



**МИНИСТЕРСТВО  
СТРОИТЕЛЬСТВА И ЖИЛИЩНО-КОММУНАЛЬНОГО  
ХОЗЯЙСТВА ПСКОВСКОЙ ОБЛАСТИ**

**ПРИКАЗ**

от 09.02.2026 № 17-02  
г. Псков

Об утверждении правил и порядка  
организации работ по защите  
персональных данных

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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», Положением о Министерстве строительства и жилищно-коммунального хозяйства Псковской области, утвержденным постановлением Правительства Псковской области от 24 июня 2025 г. № 233, ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые:

1) Положение о защите и обработке персональных данных в информационных системах Министерства строительства и жилищно-коммунального хозяйства Псковской области, согласно приложению 1.

2) Правила обработки персональных данных в Министерстве строительства и жилищно-коммунального хозяйства Псковской области, согласно приложению 2.

3) Правила рассмотрения запросов субъектов персональных данных или их представителей в Министерстве строительства и жилищно-коммунального хозяйства Псковской области, согласно приложению 3.

4) Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в Министерстве строительства и жилищно-коммунального хозяйства Псковской области, согласно приложению 4.

5) Правила работы с обезличенными персональными данными в Министерстве строительства и жилищно-коммунального хозяйства Псковской области, согласно приложению 5.

6) Перечень информационных систем, используемых в деятельности Министерства строительства и жилищно-коммунального хозяйства Псковской области, согласно приложению 6.

7) Перечень должностей Министерства строительства и жилищно-коммунального хозяйства Псковской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, согласно приложению 7.

8) Типовое обязательство служащего, непосредственно осуществляющего организацию обработки персональных данных в Министерстве строительства и жилищно-коммунального хозяйства Псковской области, ставших известными ему в связи с исполнением должностных обязанностей, согласно приложению 8.

9) Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в связи с поступлением на государственную гражданскую службу в Министерстве строительства и жилищно-коммунального хозяйства Псковской области, согласно приложению 9.

10) Порядок доступа государственных гражданских служащих Министерства строительства и жилищно-коммунального хозяйства Псковской области в помещения, в которых ведется обработка персональных данных, согласно приложению 10.

2. Признать утратившим силу приказ Комитета по строительству и жилищно-коммунальному хозяйству Псковской области от 08.05.2019 № 77-ОД.

3. Настоящий приказ вступает в силу со дня, следующего за днем его официального опубликования.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Врио министра



К.Э.Григорьева

Приложение 1  
к приказу Министерства  
строительства и жилищно-  
коммунального хозяйства  
Псковской области  
от 09.02.2026 № 17-09

ПОЛОЖЕНИЕ  
о защите и обработке персональных данных  
в информационных системах Министерства строительства  
и жилищно-коммунального хозяйства  
Псковской области

I. Общие положения

1.1. Положение о защите и обработке персональных данных в информационных системах Министерства строительства и жилищно-коммунального хозяйства Псковской области (далее также – Положение, Министерство) устанавливает требования к обеспечению безопасности персональных данных и определяет:

- порядок обработки персональных данных;
- мероприятия по обеспечению защиты прав и свобод граждан при обработке их персональных данных;
- ответственность должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Положение разработано в соответствии с:

- Конституцией Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

1.3. Целью Положения является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания или по истечении 75 лет срока их хранения, или продлевается на основании заключения комиссии по защите персональных данных Министерства, если иное не определено законом.

1.5 Персональные данные субъектов персональных данных обрабатываются в целях:

- обеспечения кадровой работы, в том числе соблюдения ограничений, запретов и обязанностей, установленных в целях противодействия коррупции;
- оформления допуска к государственной тайне;
- профилактики коррупционных и иных правонарушений;
- обеспечения личной безопасности и сохранности имущества;
- пенсионного, медицинского обеспечения и оформления соответствующих документов;
- осуществление обязательного государственного страхования;
- оформления документов при направлении в служебную командировку;
- подачи сведений в Фонд пенсионного и социального страхования Российской Федерации, Федеральную налоговую службу, Федеральный фонд обязательного медицинского страхования, Министерство

строительства и жилищно-коммунального хозяйства Российской Федерации, Правительство Псковской области, иные государственные органы;

- обработки запросов судебных органов, государственных органов по различным вопросам;

- предоставления государственных услуг;

- рассмотрения обращений граждан, поступающих в Министерство.

1.6. В целях, определенных в пункте 1.5 настоящего Положения, обрабатываются следующие категории персональных данных:

- 1) фамилия, имя, отчество;
- 2) предыдущие фамилии, имена, и (или) отчества, дата, место и причина изменения (в случае изменения);
- 3) число, месяц, год рождения;
- 4) место рождения;
- 5) пол;
- 6) сведения о гражданстве (в том числе предыдущие гражданства, иные гражданства);
- 7) вид, серия, номер документа, удостоверяющего личность, дата выдачи, наименование органа, выдавшего его);
- 8) адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;
- 9) номер контактного телефона или сведения о других способах связи;
- 10) номер страхового свидетельства обязательного пенсионного страхования;
- 11) идентификационный номер налогоплательщика;
- 12) страховой медицинский полис обязательного медицинского страхования;
- 13) свидетельство о государственной регистрации актов гражданского состояния;
- 14) свидетельство о рождении несовершеннолетних детей;
- 15) сведения о составе семьи, близких родственниках (отец, мать, братья, сестры и дети), а также супруге (супруги), в том числе бывших,

постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство (степень родства, фамилия, имя, отчество, дата рождения, место рождения, место работы, домашний адрес, с какого времени проживают за границей);

16) отношение к воинской обязанности, сведения о воинском учете (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);

17) сведения об образовании (когда и какие образовательные организации закончил (а), номера дипломов, направление подготовки или специальность по диплому, квалификация);

18) сведения о послевузовском профессиональном образовании (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);

19) сведения о профессиональной переподготовке и (или) повышении квалификации (вид документа, когда, кем выдан, направление, специальность подготовки);

20) заключение медицинского учреждения о наличии (отсутствии) заболевания, препятствующего поступлению на государственную службу или ее прохождению;

21) фотография;

22) сведения о прохождении государственной службы, классный чин государственной службы, муниципальной службы;

23) сведения о трудовой деятельности;

24) сведения, содержащиеся в служебном контракте, дополнительных соглашениях к служебному контракту, выписках их служебных контрактов и (или) в трудовом договоре, дополнительных соглашениях к трудовому договору;

25) сведения о пребывании за границей (когда, где, с какой целью);

26) сведения о наличии (отсутствии) судимости, привлечение к административной ответственности;

27) сведения об оформленных допусках к государственной тайне

(кем оформлен, форма, номер, дата);

28) сведения о государственных наградах, иных наградах и знаках отличия (кем награжден (а) и когда);

29) сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера супруга (супруги) и несовершеннолетних детей;

30) свидетельства о рождении несовершеннолетних детей;

31) номер расчетного счета

32) номер банковской карты

33) иные профессиональные данные, предусмотренные законодательством Российской Федерации.

1.7. Обработка персональных данных в Министерстве выполняется с использованием средств автоматизации или без использования таких средств и включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

## II. Основные понятия и состав персональных данных

2.1. Основные понятия, используемые Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:

- персональные данные, обработка персональных данных, распространение персональных данных, блокирование персональных данных, уничтожение персональных данных, обезличивание персональных данных, информационная система персональных данных, трансграничная передача персональных данных.

2.2. Основные понятия, используемые в настоящем Положении:

- оператор - государственный орган – Министерство строительства и жилищно-коммунального хозяйства Псковской области, организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели и содержание обработки персональных данных;

- использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

- конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

- общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.3. Персональные данные, обрабатываемые в информационных системах Министерства, содержатся в документах:

- отдела развития городской среды;
- отдела коммунальной инфраструктуры;
- отдела строительства;
- отдела модернизации жилищного фонда;
- финансово-экономического отдела;
- отдела по обращению с твердыми коммунальными отходами;
- отдела организационной и кадровой работы;
- правового отдела;
- режимно-секретного подразделения.

2.3.1. В отделе развития городской среды создаются и хранятся следующие группы документов, содержащие персональные данные отдельных категорий граждан:

- при рассмотрении обращений граждан.

