МІНІСТЕРСТВО БУДІВНИЦТВА ТА АРХІТЕКТУРИ РЕСПУБЛІКИ КРИМ

МИНИСТЕРСТВО СТРОИТЕЛЬСТВА И АРХИТЕКТУРЫ РЕСПУБЛИКИ КРЫМ

КЪЫРЫМ ДЖУМХУРИЕТИНИНЪ КЪУРУДЖЫЛЫКЪ ВЕ МИМАРЛЫКЪ НАЗИРЛИГИ

ПРИКАЗ

от 8 ноября 2021 года № 396

Об организационных мерах защиты информации, обрабатываемой в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», приказом Федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России) от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые:

1.1. Политику обработки и обеспечения безопасности персональных данных, содержащихся в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым (приложение №1);

1.2. Регламент обработки и обеспечения безопасности персональных данных, содержащихся в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым (приложение №2);

1.3. Перечень персональных данных, обрабатываемых в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым (приложение №3);

1.4. Перечень защищаемых ресурсов Государственной информационной системы обеспечения градостроительной деятельности Республики Крым (приложение №4);

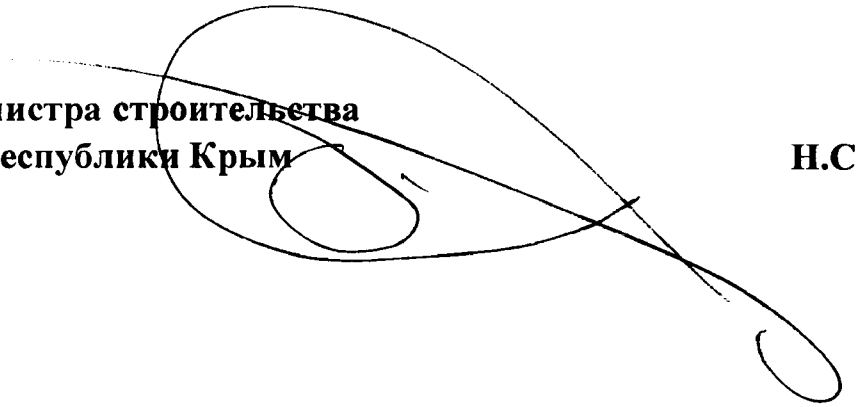
1.5. План мероприятий по контролю за обеспечением безопасности информации в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым (приложение №5);

2. Назначить заведующего отделом информационных систем обеспечения градостроительной деятельности управления реализации документов территориального планирования Фендык П.Ю.:

2.1. Ответственным за обеспечение безопасности информации (в том числе персональные данные), обрабатываемой в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым.

2.2. Ответственным за регистрацию и ведение учета пользователей в Государственной информационной системы обеспечения градостроительной деятельности Республики Крым.

2.3. Контроль за исполнением настоящего приказа оставляю за собой.



Заместитель министра строительства
и архитектуры Республики Крым **Н.С. Тарасов**

Приложение 1
к приказу Министерства
строительства и архитектуры
Республики Крым
от 08.11.2024 № 396

ПОЛИТИКА
обработки и обеспечения безопасности персональных данных в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым

Принятые определения

В настоящей Политике Министерства строительства и архитектуры Республики Крым в отношении обработки и обеспечения безопасности персональных данных Государственной информационной системе обеспечения градостроительной деятельности Республики Крым (далее – Политика) используются термины и определения в значениях, установленных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ).

Сотрудник – Государственный гражданский служащий Министерства строительства и архитектуры Республики Крым.

Оператор – Министерство строительства и архитектуры Республики Крым.

Носитель ПДн – материальный носитель (дела, книги и журналы учета, договоры, иные съемные носители информации, содержащие ПДн) с зафиксированной на нем в любой форме информацией, содержащей ПДн субъектов ПДн в виде текста, фотографии и (или) их сочетания.

1. Общие положения

1.1. Настоящая Политика разработана с целью реализации требований законодательства Российской Федерации в области обработки персональных данных (далее – ПДн) субъектов ПДн, а именно требований Федерального закон № 152-ФЗ, Приказа ФСТЭК от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказ ФСТЭК № 21).

