необходимые действия по созданию (изменению, удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к информационным ресурсам ИСПДн администрации, включению его в соответствующие группы пользователей и другие необходимые действия.

Уникальное имя (учетная запись пользователя), под которым он регистрируется и осуществляет работу в системе, присваивается каждому пользователю ИСПДн администрации для обеспечения персональной ответственности за свои действия.

При изменении должностных обязанностей сотрудника, связанных с переводом в другое структурное подразделение, переводом на другую должность и т.п., учетная запись пользователя на основании заявки начальника соответствующего структурного подразделения подлежит изменению (корректировке), при этом старые полномочия аннулируются.

При увольнении сотрудника, имеющего доступ к информационным ресурсам ИСПДн администрации и/или лишения его прав доступа к ИСПДн администрации начальник структурного подразделения, в котором работает

увольняемый сотрудник, подает заявку курирующему данное структурное подразделение заместителю главы администрации или главе администрации.

Все изменения в правах доступа, связанные с увольнением пользователя ИСПДн территориального органа Росреестра, выполняются администраторами не позднее трех суток с момента получения заявки на внесение изменений.

Сотрудники, допущенные к работе с персональными данными, несут ответственность в соответствии с требованиями законодательства Российской Федерации, нормативных правовых актов администрации.

Контроль доступа сотрудников (пользователей) структурных подразделений администрации к информационным ресурсам ИСПДн и обеспечение информационной безопасности при работе с информационными ресурсами ИСПДн возлагается на администратора ИСПДн.

Настоящее Положение о разрешительной системы допуска пользователей к ИСПДн распространяется на все информационные системы администрации.

Ознакомлены:

№ пп	Фамилия, имя и отчество	Наименование подразделения	Должность	Дата	Подпись
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					
21.					
22.					
23.					
24.					
25.					
26.					
27.					
28.					
29.					
30.					
31.					
32.					
33.					
34.					
35.					
36.					
37.					
38.					
39.					
40.					
41.					
42.					
43.					
44.					