2.3.2. В отделе коммунальной инфраструктуры создаются и хранятся следующие группы документов, содержащие персональные

данные отдельных категорий граждан:

- при рассмотрении обращений граждан;
- при работе в Государственной информационной системе жилищно-коммунального хозяйства (ГИС ЖКХ).

2.3.3. В отделе строительства создаются и хранятся следующие группы документов, содержащие персональные данные отдельных категорий граждан:

- при рассмотрении обращений граждан;
- при работе в Государственной информационной системе обеспечения градостроительной деятельности Псковской области (ГИСОГД);
- при рассмотрении заявлений граждан, желающих получить государственные услуги.

2.3.4. В отделе модернизации жилищного фонда создаются и хранятся следующие группы документов, содержащие персональные данные отдельных категорий граждан:

- при рассмотрении обращений граждан.

2.3.5. В финансово-экономическом отделе создаются и хранятся следующие документы, содержащие данные о работниках в единичном или сводном виде:

- карточка-справка;
- копия паспорта;
- копия страхового пенсионного свидетельства;
- копия ИНН;
- копия личного счета для зачисления заработной платы;
- копии свидетельств о рождении детей работников;
- копии приказов с расчетами;
- отчеты в органы статистики;
- отчеты в налоговые органы и другие организации.

2.3.6. В отделе по обращению с твердыми коммунальными отходами создаются и хранятся следующие группы документов, содержащие персональные данные отдельных категорий граждан:

- при рассмотрении обращений граждан.

2.3.7. В отделе организационной и кадровой работы создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

- документы, содержащие персональные данные работников Министерства (комплекты документов, сопровождающие процесс оформления государственно-служебных и трудовых отношений при приеме на работу (назначение на должность государственной гражданской службы области), переводе, увольнении;
- комплект материалов по анкетированию, тестированию, проведению собеседований с кандидатами на должность;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки работников;
- дела, содержащие основания к приказу по личному составу;
- дела, содержащие материалы аттестации работников, служебных проверок;
- копии отчетов, направляемых в государственные органы статистики, налоговые и другие органы;
- документы по планированию, учету, анализу и отчетности в части работы с персоналом Министерства.

2.3.9. В правовом отделе создаются и хранятся следующие группы документов, содержащие персональные данные отдельных категорий граждан:

- при рассмотрении обращений граждан;
- при судебной работе.

2.3.10. В режимно-секретном подразделении создаются и хранятся группы документов, содержащие персональные данные отдельных категорий граждан, оформляемых для допуска к государственной тайне.

### III. Порядок получения и обработки персональных данных

3.1. Порядок получения персональных данных о государственных гражданских служащих Министерства.

3.1.1. Все персональные данные государственного гражданского

служащего Министерства следует получать у него самого. Если персональные данные государственного гражданского служащего возможно получить только у третьей стороны, то государственный гражданский служащий должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо Министерства должно сообщить государственному гражданскому служащему Министерства о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа государственного гражданского служащего дать письменное согласие на их получение.

3.1.2. Должностные лица Министерства не имеют права получать и обрабатывать персональные данные государственного гражданского служащего Министерства о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации должностные лица Министерства вправе получать и обрабатывать данные о частной жизни государственного гражданского служащего только с его письменного согласия.

3.1.3. Письменное согласие государственного гражданского служащего на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором

способов обработки персональных данных;

- срок, в течение которого действует согласие, а также порядок его отзыва.

Форма заявления о согласии работника на обработку персональных данных в соответствии с приложением 1 к настоящему Положению.

3.1.4. Согласие государственного гражданского служащего не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

2) обработка персональных данных осуществляется в целях исполнения служебного контракта;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов государственного гражданского служащего, если получение его согласия невозможно.

3.2. Порядок обработки, передачи и хранения персональных данных государственных гражданских служащих Министерства.

3.2.1. Государственный гражданский служащий Министерства предоставляет в отдел организационной и кадровой работы достоверные сведения о себе. Отдел организационной и кадровой работы проверяет достоверность сведений, сверяя данные, предоставленные государственным гражданским служащим, с имеющимися в отделе организационной и кадровой работы документами.

3.2.2. В соответствии со статьей 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина министр строительства и жилищно-коммунального хозяйства Псковской области и его представители при обработке персональных данных государственного гражданского служащего должны соблюдать следующие общие требования:

3.2.2.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия государственным гражданским служащим в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности государственных гражданских служащих, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2.2. При определении объема и содержания, обрабатываемых персональных данных должностные лица Министерства должны руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

3.2.2.3. При принятии решений, затрагивающих интересы государственного гражданского служащего, должностные лица Министерства не имеют права основываться на персональных данных государственного гражданского служащего, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.2.2.4. Защита персональных данных государственного гражданского служащего от неправомерного их использования или утраты обеспечивается должностными лицами Министерства за счет средств Министерства в порядке, установленном нормативными правовыми актами.

3.2.2.5. Государственные гражданские служащие и их представители должны быть ознакомлены под расписку с документами Министерства, устанавливающими порядок обработки персональных данных государственных гражданских служащих, а также об их правах и обязанностях в этой области.

3.2.2.6. Во всех случаях отказ государственного гражданского служащего от своих прав на сохранение и защиту тайны недействителен.

3.3. Порядок получения и обработки персональных данных граждан, получающих государственные услуги в Министерстве:

3.3.1. Гражданин, желающий получить государственную услугу, обратившийся в отдел строительства Министерства предоставляет

документы для регистрации его персональных данных.

3.3.2. Обработка персональных данных граждан, получающих государственные услуги в Министерстве, производится в соответствии с разделом 3.2. настоящего Положения.

#### IV. Обеспечение защиты персональных данных

4.1. Безопасность персональных данных достигается путём исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

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

4.3. Для обеспечения безопасности персональных данных осуществляется защита информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

4.4. При обработке персональных данных должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного

доступа к персональным данным;

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

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

- постоянный контроль за обеспечением уровня защищённости персональных данных.

4.5. Мероприятия по обеспечению безопасности персональных данных включают в себя:

4.5.1. определение информационных систем, содержащих персональные данные;

4.5.2. определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

4.5.3. разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

4.5.4. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

4.5.5. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

4.5.6. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

4.5.7. учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

4.5.8. учёт лиц, допущенных к работе с персональными данными в информационной системе;

4.5.9. контроль за соблюдением условий использования средств

защиты информации, предусмотренных эксплуатационной и технической документацией;

4.5.10. составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищённости персональных данных, разработку и принятие мер по предотвращению возможных опасных нарушений.

## V. Передача персональных данных

5.1. Передача персональных данных государственных гражданских служащих Министерства.

5.1.1. Работодатель не вправе предоставлять персональные данные государственного гражданского служащего третьей стороне без письменного согласия последнего, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью государственного гражданского служащего, а также в случаях, установленных федеральным законодательством.

5.1.2. В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных государственного гражданского служащего или отсутствует письменное согласие государственного гражданского служащего на предоставление его персональных сведений, работодатель обязан отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

5.1.3. Персональные данные государственного гражданского служащего могут быть переданы представителем государственного гражданского служащего в том объёме, в каком это необходимо для выполнения указанными представителями их функций.

5.1.4. Финансово-экономический отдел Министерства обрабатывает

и предоставляет персональные данные по установленному регламенту в отделение Пенсионного Фонда Российской Федерации по Псковской области и Управление Федеральной налоговой службы Российской Федерации по Псковской области с помощью программы «Сбис Электронная отчетность» без передачи по открытым каналам связи.

5.2. При передаче персональных данных государственного гражданского служащего внутри структурного подразделения или в другое структурное подразделение Министерства, информация ограничивается только теми персональными данными государственного гражданского служащего, которые необходимы для выполнения должностными лицами их функций.

5.3. Передача персональных данных граждан, получающих государственные услуги в Министерстве не производится.

5.3.1. Гражданин, являющийся субъектом персональных данных, имеет право предоставить запрос в Министерство и получить информацию, касающуюся обработки его персональных данных.

5.4. Порядок приостановки предоставления персональных данных в случае обнаружения нарушений порядка их предоставления.