1.2. Если в отношениях с Оператором участвуют законные представители субъектов ПДн, то Оператор становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие локальные акты Оператора распространяются на случаи обработки и обеспечения безопасности ПДн законных представителей субъектов ПДн, даже если эти лица в локальных актах прямо не упоминаются, но фактически участвуют в правоотношениях с Оператором.

1.3. Оператор до начала обработки ПДн осуществляет уведомление уполномоченного органа по защите прав субъектов ПДн о своем намерении

осуществлять обработку ПДн. Оператор уведомляет уполномоченный орган по защите прав субъектов ПДн об изменении сведений, поданных ранее, согласно требованиям Федерального закона № 152-ФЗ.

1.4. В рамках политики реализуются следующие требования законодательства РФ:

1.4.1. Политика описывает принципы обработки оператором ПДн в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым (далее – ГИСОГД РК), права и обязанности Министерства строительства и архитектуры Республики Крым при обработке ПДн, права субъектов ПДн, а также включает перечень мер, применяемых Министерством строительства и архитектуры Республики Крым в целях обеспечения безопасности ПДн при их обработке.

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

1.2.3. Политика является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке и обеспечению безопасности ПДн в информационных системах.

2. Информация об операторе

2.1. Полное наименование: Министерство строительства и архитектуры Республики Крым.

2.2. ИНН: 9102001000.

2.3. Адрес: 295001, Республика Крым, г. Симферополь, ул. Ленина 17.

2.4. Регистрационный номер в Реестре операторов персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (http://rkn.gov.ru/personal-data/register/) (далее – Реестр): 91-15-000700.

2.5. Министерство строительства и архитектуры Республики Крым внесено в Реестр приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 13.12.2019 №92.

3. Правовые основания обработки ПДн

3.1. Обработка ПДн субъектов Оператора осуществляется на основании согласия субъекта ПДн на обработку его ПДн, либо его законного представителя (подпункт 1 пункта 1 статьи 6 Федерального закона № 152-ФЗ).

3.2. Обработка ПДн необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей (подпункт 2 пункта 1 статьи 6 Федерального закона № 152-ФЗ).

3.3. Обработка ПДн необходима для автоматизации процессов информационного обмена, связанные с предоставлением гражданам и

организациям актуальной информации о деятельности органов государственной власти Республики Крым.

4. Объем обрабатываемых ПДн

В ГИСОГД РК обрабатываются ПДн более 100 000 субъектов ПДн.

5. Цели обработки ПДн

5.1. Обработка ПДн осуществляется с целью:

- Осуществление государственных (муниципальных) функций и предоставление государственных (муниципальных) услуг в сфере градостроительной деятельности - предоставление картографических данных гражданам;
- Рассмотрение информации, направляемой для размещения в ГИСОГД РК.

6. Документы, которыми руководствуется Оператор при работе с ПДн

6.1. Оператор при работе с ПДн руководствуется следующими правовыми актами Российской Федерации и руководящими документами ФСТЭК России и ФСБ России:

- Конституцией Российской Федерации;
- Уголовным кодексом Российской Федерации;
- Кодексом Российской Федерации об административных правонарушениях;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Указом Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Распоряжением Президента Российской Федерации от 10 июля 2001 г. № 366-рп «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- 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»;

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

• Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 г.;

• Методикой оценки угроз безопасности информации, утвержденной заместителем директора Федеральной службы по техническому и экспортному контролю 5 февраля 2021 г.;

• Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21;

• Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденного приказом ФСБ России от 10 июля 2014 г. № 378.

7. Принципы обработки ПДн

7.1. Оператор в своей деятельности обеспечивает соблюдение принципов обработки ПДн, указанных в ст. 5 Федерального закона № 152-ФЗ.

7.2. При обработке ПДн обеспечивается исключение:

7.2.1. неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

7.2.2. неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

7.2.3. неправомерного блокирования информации (обеспечение доступности информации).

8. Сроки обработки ПДн

8.1. Сроки обработки ПДн субъектов ПДн в информационных системах Оператора установлены в соответствии с целями обработки ПДн и закреплены в Перечнях информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, обрабатываемой в информационной системе, утверждаемых приказами министра.