5.6.1. При обнаружении нарушений порядка предоставления персональных данных сотрудник Министерства должен немедленно приостановить предоставление персональных данных.

5.6.2. Министр строительства и жилищно-коммунального хозяйства Псковской области назначает служебную проверку для выявления причин нарушения.

5.6.3. После устранения нарушений предоставление персональных данных возобновляется.

## VI. Хранение персональных данных

6.1. Персональные данные государственных гражданских служащих Министерства обрабатываются и хранятся в отделе организационной и кадровой работы и в финансово-экономическом отделе как на бумажных носителях, так и в электронном виде в локальных

информационных системах.

6.2. Персональные данные граждан, получающих государственные услуги в Министерстве, хранятся в отделе строительства как на бумажных носителях, так и в электронном виде в локальных информационных системах.

6.3. Персональные данные граждан, поступивших в ГИСЖКХ, ГИСОГД, СЭД ПШО, через Платформу обратной связи Псковской области, в интернет приемную Правительства Псковской области хранятся в локальных информационных системах на персональных компьютерах ответственных исполнителей.

## VII. Доступ к персональным данным

7.1. Доступ государственных гражданских служащих Министерства к персональным данным ограничен. В Министерстве введена разрешительная система доступа к персональным данным, согласно которой разрешается доступ только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной служебной функции.

7.2. Право доступа к персональным данным государственных гражданских служащих Министерства имеют:

- министр и его заместители;
- сотрудники отдела организационной и кадровой работы;
- сотрудники финансово-экономического отдела;
- руководители структурных подразделений по направлению деятельности (доступ к персональным данным только государственных гражданских служащих своего подразделения);
- государственные гражданские служащие отдела организационной и кадровой работы, работающие с архивными документами;
- администратор безопасности информационных систем персональных данных.

## VIII. Порядок действий должностных лиц в случае обнаружения нарушений, угрожающих конфиденциальности обрабатываемых персональных данных

8.1. В случае обнаружения фактов несоблюдения условий хранения носителей персональных данных, неисправности средств защиты информации, нарушения порядка предоставления персональных данных или иных нарушений, угрожающих конфиденциальности обрабатываемых персональных данных (далее – инцидент информационной безопасности), обнаружившие инцидент государственные гражданские служащие Министерства обязаны немедленно информировать о нем ответственного за организацию обработки персональных данных.

8.2. Предположение о том, что произошел инцидент информационной безопасности, может основываться на следующих признаках:

8.2.1. уведомление антивирусного средства о нарушении информационной безопасности;

8.2.2. сообщение пользователей об отклонениях в работе системных или прикладных программ;

8.2.3. сообщение пользователей о снижении производительности их рабочих станций;

8.2.4. наличие файлов с нечитаемыми названиями;

8.2.5. множественные неудачные попытки авторизации.

8.3. Ответственным за организацию обработки персональных данных проводится оценка риска и последствий инцидента, вследствие чего вырабатывается стратегия реагирования на инцидент.

8.4. В случае возможности нарушения конфиденциальности обрабатываемых персональных данных, дальнейшая работа информационных систем прекращается.

8.5. В случае возникновения нарушений на рабочей станции или сервере необходимо произвести полное дублирование информации и проводить работы по расследованию нарушения на отдельном

компьютере.

8.6. Электронные журналы должны быть тщательно изучены и проанализированы.

8.7. События инцидента подлежат документированию. Документирование необходимо для сбора и последующего обобщения свидетельств расследования. Документированию подлежат все факты и доказательства злонамеренного воздействия.

8.8. Рекомендуется ведение журнала расследования инцидента, форма которого предлагается ответственным за осуществление мероприятий по защите персональных данных. Ключевыми позициями данного журнала являются:

- текущий статус расследования;
- описание инцидента;
- действия, производимые в процессе обработки инцидента;
- перечень свидетельств, собранных в ходе обработки инцидента, с обязательным указанием источников.

8.9. В ходе расследования инцидента все свидетельства должны быть защищены от дискредитации, поскольку данные могут содержать информацию о действенных уязвимостях информационной системы.

8.10. Ответственным за организацию обработки персональных данных составляется заключение по факту инцидента информационной безопасности, включающее в себя:

- исходное протоколирование инцидента;
- причины и следствия возникновения инцидента;
- меры, предпринятые для ликвидации инцидента и его последствий;
- предложения по внесению изменений в систему обеспечения безопасности информации.

8.11. Ответственным за организацию обработки персональных данных должен быть классифицирован и описан каждый инцидент, произошедший в Министерстве, а также классифицированы и описаны возможные инциденты, предположения о которых были сделаны на основе анализа рисков.

## IX. Обязанности должностных лиц по обеспечению безопасности персональных данных

9.1. Ответственный за организацию обработки персональных данных в Министерстве назначается приказом Министерства.

9.2. Безопасность персональных данных при их обработке обеспечивают должностные лица Министерства, эксплуатирующие информационные системы.

9.3. Должностные лица Министерства допускаются к соответствующим персональным данным на основании разрешительной системы доступа Министерства. Изменения и дополнения в разрешительную систему доступа вносятся на основании приказа Министерства.

9.4. Государственные гражданские служащие Министерства, допущенные к обработке персональных данных обязаны:

9.4.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами информационных систем;

9.4.2. Хранить в тайне свой пароль (пароли). В соответствии с разделом XI «Правила парольной защиты» настоящего Положения с установленной периодичностью менять свой пароль (пароли);

9.4.3. Выполнять требования части XII «Правила антивирусной защиты» настоящего Положения в части касающейся действий пользователей рабочих станций информационной системы;

9.4.4. Немедленно вызывать ответственного за организацию обработки персональных данных в Министерстве и ставить в известность непосредственного руководителя при обнаружении следующих нарушений:

нарушений целостности пломб (наклеек, печатей) на аппаратных средствах рабочих станций или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищённой рабочей станции;

несанкционированных изменений в конфигурации программных или аппаратных средств рабочей станции;

нарушений в работе средств защиты информации;

отклонений в работе системных или прикладных программных программ, затрудняющих эксплуатацию рабочей станции, выхода их из строя или неустойчивого функционирования узлов рабочей станции или периферийных устройств (дисководов, принтера и т.п.), а также перебоях в системе электроснабжения;

некорректного функционирования установленных на рабочей станции технических средств защиты;

непредусмотренных формуляром рабочей станции отводов кабелей и подключенных устройств.

## X. Правила учета средств защиты информации и носителей персональных данных

10.1. Средства защиты информации, используемые в информационной системе персональных данных, подлежат учёту в журнале учёта средств защиты информации, в котором отражается:

- наименование средств защиты;
- серийный (заводской) номер;
- номер и срок действия сертификата на средство защиты;
- наименование организаций, установивших средства защиты;
- место установки средств защиты информации.

10.2. Журнал ведется в электронном виде.

10.3. Все съемные магнитные, оптические и другие машинные носители персональных данных, используемые в информационной системе персональных данных, подлежат обязательному учету. На съемные носители информации наносится маркировка, позволяющая идентифицировать и организовать их учёт. Съемные носители информации, в том числе с резервными копиями персональных данных, регистрируются в журнале учета машинных носителей персональных данных, в котором отражается:

- тип и ёмкость носителя;
- учётный номер носителя;

- место установки (использования) носителя;
- дата установки носителя;
- ответственное должностное лицо;
- сведения о списании носителя и уничтожении информации.

10.4. Ответственным за организацию обработки персональных данных должна организовываться периодическая проверка наличия, сохранности и соблюдения правил обращения со съемными носителями персональных данных, журнала учёта съемных носителей персональных данных, журнала учёта средств защиты информации, не реже 1 раза в полгода.

10.6. Результаты контроля заносятся в журнал учета мероприятий по контролю за соблюдением режима защиты персональных данных с указанием мероприятия, даты проведения проверки, ответственного исполнителя и результатов контроля.

10.7. Журнал ведется в электронном виде.

## XI. Правила парольной защиты

11.1 Контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на ответственного за организацию обработки персональных данных.

11.2. Пароли должны генерироваться и распределяться централизованно или выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

11.2.1. Длина пароля должна быть не менее 6 - 8 символов в зависимости от класса системы.

11.2.2. В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (например - \$, @, #, %, & и другие символы).

11.2.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и другие сочетания).

11.2.4. При смене пароля новое значение должно отличаться

от предыдущего не менее чем в 6 позициях.

11.2.5. Личный пароль пользователь не имеет права сообщать никому.

11.3. Государственные гражданские служащие Министерства, имеющие доступ к персональным данным, должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

11.4. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора информационной безопасности.

11.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 2 месяца.

11.6. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы, в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и другие изменения), должна проводиться ответственным за организацию обработки персональных данных немедленно после окончания последнего сеанса работы данного пользователя с системой.

11.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие изменения) государственных гражданских служащих, которым были предоставлены полномочия по управлению парольной защитой.

11.8. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры по внеплановой смене паролей.

11.9. Хранение государственным гражданским служащим значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, или в сейфах ответственного за информационную безопасность или руководителя структурного подразделения.

11.10. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за эксплуатацию информационной системы персональных данных, периодический контроль возлагается на ответственного за осуществление мероприятий по защите персональных данных.

## XII. Правила антивирусной защиты

12.1. В Министерстве допускаются к использованию только лицензионные антивирусные средства.

12.2. Установка и настройка параметров средств антивирусного контроля на рабочих местах государственных гражданских служащих Министерства осуществляется сотрудниками государственного бюджетного учреждения Псковской области «Центр информационных систем» (далее – ГБУ ПО «ЦИС»).

12.3. Ежедневно после включения компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютера.

12.4. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, текстовые файлы любых форматов), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после её приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

12.5. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

12.6. Устанавливаемое (изменяемое) программное обеспечение

должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка.

12.7. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) государственный гражданский служащий Министерства самостоятельно или вместе с ответственным за организацию обработки персональных данных должен организовать проведение внеочередного антивирусного контроля компьютера. При необходимости привлечь специалистов ГБУ ПО «ЦИС» для определения ими факта наличия или отсутствия компьютерного вируса.

12.8. В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов государственные гражданские служащих обязаны:

12.8.1. Приостановить работу.

12.8.2. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за организацию обработки персональных данных, владельца заражённых файлов, смежные подразделения, использующие эти файлы в работе.

12.8.3. Организовать лечение или уничтожение зараженных файлов.

12.9. Ежедневно в автоматическом режиме должно проводиться обновление антивирусных баз.

12.10. Государственным гражданским служащим ответственным за обеспечение информационной безопасности должны проводиться периодические проверки обновлений компонентов антивирусного средства не реже одного раза в месяц.

### ХIII. Правила обновления общесистемного и прикладного программного обеспечения

13.1. Под обновлением понимается замена программного обеспечения (далее – ПО) устаревшей версии на новую версию

этого же ПО. Обновление ПО допустимо лишь в той мере и в том случае, если это подтверждено производственной необходимостью и имеет непосредственное отношение к технологическому процессу обработки информации.

13.2. В процессе обновления ПО допускается ввод информации с CD и внешних магнитных носителей.

13.3. Установка и обновление ПО производится только с лицензионных дистрибутивных носителей.

13.4. Обновления должны подвергаться антивирусному контролю в соответствии с разделом XII «Правила антивирусной защиты» настоящего Положения.

13.5. Установка нового автоматизированного рабочего места для пользователя информационной системы производится после выполнения требований к системе защиты персональных данных и настоящего Положения. По окончании работ производится оценка соответствия информационной системы требованиям безопасности персональных данных и вносятся необходимые изменения и дополнения в техническую документацию.

13.6. Все вышеперечисленные работы выполняются сотрудниками ГБУ ПО «ЦИС» по соответствующей заявке от Министерства.

#### XIV. Порядок контроля за соблюдением условий использования средств защиты информации

14.1 Целями контроля за соблюдением условий использования средств защиты информации являются:

14.1.1. Установление степени соответствия принятых мер требованиям законодательных и иных нормативных правовых актов, стандартов, норм, правил и инструкций по защите информации.

14.1.2. Выявление технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на информацию, содержащую сведения о персональных данных и выработка рекомендаций по закрытию этих каналов.

14.2. Контроль за соблюдением условий использования средств защиты информации (далее – Контроль) осуществляется ответственным за организацию обработки персональных данных посредством проведения проверок (изучений, ознакомлений).

14.3 При Контроле необходимо проверять срок действия сертификатов используемых средств защиты информации.

14.4. Контроль должен проводиться регулярно. Результаты Контроля докладываются министру строительства и жилищно-коммунального хозяйства Псковской области.

14.5. При обнаружении нарушений в ходе Контроля должностные лица Министерства обязаны руководствоваться положениями части VIII настоящего Положения.

14.6. Ежегодная комплексная проверка состояния безопасности персональных данных при их обработке в информационных системах Министерства проводится комиссией по защите персональных данных. По окончании проверки составляется справка, в которой отражаются результаты проверки, выводы и рекомендации по совершенствованию системы технической защиты информации. Содержание справки доводится до министра строительства и жилищно-коммунального хозяйства Псковской области.

#### XV. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

15.1. Государственные гражданские служащие Министерства, виновные в нарушении норм настоящего Положения, а также законодательства Российской Федерации, регулирующего получение, обработку и защиту персональных данных должностного лица, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

---

Приложение 1  
к Положению о защите и обработке  
персональных данных  
в информационных системах  
Министерства строительства  
и жилищно-коммунального хозяйства  
Псковской области

Министру строительства  
и жилищно-коммунального хозяйства  
Псковской области

от \_\_\_\_\_  
(фамилия, имя, отчество)  
проживающего (ей) по адресу \_\_\_\_\_  
\_\_\_\_\_  
документ, удостоверяющий личность  
\_\_\_\_\_ серия \_\_\_\_\_ № \_\_\_\_\_  
выдан \_\_\_\_\_  
\_\_\_\_\_ г.

### ЗАЯВЛЕНИЕ

о согласии на обработку персональных данных

В соответствии со статьей 9 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» я, \_\_\_\_\_,

(фамилия, имя, отчество)

даю согласие Министерству строительства и жилищно-коммунального хозяйства Псковской области на обработку и использование следующих персональных данных с целью оформления государственно-служебных отношений, выполнения трудовых функций:

1. Дата рождения \_\_\_\_\_

(число, месяц, год)

2. Пол \_\_\_\_\_

(женский, мужской - указать нужное)

3. Документ, удостоверяющий личность

\_\_\_\_\_  
\_\_\_\_\_  
(наименование, номер и серия документа, кем и когда выдан)

4. Адрес регистрации по месту  
жительства \_\_\_\_\_

\_\_\_\_\_ (почтовый адрес)

5. Адрес фактического проживания

\_\_\_\_\_ (почтовый адрес фактического проживания, контактный телефон)

6. Наименование страховой медицинской организации, серия и номер полиса  
страхового медицинского обязательного страхования граждан

7. Индивидуальный номер налогоплательщика (ИНН)

8. Номер страхового свидетельства государственного пенсионного  
страхования \_\_\_\_\_

9. Сведения о себе и членах своей семьи, а также сведения о полученных доходах собою и принадлежащем себе на праве собственности имуществе, являющихся объектами налогообложения, об обязательствах имущественного характера (в соответствии с пунктом 9 статьи 15 Федерального закона от 27.07.2004 №79-ФЗ «О государственной гражданской службе Российской Федерации»).

Срок действия заявления: с даты подписания заявления до истечения срока хранения документов в архиве.

« \_\_\_\_ » \_\_\_\_\_ г. Подпись \_\_\_\_\_ / \_\_\_\_\_ /  
(расшифровка подписи)

Данные, указанные в заявлении, соответствуют представленным документам.

Принял

\_\_\_\_\_ / \_\_\_\_\_ /  
(дата приема заявления) (подпись специалиста) (расшифровка подписи)

Приложение 2  
к приказу Министерства  
строительства и жилищно-  
коммунального хозяйства  
Псковской области  
от 09.02.2026 № 17-09

ПРАВИЛА  
обработки персональных данных  
в Министерстве строительства и жилищно-  
коммунального хозяйства Псковской области

I. Общие положения

1.1. Настоящие Правила обработки персональных данных (далее – Правила) в Министерстве строительства и жилищно-коммунального хозяйства Псковской области (далее – Министерство) разработаны на основании требований Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон), постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления 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 и муниципальными органами» и устанавливают порядок обработки, распространения и использования персональных данных в Министерстве, процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а так же определяющие для каждой цели обработки 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 должна осуществляться на законной и справедливой основе.