8.2. В соответствии с Федеральным законом № 152-ФЗ установлены следующие сроки и условия прекращения обработки ПДн:

8.2.1. не более 30 дней с момента достижения цели обработки ПДн;

8.2.2. не более 30 дней с момента утраты необходимости в достижении целей обработки ПДн;

8.2.3. не более 7 дней с момента предоставления субъектом ПДн, его наследником или представителем субъекта ПДн сведений, подтверждающих, что ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

8.2.4. не более 10 дней с момента выявления невозможности обеспечить правомерность обработки ПДн;

8.2.5. не более 30 дней с момента отзыва субъектом ПДн согласия на обработку ПДн[1], если сохранение ПДн более не требуется для целей обработки ПДн.

9. Способы обработки ПДн

9.1. Обработка ПДн Оператором включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

9.2. Оператор не производит трансграничную передачу ПДн.

9.3. Оператор не принимает решения, порождающие юридические последствия в отношении субъектов ПДн или иным образом затрагивающие их права и законные интересы, на основании исключительно автоматизированной обработки их ПДн.

9.4. Оператор не осуществляет передачу ПДн третьим лицам, за исключением случаев, предусмотренных нормативными правовыми актами Российской Федерации.

9.5. Оператор осуществляет обработку ПДн с использованием средств автоматизации.

10. Состав обрабатываемых ПДн

10.1. Оператор обрабатывает только ПДн, которые отвечают целям, указанным в пункте 5 Политики.

10.2. Оператор не осуществляет обработку биометрических ПДн.

11. Меры по надлежащей организации обработки и обеспечению безопасности ПДн

11.1. Оператор при обработке ПДн принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности ПДн достигается, в частности,

---

[1] Форма отзыва согласия субъектом ПДн на обработку ПДн приведена в приложении А к настоящей Политике.

следующими способами:

11.1.1. Назначением лиц, ответственных за организацию обработки ПДн, и лиц, ответственных за обеспечение безопасности информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, в том числе ПДн (далее – Администратор безопасности информации).

11.1.2. Осуществлением внутреннего контроля соответствия обработки ПДн Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям по обеспечению безопасности ПДн.

11.1.3. Ознакомлением сотрудников Оператора, осуществляющих обработку ПДн, с законодательством Российской Федерации о защите информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, в том числе с требованиями по обеспечению безопасности ПДн, актами в отношении обработки ПДн и/или обучением сотрудников Оператора.

11.1.4. Определением угроз безопасности ПДн при их обработке в информационных системах ПДн.

11.1.5. Применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн, а также на материальных носителях, необходимых для выполнения требований по обеспечению безопасности ПДн.

11.1.6. Оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн.

11.1.7. Учетом носителей ПДн.

11.1.8. Выявлением фактов несанкционированного доступа к ПДн и принятием мер в соответствии с законодательством Российской Федерации об обеспечении безопасности ПДн.

11.1.9. Восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

11.1.10. Установкой правил доступа к ПДн, обрабатываемым в информационной системе ПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в информационной системе ПДн.

11.1.11. Контролем над принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности информационных систем ПДн.

11.2. Обязанности сотрудников Оператора, осуществляющих обработку и защиту ПДн, а также их ответственность, определяются в соответствующих должностных инструкциях сотрудников Оператора.

12. Сотрудники Оператора, ответственные за организацию обработки ПДн и Администратор безопасности информации

12.1. Права, обязанности и юридическая ответственность сотрудников Оператора, ответственных за организацию обработки ПДн и Администратора безопасности информации, установлены Федеральным законом № 152-ФЗ и приказами Министерства строительства и архитектуры Республики Крым.

12.2. Назначение на должность сотрудников Оператора, ответственных за организацию обработки ПДн, и Администратора безопасности информации и

освобождение от нее осуществляется приказом Министерства строительства и архитектуры Республики Крым.

12.3. Сотрудники Оператора, ответственные за организацию обработки ПДн:

12.3.1. Организуют осуществление внутреннего контроля над соблюдением сотрудниками Оператора законодательства Российской Федерации о ПДн, в том числе требований к обеспечению безопасности ПДн.

12.3.2. Доводят до сведения сотрудников Оператора положений законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к обеспечению безопасности ПДн.

12.3.3. Организуют прием и обработку обращений, запросов субъектов ПДн, и осуществляют контроль над приемом и обработкой таких обращений и запросов.