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

1.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

1.5. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

1.6. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

1.7. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

## II. Процедуры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством.

2.1. К процедурам, направленным на предотвращение и выявление нарушений законодательства в отношении обработки персональных данных и устранение таких последствий относятся:

2.1.1. осуществление внутреннего контроля соответствия обработки

персональных данных требованиям к защите персональных данных, установленным Федеральным законом и принятым в соответствии с ним нормативным правовым актам;

2.1.2. оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

2.1.3. ознакомление государственных гражданских служащих, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2.2. Обеспечение безопасности персональных данных достигается, в частности:

2.2.1. определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

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

2.2.3. применением прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

2.2.4. оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

2.2.5. учетом машинных носителей персональных данных;

2.2.6. обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

2.2.7. восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

2.2.8. установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных.

### III. Цели обработки персональных данных

3.1. Целями обработки персональных данных являются:

3.1.1. обеспечение соблюдения законов и иных нормативных правовых актов в связи с оказанием государственных услуг;

3.1.2. соблюдение порядка и правил приема на государственную гражданскую службу, установленных Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», Законом Псковской области от 05.12.2005 № 491-ОЗ «О государственной гражданской службе Псковской области» и иными нормативными правовыми актами;

3.1.3. заполнение и использование информационных баз бухгалтерского учета в целях повышения эффективности, быстрого поиска, формирования отчетов.

Субъектами, персональные данные которых обрабатываются, для указанных в п. 3.1. целей, являются:

- лица, замещающие должности государственной гражданской службы Псковской области в Министерстве;

- лица, претендующие на замещение должностей государственной гражданской службы Псковской области в Министерстве;

- лица, состоящие в кадровом резерве Министерства;

- лица, участвовавшие в конкурсе на замещение вакантной должности государственной гражданской службы Псковской области в Министерстве;

- лица, ранее состоявшие на государственной гражданской службе (в трудовых отношениях) в Министерстве, личные дела которых не переданы на хранение в ГКУ Псковской области «Государственный

архив Псковской области»;

- лица, обратившиеся за предоставлением государственных услуг.

#### IV. Порядок обработки персональных данных субъектов персональных данных, осуществляемой с использованием средств автоматизации, содержание персональных данных

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

4.2. Уполномоченными должностными лицами при обработке персональных данных в информационных системах персональных данных должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации.

4.3. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

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

4.5. Должностному лицу, ответственному за обеспечение безопасности персональных данных при их обработке в информационных системах, должно быть обеспечено:

4.5.1. своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до министра строительства и жилищно-коммунального

хозяйства Псковской области;

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

4.5.3. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

4.5.4. постоянный контроль за обеспечением уровня защищенности персональных данных;

4.5.5. знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

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

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

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

4.6. В случае выявления нарушений порядка обработки персональных данных в информационных системах принимаются меры по установлению причин нарушений и их устранению.

## V. Порядок обработки персональных данных субъектов персональных данных, осуществляемой без использования средств автоматизации

5.1. Обработка персональных данных без использования средств автоматизации уполномоченным должностным лицом Министерства осуществляется на материальных (бумажных) носителях персональных данных для целей, указанных в подпунктах 1, 2 пункта 3.1. настоящих Правил на основании постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

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

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

## VI. Порядок обработки персональных данных государственных гражданских служащих Министерства

6.1. Обработка персональных данных государственных гражданских служащих Министерства возможна только с их согласия либо без их согласия в следующих случаях:

- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья государственного гражданского служащего и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;
- по требованию полномочных государственных органов в случаях, предусмотренных федеральными законами.

6.2. Обработка персональных данных государственных гражданских служащих Министерства осуществляется как с использованием средств автоматизации, так и без использования таких средств.

6.3. Порядок обработки, передачи и хранения персональных данных осуществляется следующим образом:

6.3.1. Государственный гражданский служащий Министерства предоставляет в отдел организационной и кадровой работы достоверные сведения о себе. Отдел организационной и кадровой работы проверяет достоверность сведений, сверяя данные, предоставленные государственным гражданским служащим, с имеющимися документами.

6.3.2. В соответствии со статьей 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина министр строительства и жилищно-коммунального хозяйства Псковской области и его представители при обработке персональных данных государственного гражданского служащего должны соблюдать следующие общие требования:

6.3.2.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности государственных гражданских служащих, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

6.3.2.2. При определении объема и содержания, обрабатываемых персональных данных должностные лица Министерства должны руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

6.3.2.3. При принятии решений, затрагивающих интересы государственного гражданского служащего, должностные лица Министерства не имеют права основываться на персональных данных государственного гражданского служащего, полученных исключительно в результате их автоматизированной обработки или электронного получения.

6.3.2.4. Защита персональных данных государственного гражданского служащего от неправомерного их использования

или утраты обеспечивается должностными лицами Министерства за счет средств Министерства в порядке, установленном нормативными правовыми актами.

6.4. В целях обеспечения защиты персональных данных государственные гражданские служащие Министерства вправе:

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

6.4.2. осуществлять свободный доступ к своим персональным данным, включая право получать копии любой записи, за исключением случаев, предусмотренных Федеральным законом;

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

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

## VII. Сроки обработки и хранения персональных данных, порядок их уничтожения при достижении целей обработки или при наступлении иных законных оснований

7.1. 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 является субъект персональных данных. Обработываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

7.2. В случае выявления неправомерной обработки персональных

данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

7.3. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 (тридцати) рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

7.4. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить

обработку персональных данных и уничтожить персональные данные в срок, не превышающий 3 (трех) рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

7.5. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

---



Приложение 3  
к приказу Министерства  
строительства и жилищно-  
коммунального хозяйства  
Псковской области  
от 09.02.2026 № 17-ОД

## ПРАВИЛА

рассмотрения запросов субъектов персональных данных  
или их представителей в Министерстве строительства и жилищно-  
коммунального хозяйства Псковской области

### I. Общие положения

1.1. Правила рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила) в Министерстве строительства и жилищно-коммунального хозяйства Псковской области (далее – Министерство) определяют сроки и последовательность действий структурных подразделений и должностных лиц Министерства, а также порядок их взаимодействия при рассмотрении поступающих в Министерство запросов субъектов персональных данных или их представителей.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон), 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 и муниципальными органами».

1.3. Субъектами персональных данных в Министерстве являются:

- лица, замещающие должности государственной гражданской службы Псковской области в Министерстве;

- лица, претендующие на замещение должностей государственной гражданской службы Псковской области в Министерстве;

- лица, состоящие в кадровом резерве Министерства;

- лица, участвовавшие в конкурсе на замещение вакантной должности государственной гражданской службы Псковской области в Министерстве;

- лица, ранее состоявшие на государственной гражданской службе (в трудовых отношениях) в Министерстве, личные дела которых не переданы на хранение в ГКУ Псковской области «Государственный архив Псковской области».

1.4. Представитель субъекта персональных данных – лицо, действующее от имени субъекта персональных данных в силу полномочий, выраженных в доверенности, указании закона, либо акте уполномоченного на то государственного органа или органа местного самоуправления.

При обращении представителя субъекта персональных данных в Министерство представляется документ, подтверждающий его полномочия, оформленный в соответствии с действующим законодательством.

1.5. Запрос субъекта персональных данных или его представителя представляется в Министерство для рассмотрения в документированной форме. Запрос должен содержать фамилию, имя, отчество заявителя, номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Министерством (реквизиты приказа о назначении на должность либо увольнения с должности, решения конкурсной комиссии и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Министерством, подпись субъекта персональных данных или его представителя.