13. Права субъектов ПДн

13.1. Субъект ПДн имеет право на получение сведений об обработке его ПДн в Министерства строительства и архитектуры Республики Крым. Форма запроса для получения данных сведений приведена в приложении Б к настоящей Политике.

13.2. Субъект ПДн вправе требовать от Оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

13.3. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

13.4. Для реализации и защиты своих прав и законных интересов субъект ПДн имеет право обратиться в Министерство строительства и архитектуры Республики Крым. Оператор рассматривает любые обращения и жалобы со стороны субъектов ПДн, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных сотрудников Оператора и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

14. Уполномоченный орган по защите прав субъектов ПДн в Республике Крым

14.1. Полное наименование: Управление федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Крым.

14.2. Краткое наименование: Управление Роскомнадзора по Республике Крым и г. Севастополь.

14.3. Адрес: 295000, Республика Крым, город Симферополь, улица Генерала Васильева, дом 27в.

14.4. Телефон: 8(3652) 66-92-93.

14.5. Адрес электронной почты: rsockanc82@rkn.gov.ru.
14.6. Веб-сайт: https://82.rkn.gov.ru/.

15. Доступ к Политике

15.1. Действующая редакция Политики на бумажном носителе хранится по месту нахождения Оператора по адресу: Республика Крым, г. Симферополь, ул. Ленина, 17.

16. Ответственность

16.1. Сотрудники Оператора, виновные в нарушении норм, регулирующих обработку и обеспечение безопасности ПДн, несут ответственность, предусмотренную законодательством Российской Федерации, локальными актами Оператора.

Приложение 1 к Политике обработки и обеспечения безопасности персональных данных в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым Министерства строительства и архитектуры Республики Крым

Министерство строительства и архитектуры Республики Крым
от _____
паспорт: серия _____,
ФИО

номер _____, выдан _____
_____
_____,
Кем выдан

дата выдачи
_____.

Адрес для получения ответа:

_____.

ЗАПРОС

На основании п.2 ст.9 Федерального Закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» прошу в установленный срок прекратить обработку моих персональных данных в информационной системе _____ в связи с отзывом мною согласия на обработку моих персональных данных.

_____ _____ « » 20 г.
Подпись ФИО Дата

Приложение 2 к Политике обработки и обеспечения безопасности персональных данных в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым Министерства строительства и архитектуры Республики Крым

Министерству строительства и архитектуры Республики Крым
от _____
паспорт: серия _____,
ФИО
номер _____, выдан _____
_____
_____,
Кем выдан
дата выдачи
_____.

Адрес для получения ответа:

_____.

ЗАПРОС

На основании п.1 ст.14 Федерального Закона от 27.07.2006 года №152-ФЗ «О персональных данных» прошу в установленный срок предоставить мне как субъекту персональных данных доступ к моим персональным данным, обрабатываемым в Министерстве строительства и архитектуры Республики Крым на основании заявления №_____, а также следующую информацию:

1) подтверждение факта обработки персональных данных, а также цель такой обработки;
2) сведения об операторе персональных данных;
3) способы обработки персональных данных, применяемые оператором;
4) реализация оператором обязанности по обеспечению безопасности персональных данных;
5) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
6) перечень обрабатываемых персональных данных и источник их получения;
7) сроки обработки персональных данных, в том числе сроки их хранения;

8) сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

_____	_____	« » 20 г.
Подпись	ФИО	Дата

Приложение 2
к приказу Министерства
строительства и архитектуры
Республики Крым
от 08.11.2021 № 396

РЕГЛАМЕНТ

обработки и обеспечения безопасности персональных данных, содержащихся в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым

1. Общие положения

Регламент Министерства строительства и архитектуры Республики Крым в отношении обработки и обеспечения безопасности персональных данных в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым (далее – Регламент) принят в целях защиты информации, в том числе персональных данных (далее – ПДн), обрабатываемых в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым (далее – Оператор).

Регламент определяет права и обязанности государственных гражданских служащих Министерства строительства и архитектуры Республики Крым (далее – Сотрудников) Оператора, порядок использования указанных данных в служебных целях, а также порядок обработки ПДн.