## II. Права субъектов персональных данных

2.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 2.1.1. подтверждение факта обработки персональных данных Министерством;
- 2.1.2. правовые основания и цели обработки персональных данных;
- 2.1.3. цели и применяемые Министерством способы обработки персональных данных;
- 2.1.4. наименование и местонахождение Министерства, сведения о лицах (за исключением государственных гражданских служащих Министерства), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Министерством или на основании Федерального закона;
- 2.1.5. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством;
- 2.1.6. сроки обработки персональных данных, в том числе сроки их хранения;
- 2.1.7. порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;
- 2.1.8. информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 2.1.9. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению министра строительства и жилищно-коммунального хозяйства Псковской области, если обработка поручена или будет поручена такому лицу;
- 2.1.10. иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

2.2. Право субъекта персональных данных на доступ к его

персональным данным может быть ограничено в соответствии с федеральным законодательством, в том числе если:

2.2.1. обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2.2.2. обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

2.2.3. обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

2.2.4. доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

2.2.5. обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

2.3. Субъект персональных данных вправе требовать от Министерства уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также

принимать предусмотренные законодательством меры по защите своих прав.

2.4. Субъект персональных данных или его представитель вправе направить в Министерство повторный запрос в целях получения сведений, указанных в пункте 2.1. настоящих Правил, и ознакомления с такими персональными данными не ранее чем через 30 (тридцать) рабочих дней после направления первоначального запроса, если более короткий срок не установлен федеральным законодательством, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

2.5. Субъект персональных данных или его представитель вправе направить повторный запрос в целях получения сведений, указанных в пункте 2.1. настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 2.4. Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального запроса. Повторный запрос наряду со сведениями, указанными в пункте 1.5. настоящих Правил, должен содержать обоснование направления повторного запроса.

### III. Порядок рассмотрения запросов субъектов персональных данных или их представителей

3.1. В день поступления запроса субъекта персональных данных или его представителя в Министерство указанный запрос регистрируется в приемной Министерства и передается министру строительства и жилищно-коммунального хозяйства Псковской области в соответствии с правилами документооборота, установленными в Министерстве.

3.2. Структурное подразделение Министерства, ответственное за исполнение указанного запроса, обеспечивает рассмотрение запроса и подготовку необходимой информации в установленный действующим

законодательством срок, после чего передает указанную информацию секретарю Министерства для регистрации и направления ее субъекту персональных данных или его представителю в срок не позднее следующего рабочего дня.

3.3. Министерство обязано сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными в течение 30 (тридцати) рабочих дней с даты получения запроса субъекта персональных данных или его представителя.

3.4. Сведения должны быть предоставлены субъекту персональных данных или его представителю Министерством в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

3.5. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных, субъекту персональных данных или его представителю при получении запроса субъекта персональных данных или его представителя Министерство обязано дать в письменной форме мотивированный ответ, с указанием причин отказа со ссылкой на положение пункта 2.2. настоящих Правил, части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) рабочих дней с даты получения запроса субъекта персональных данных или его представителя.

3.6. В случае отказа субъекту персональных данных или его представителю в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 2.4. и 2.5. настоящих Правил, Министерство обязано дать мотивированный ответ.

3.7. Министерство обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту

персональных данных.

3.8. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Министерство обязано внести в них необходимые изменения.

В срок, не превышающий 7 (семи) рабочих дней со дня представления в Министерство субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Министерство обязано уничтожить такие персональные данные.

Министерство обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.9. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица Министерства обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных в течение трех дней с момента такого обращения или получения указанного запроса на период проверки.

3.10. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица Министерства обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, в течение трех дней с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных

не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.11. В случае подтверждения факта неточности персональных данных уполномоченные должностные лица Министерства на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в течение 7 (семи) рабочих дней со дня представления таких сведений в Министерство и снять блокирование персональных данных.

3.12. В случае выявления неправомерной обработки персональных данных уполномоченные должностные лица Министерства в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных.

В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченные должностные лица Министерства в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение.

Об устранении допущенных нарушений или об уничтожении персональных данных Министерство обязано уведомить в письменной форме субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.13. Для проверки фактов, изложенных в запросах, при необходимости, в Министерстве организуются служебные проверки в соответствии с законодательством Российской Федерации.

3.14. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы субъекту персональных данных либо его представителю.

---

Приложение 4  
к приказу Министерства  
строительства и жилищно-  
коммунального хозяйства  
Псковской области  
от 09.02.2020 № 17-09

ПРАВИЛА  
осуществления внутреннего контроля  
соответствия обработки персональных данных требованиям  
к защите персональных данных, установленных Федеральным законом  
от 27.07.2006 № 152-ФЗ «О персональных данных»  
в Министерстве строительства и жилищно-коммунального хозяйства  
Псковской области

I. Общие положения

1.1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в Министерстве строительства и жилищно-коммунального хозяйства Псковской области (далее – Министерство) определяются:

- процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;
- основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.200 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 15.09.2008 № 687

«Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», 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 и муниципальными органами», приказом ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами.

1.3. Целью настоящих Правил является выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

1.4. В Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

## II. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Министерстве организовывается проведение периодических проверок условий обработки персональных данных.

2.2. Проверки проводятся комиссией по защите персональных данных в Министерстве.

Общее руководство по выполнению мероприятий, связанных с организацией и проведением проверок, возлагается на первого заместителя министра строительства и жилищно-коммунального хозяйства Псковской области – председателя комиссии по защите

персональных данных.

2.3. В проведении проверки не может участвовать государственный гражданский служащий Министерства, прямо или косвенно заинтересованный в ее результатах.

2.4. Проверки соответствия обработки персональных данных установленным требованиям проводятся на основании Плана внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных (приложение 1), утверждаемого приказом Министерства или на основании поступившего письменного заявления субъекта персональных данных о нарушениях правил обработки персональных данных (внеплановые проверки).

2.5. Проведение внеплановой проверки организуется в течение 3 (трех) рабочих дней с момента поступления соответствующего заявления.

2.6. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

2.6.1. порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

2.6.2. порядок и условия применения средств защиты информации;

2.6.3. эффективность принимаемых мер по обеспечению безопасности персональных данных;

2.6.4. состояние учета машинных носителей персональных данных;

2.6.5. соблюдение правил доступа к персональным данным;

2.6.6. наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

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

2.6.8. осуществление мероприятий по обеспечению целостности

персональных данных.

2.7. Комиссия по защите персональных данных при проведении проверки условий обработки персональных данных имеет право:

2.7.1. запрашивать у государственных гражданских служащих Министерства информацию, необходимую для реализации полномочий;

2.7.2. требовать от должностных лиц Министерства, непосредственно осуществляющих обработку персональных данных, уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;

2.7.3. вносить министру строительства и жилищно-коммунального хозяйства Псковской области предложения по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

2.7.4. вносить министру строительства и жилищно-коммунального хозяйства Псковской области предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке.

2.8. Председатель и члены комиссии по защите персональных данных при проведении проверки условий обработки персональных данных должны обеспечивать конфиденциальность ставших им известными в ходе проведения мероприятий внутреннего контроля персональных данных.

2.9. Проверка условий обработки персональных данных должна быть завершена не позднее чем через 30 (тридцать) календарных дней со дня принятия решения о ее проведении.

2.10. По результатам проведенной проверки условий обработки и защиты персональных данных ответственный за организацию обработки персональных данных представляет министру строительства и жилищно-коммунального хозяйства Псковской области письменное заключение о результатах проведенной проверки с указанием мер, необходимых для устранения выявленных нарушений.

---





Приложение 5  
к приказу Министерства  
строительства и жилищно-  
коммунального хозяйства  
Псковской области  
от 09.02.2026 № 17-09

## ПРАВИЛА

работы с обезличенными персональными данными  
в Министерстве строительства и жилищно-коммунального хозяйства  
Псковской области

### I. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными (далее – Правила) в Министерстве строительства и жилищно-коммунального хозяйства Псковской области (далее – Министерство) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления 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».

1.2. Настоящие Правила определяют порядок работы с обезличенными данными в Министерстве.

### II. Основные понятия и определения

2.1. Основные понятия, используемые в настоящих Правилах:

- персональные данные – любая информация, относящаяся

к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

- обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

- обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

### III. Условия обезличивания

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

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;

- обобщение - понижение точности некоторых сведений;

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

- деление сведений на части и обработка в разных информационных системах;

- другие способы.