Настоящий Регламент разработан на основе и во исполнение части 1статьи 23, статьи 24 Конституции Российской Федерации, пункта 2 и 3 части 1 статьи 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Положения Регламента распространяются на отношения по обработке и защите ПДн, полученных Оператором как до, так и после утверждения Регламента, за исключением случаев, когда по причинам правового, организационного и иного характера положения Регламента не могут быть распространены на отношения по обработке и обеспечению безопасности ПДн, полученных до его утверждения. Лица из числа сотрудников Оператора, уполномоченные на обработку ПДн, обеспечивающие обработку ПДн в соответствии с требованиями Федерального закона № 152-ФЗ, других правовых актов Российской Федерации и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение мер по обеспечению безопасности этих ПДн, назначаются приказами министра строительства и архитектуры Республики Крым.

Если в отношениях с Оператором участвуют законные представители субъектов ПДн, то Оператор становится оператором ПДн лиц, представляющих указанных субъектов. Положения Регламента и другие локальные акты Оператора распространяются на случаи обработки и обеспечения безопасности ПДн законных представителей субъектов ПДн, даже если эти лица в локальных актах прямо не упоминаются, но фактически участвуют в правоотношениях с Оператором.

1.1. Основные термины и определения

В настоящем Регламенте применяются термины и определения, установленные Федеральным законом № 152-ФЗ, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также руководящими документами ФСТЭК России, регулирующими вопросы обработки и обеспечения безопасности ПДн.

Сотрудник – Государственный гражданский служащий Министерства строительства и архитектуры Республики Крым.

Оператор – Министерство строительства и архитектуры Республики Крым.

Система – Государственная информационная система обеспечения градостроительной деятельности Республики Крым (далее – ГИСОГД РК).

1.2. Документы, которыми руководствуется Оператор при обработке ПДн

Оператор при обработке ПДн руководствуется документами, указанными в разделе 6 Политики Министерства строительства и архитектуры Республики Крым в отношении обработки и обеспечения безопасности персональных данных в ГИСОГД РК.

Сотрудник Оператора, ответственный за обеспечение безопасности информации в ГИСОГД РК (далее – Администратор безопасности информации) в своей работе помимо документов, указанных в разделе 6 Политики Министерства строительства и архитектуры Республики Крым в отношении обработки и обеспечения безопасности персональных данных в ГИСОГД РК, должен руководствоваться следующими локальными актами Оператора:

- настоящим Регламентом;
- политикой Министерства строительства и архитектуры Республики Крым в отношении обработки и обеспечения безопасности персональных данных в ГИСОГД РК;
- планом мероприятий по контролю над обеспечением безопасности персональных данных и уровня защищенности информационной системы;
- иными локальными актами Оператора в сфере обработки и обеспечения безопасности ПДн.

Сотрудники Оператора, непосредственно осуществляющие обработку ПДн в ГИСОГД РК, в своей работе помимо вышеперечисленных правовых актов должны руководствоваться следующими локальными актами Оператора:

- настоящим Регламентом;
- политикой Министерства строительства и архитектуры Республики Крым в отношении обработки и обеспечения безопасности персональных данных в ГИСОГД РК;
- иными локальными актами Оператора в сфере обработки и обеспечения безопасности ПДн.

1.3. Принципы обработки ПДн

Обработка ПДн осуществляется в соответствии с принципами, установленными статьей 5 Федерального закона № 152-ФЗ, а также пунктом 7 документа «Политика Министерства строительства и архитектуры Республики Крым в отношении обработки и обеспечения безопасности персональных данных в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым».

Сотрудники Оператора, в чьи должностные обязанности входит обработка ПДн, подписывают обязательство о неразглашении информации, форма которого приведена в приложении А к настоящему Регламенту.

1.4. Состав, сроки и цели обработки ПДн

Цели, сроки и состав обрабатываемых персональных данных приведены в документе: «Перечень персональных данных, обрабатываемых в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым».

1.5. Способы обработки ПДн

Обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Обработка ПДн осуществляется с применением информационных технологий и технических средств в ГИСОГД РК. Под техническими средствами, позволяющими осуществлять обработку ПДн, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки

речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и прочее), средства обеспечения безопасности ПДн, применяемые в информационных системах.

1.7. Носители ПДн

Носителями ПДн могут являться:

• отчуждаемые электронные носители – магнитные и оптические (CD и DVD) накопители, съемные жесткие диски и флэш-накопители, применяемые для получения информации;

• неотчуждаемые электронные носители – серверы, ноутбуки, персональные компьютеры и другие электронно-вычислительные машины.