3.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

3.4. Для обезличивания персональных данных применяются способы, не противоречащие действующему законодательству.

#### IV. Порядок обезличивания персональных данных

4.1. Порядок обезличивания персональных данных в Министерстве.

4.1.1. Руководители структурных подразделений Министерства готовят предложения по обезличиванию персональных данных, обоснование такой необходимости, способ обезличивания и предоставляют курирующему заместителю министра строительства и жилищно-коммунального хозяйства Псковской области (министру строительства и жилищно-коммунального хозяйства Псковской области).

4.1.2. Курирующий заместитель министра и комиссия по защите персональных данных рассматривают и готовят предложения для утверждения министром.

4.1.3. Министр утверждает подготовленные предложения.

4.2. С целью предоставления статистической отчетности в Территориальный орган Федеральной службы государственной статистики по Псковской области обезличивание персональных данных производится должностными лицами отдела организационной и кадровой работы и финансово-экономического отдела.

#### V. Порядок работы с обезличенными персональными данными

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

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

5.3. При обработке обезличенных персональных данных

с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используются);
- правил резервного копирования;
- правил доступа в помещения, где расположены информационные системы персональных данных.

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

- правил хранения бумажных носителей;
  - правил доступа к ним и в помещения, где они хранятся.
-

Приложение 6  
к приказу Министерства  
строительства и жилищно-  
коммунального хозяйства

Псковской области

от 09.02.2026 № 17-08

ПЕРЕЧЕНЬ

информационных систем, используемых в деятельности

Министерства строительства и жилищно-коммунального хозяйства Псковской области

№ п/п	Наименование информационной системы	Область применения	Сопровождение информационной системы	Пользователи	Статус информации
1	1С: Предприятие 8.3 (8.3.13.1690)	обеспечивает автоматизацию бухгалтерского учета государственных (муниципальных) учреждений, состоящих на самостоятельном балансе, финансируемых из федерального (регионального) или местного бюджетов, а также из бюджета государственного внебюджетного фонда, обеспечивает автоматизацию кадрового учета и расчета заработной платы в государственных учреждениях в соответствии с законодательством РФ	Управление цифрового развития и связи Правительство Псковской области	финансово-экономический отдел отдел организационной и кадровой работы	ограничения к распространению – персональные данные

2	Прикладное программное обеспечение «Система удаленного финансового документооборота» (ШО СУФД АСФК), 7.310.90 (031.030.700T04)	обеспечивает удаленное online-взаимодействие участников бюджетного процесса с органом Федерального казначейства	Федеральное казначейство РФ	финансово-экономический отдел	ограничения к распространению – персональные данные
3	СБИС Электронная отчетность, 2.4.638	предназначена для подготовки, проверки и отправки через интернет отчетности в госорганы		финансово-экономический отдел; организационной и кадровой работы	ограничения к распространению – персональные данные
4	Сбербанк Бизнес Онлайн, 4.3	обеспечивает электронный документооборот с банком	Служба технической поддержки ПАО Сбербанк	финансово-экономический отдел	ограничения к распространению – персональные данные
5	Программа подготовки документов для государственной регистрации, 1.4.11	предназначена для автоматизированной подготовки документов, используемых при государственной регистрации, а также формирования контейнера для подачи заявления о государственной регистрации в электронном виде	Федеральное казначейство РФ	финансово-экономический отдел	ограничения к распространению – персональные данные
6	ПК «Бюджет-СМАРТ Про», 19.1.2.12270	предназначен для автоматизации процессов составления, анализа и исполнения бюджета субъекта и бюджетов муниципальных образований	Федеральное казначейство РФ	финансово-экономический отдел	ограничения к распространению – персональные данные
7	ПК «Свод-Смарт», 18.2.2.28127	обеспечивает формирование консолидированной отчетности всеми участниками бюджетного процесса в масштабе субъекта РФ, главного распорядителя, муниципального образования	Федеральное казначейство РФ	финансово-экономический отдел	ограничения к распространению – персональные данные

8	ПК «Региональная система учета государственных и муниципальных платежей» (РСУ ГМП), 19.1.5.1150	- обеспечивает централизованный учет доходов региона и региональных учреждений, ведущих учет платы за оказываемые государственные (муниципальные) услуги, а также иных доходов бюджетов в рамках исполнения Федерального закона № 210-ФЗ, в сочетании с реализацией комплекса мер, направленных на защиту информации при передаче по открытым каналам связи в информационных системах, подключаемых к СМЭВ	Федеральное казначейство РФ	финансово-экономический отдел	ограничения к распространению – персональные данные
9	ПК «Хранилище-КС», 15.4.262.24147	предназначен для проведения многомерного анализа финансовой и другой информации и представляет собой средство для решения стратегических задач бюджетного управления	Федеральное казначейство РФ	финансово-экономический отдел	ограничения к распространению – персональные данные
10	Программа сбора отчетных данных в электронном виде (Data Stretch), 4.5.1	обеспечивает предоставление сведений об органе исполнительной власти и его имуществе	Управление цифрового развития и связи Правительство Псковской области	финансово-экономический отдел	ограничения к распространению – персональные данные
11	Личный кабинет юридического лица на сайте Федеральной налоговой службы	предназначен для электронного документооборота с налоговыми органами	Федеральная налоговая служба	финансово-экономический отдел	ограничения к распространению – персональные данные
12	Личный кабинет на автоматизированной системе торговой площадки сбербанк-АСТ (sberbank-ast.ru)	предназначена для проведения закупок товаров, услуг и работ за бюджетные деньги (согласно ФЗ-44)	Служба технической поддержки ПАО Сбербанк	финансово-экономический отдел	ограничения к распространению – персональные данные

13	Личный кабинет на официальном сайте государственных госзакупок <a href="http://Zakupki.gov.ru">Zakupki.gov.ru</a>	предназначен для предоставления государственному заказчику автоматизации процессов подготовки и размещения закупок	Служба технической поддержки ЕИС	финансово-экономический отдел; отдел организационной и кадровой работы	ограничения к распространению – персональные данные
14	Личный кабинет на сайте Государственной информационной системы «Государственные и муниципальные закупки Псковской области» ( <a href="http://gz.pskov.ru">gz.pskov.ru</a> )	предназначен для предоставления государственному заказчику автоматизации процессов подготовки и размещения закупок	Управление цифрового развития и связи Правительства Псковской области	отдел организационной и кадровой работы	ограничения к распространению – персональные данные
15	Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации	является базовым государственным информационным ресурсом в отношении информации о кадровом составе государственных органов	Министерство связи и массовых коммуникаций Российской Федерации	отдел организационной и кадровой работы	ограничения к распространению – персональные данные
16	Государственная и информационная система жилищно-коммунального хозяйства (ГИСЖКХ)	единая федеральная централизованная система для сбора, обработки, хранения, предоставления, размещения и использования информации, связанной с жилищно-коммунальным хозяйством	Министерство строительства и жилищно-коммунального хозяйства Российской Федерации	отдел коммунальной инфраструктуры; отдел по обращению с твердыми коммунальными отходами; отдел модернизации жилищного фонда	ограничения к распространению – персональные данные
17	Государственная информационная система обеспечения градостроительной деятельности Псковской области (ГИСОГД)	единая цифровая платформа для сбора, хранения, систематизации, обработки и предоставления информации, необходимой для осуществления градостроительной деятельности	ООО «БингоСофт»	отдел строительства	ограничения к распространению – персональные данные

18	Система электронного документооборота Правительства Псковской области (СЭД ПШО)	предназначена для электронного документооборота в подразделениях Аппарата Правительства Псковской области и исполнительных органах Псковской области	Управление цифрового развития и связи Правительства Псковской области	Министерство строительства и жилищно-коммунального хозяйства Псковской области	ограничения к распространению – персональные данные
19	Личный кабинет на Едином портале государственных и муниципальных услуг	предназначен для предоставления государственных услуг	Управление цифрового развития и связи Правительства Псковской области	отдел строительства	ограничения к распространению – персональные данные
20	Платформа обратной связи Псковской области	предназначена для рассмотрения поступивших обращений граждан	Управление цифрового развития и связи Правительства Псковской области	Министерство строительства и жилищно-коммунального хозяйства Псковской области	ограничения к распространению – персональные данные



Приложение 7  
к приказу Министерства  
строительства и жилищно-  
коммунального хозяйства  
Псковской области  
от 09.02.2016 № 17-02

ПЕРЕЧЕНЬ

должностей Министерства строительства и жилищно-коммунального хозяйства Псковской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

1. Министр строительства и жилищно-коммунального хозяйства Псковской области.
2. Первый заместитель министра строительства и жилищно-коммунального хозяйства Псковской области.
3. Заместитель министра строительства и жилищно-коммунального хозяйства Псковской области.
4. Заместитель министра – начальник отдела развития городской среды.
5. Заместитель министра – начальник финансово-экономического отдела.
6. Начальник отдела коммунальной инфраструктуры.
7. Начальник отдела строительства.
8. Начальник отдела модернизации жилищного фонда.
9. Начальник отдела по обращению с твердыми коммунальными отходами.
10. Начальник отдела организационной и кадровой работы.
11. Начальник правового отдела.
12. Заместитель начальника отдела развития городской среды.
13. Заместители начальника отдела коммунальной инфраструктуры.
14. Заместитель начальника отдела строительства.
15. Заместители начальника отдела модернизации жилищного

фонда.

16. Заместители начальника финансово-экономического отдела.
  17. Заместитель начальника отдела по обращению с твердыми коммунальными отходами.
  18. Консультант отдела развития городской среды.
  19. Консультант отдела коммунальной инфраструктуры.
  20. Консультанты отдела строительства.
  21. Консультант отдела модернизации жилищного фонда.
  22. Консультант финансово-экономического отдела.
  23. Консультант отдела по обращению с твердыми коммунальными отходами.
  24. Консультант отдела организационной и кадровой работы.
  25. Консультант правового отдела.
  26. Консультант Министерства с возложением функций режимно-секретного подразделения.
-

Приложение 8  
к приказу Министерства  
строительства и жилищно-  
коммунального хозяйства  
Псковской области  
от 09.02.2026 № 17-09

### ТИПОВОЕ ОБЯЗАТЕЛЬСТВО

служащего, непосредственно осуществляющего организацию обработки персональных данных в Министерстве строительства и жилищно-коммунального хозяйства Псковской области, ставших известными ему в связи с исполнением должностных обязанностей

Я, \_\_\_\_\_,  
замещающий (-ая) должность \_\_\_\_\_

предупрежден (-а) о том, что на период исполнения мною должностных обязанностей по замещаемой должности мне предоставлен доступ к персональным данным сотрудников Министерства строительства и жилищно-коммунального хозяйства Псковской области (далее – Министерство).

Настоящим добровольно принимаю на себя обязательства:

не передавать и не разглашать третьим лицам, сотрудникам Министерства, не имеющим доступа к персональным данным, информацию, содержащую персональные данные сотрудников, за исключением их собственных персональных данных;

не использовать информацию, содержащую персональные данные, с целью получения выгоды;

выполнять требования федерального законодательства и иных нормативных правовых актов Российской Федерации, а также правовых актов Псковской области, регламентирующих вопросы порядка обработки и защиты персональных данных;

прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, после прекращения права на доступ к информации, содержащей персональные данные (в случае перевода на иную должность, не предусматривающую доступ к персональным данным, или в случае прекращения служебного контракта).

Я предупрежден (-а) о том, что в случае нарушения данного обязательства буду привлечен (-а) к дисциплинарной ответственности или иной ответственности в соответствии с действующим законодательством Российской Федерации.

\_\_\_\_\_/\_\_\_\_\_/

(подпись)

(расшифровка подписи)

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

Приложение 9  
к приказу Министерства  
строительства и жилищно-  
коммунального хозяйства  
Псковской области  
от 09.02.2026 № 17-09

ТИПОВАЯ ФОРМА  
разъяснения субъекту персональных данных  
юридических последствий отказа предоставить  
свои персональные данные в связи с поступлением  
на государственную гражданскую службу в Министерство строительства  
и жилищно-коммунального хозяйства Псковской области

Мне,

\_\_\_\_\_  
Претендующему (-ей) на должность \_\_\_\_\_

\_\_\_\_\_  
разъяснены юридические последствия отказа предоставить свои  
персональные данные в Министерство строительства и жилищно-  
коммунального хозяйства Псковской области.

В соответствии со статьями 26, 42 Федерального закона от  
27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской  
Федерации», Положением о персональных данных государственного  
гражданского служащего Российской Федерации и ведении его личного  
дела, утвержденного Указом Президента Российской Федерации  
от 30.05.2005 г. № 609, определен перечень персональных данных,  
которые субъект персональных данных обязан предоставить в связи  
с поступлением на государственную гражданскую службу  
или прохождением государственной гражданской службы.

Без представления субъектом персональных данных обязательных  
для заключения служебного контракта сведений, служебный контракт  
не может быть заключен.

« \_\_\_\_ » \_\_\_\_\_ Г.

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(расшифровка подписи)



Приложение 10  
к приказу Министерства  
строительства и жилищно-  
коммунального хозяйства  
Псковской области  
от 09.02.2026 № 17-09

## ПОРЯДОК

доступа государственных гражданских служащих  
Министерства строительства и жилищно-коммунального хозяйства  
Псковской области в помещения, в которых ведется обработка  
персональных данных

1. Настоящий Порядок доступа государственных гражданских служащих Министерства строительства и жилищно-коммунального хозяйства Псковской области (далее – Министерство) в помещения, в которых ведется обработка персональных данных, разработан с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ 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».
2. В Министерстве персональные данные государственных гражданских служащих и граждан хранятся в соответствующих кабинетах, в которых размещены автоматизированные рабочие места информационных систем персональных данных.
3. Помещения, в которых ведется обработка персональных данных, должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами.
4. Персональные данные на бумажных носителях должны

находиться в недоступном для посторонних лиц месте.

5. Бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) хранятся в металлических шкафах.

6. В Министерстве осуществляется контроль доступа в контролируемую зону (посредством домофона), помещения, в которых ведется обработка персональных данных, запираются на замок.

7. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании служебного дня государственные гражданские служащие Министерства, имеющие право доступа в помещения, обязаны:

7.1. убрать бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) в шкафы, закрыть их;

7.2. отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

7.3. закрыть окна;

7.4. закрыть двери.

8. Перед открытием помещений, в которых ведется обработка персональных данных, государственные гражданские служащие, имеющие право доступа в помещения, обязаны:

8.1. провести внешний осмотр входной двери с целью установления целостности двери и замка;

8.2. открыть дверь и осмотреть помещение, проверить наличие и целостность печатей на шкафах;

9. При обнаружении неисправности двери и запирающих устройств государственные гражданские служащие Министерства обязаны:

9.1. не вскрывая помещение, в котором ведется обработка персональных данных, доложить об обнаруженных неисправностях начальнику структурного подразделения (курирующему заместителю министра);

9.2. в присутствии не менее двух иных государственных гражданских служащих, включая начальника структурного подразделения, вскрыть помещение и осмотреть его;

9.3. составить акт о выявленных нарушениях и передать его министру строительства и жилищно-коммунального хозяйства Псковской области для организации служебного расследования.

10. Право самостоятельного входа в помещения, где обрабатываются персональные данные, имеют только государственные гражданские служащие, непосредственно работающие в данном помещении.

11. Иные работники имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии государственных гражданских служащих, непосредственно работающих в данных помещениях.

12. При работе с информацией, содержащей персональные данные, двери помещений должны быть всегда закрыты.

13. Присутствие государственных гражданских служащих, не имеющих права доступа к персональным данным, должно быть исключено.

14. Техническое обслуживание компьютерной и организационной техники, сопровождение программных средств, в котором ведется обработка персональных данных, а также проведение других работ осуществляются в присутствии государственного гражданского служащего, работающего в данном помещении.

15. В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещение, в котором ведется обработка персональных данных, вскрывается комиссией по защите персональных данных в составе не менее двух человек.

16. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на первого заместителя министра строительства и жилищно-коммунального хозяйства Псковской области.