2. Требования к сотрудникам Оператора

Приказом министра строительства и архитектуры назначается Администратор безопасности информации. Существенным условием является обязанность Администратора безопасности информации обеспечить конфиденциальность ПДн и их безопасность при обработке в ГИСОГД РК.

Сотрудники Оператора, доступ которых к ПДн, обрабатываемым в ГИСОГД РК, необходим для выполнения служебных (трудовых) обязанностей, допускается к соответствующим ПДн на основании перечня, утверждаемого приказом министра.

При работе с ПДн в ГИСОГД РК сотрудники Оператора, допущенные к обработке этих данных в процессе выполнения служебных обязанностей, должны обеспечивать:

1) проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и(или) передачи их лицам, не имеющим права доступа к такой информации;

2) своевременное обнаружение фактов несанкционированного доступа к ПДн;

3) недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование и целостность данных;

4) возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5) постоянный контроль за обеспечением уровня защищенности ПДн.

Требования к сотрудникам Оператора, работающим с ПДн, включаются в их должностные обязанности в соответствии с Квалификационным справочником должностей руководителей, специалистов и других служащих, утвержденным постановлением Министерства труда и социального развития Российской Федерации от 21 августа 1998 г. № 37.

3. Порядок взаимодействия с субъектами ПДн

Субъект ПДн имеет права на доступ к его ПДн в соответствии со статьей 14 Федерального закона № 152-ФЗ.

Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы на основании исключительно автоматизированной обработки его ПДн не принимается.

Оператор разъясняет цели обработки ПДн субъекту ПДн в случае необходимости, а также получает согласие субъекта ПДн на обработку его ПДн в форме, позволяющей подтвердить наличие такого согласия. Форма согласия на обработку и форма разъяснения приведены в приложении Б и приложении В, соответственно, к настоящему Регламенту.

Оператор рассматривает возражение против автоматизированной обработки в течение тридцати дней со дня его получения и уведомляет субъект ПДн о результатах рассмотрения такого возражения.

4. Реализация Регламента

Оператор принимает необходимые и достаточные меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

Ответственный за организацию обработки ПДн в Министерстве строительства и архитектуры Республики Крым обязан:

1) осуществлять внутренний контроль за соблюдением в Министерства строительства и архитектуры Республики Крым требований нормативных правовых актов и локальных актов Оператора в области обработки и обеспечения безопасности ПДн;

2) доводить до сведения сотрудников Оператора положения нормативных правовых актов Российской Федерации и локальных актов Оператора в области обработки и обеспечения безопасности ПДн;

3) организовывать прием и обработку обращений и запросов субъектов ПДн или их законных представителей и(или) осуществлять контроль приема и обработки таких обращений и запросов.

В соответствии с требованиями нормативных правовых актов в области обработки и обеспечения безопасности ПДн, обработки ПДн с использованием средств автоматизации в Министерства строительства и архитектуры Республики Крым создается ГИСОГД РК.

При необходимости проводится периодическая классификация ГИСОГД РК, определение уровня защищенности, оценка соответствия требованиям по обеспечению безопасности ПДн, оценка эффективности системы защиты информации в соответствии с требованиями нормативных правовых актов в области обеспечения безопасности ПДн.

Для ГИСОГД РК:

1) сформирована модель угроз безопасности информации. На основе модели угроз безопасности информации проводятся мероприятия по обеспечению безопасности информации в соответствии с требованиями, предъявляемым и к установленному классу защищенности (уровню защищенности) информационной системы;

2) разработан Технический паспорт информационной системы.

3) определен Технологический процесс обработки информации в информационной системе;

4) разработан Перечень персональных данных, обрабатываемых в ГИСОГД РК;

5) разработан Перечень защищаемых ресурсов ГИСОГД РК.

Уточнение модели угроз безопасности информации для ГИСОГД РК осуществляется:

а) по решению оператора сегмента ГИСОГД РК на основе периодически проводимого анализа угроз безопасности защищаемой информации с учетом особенностей и (или) изменений в ГИСОГД РК;

б) по результатам контроля выполнения требований к обеспечению безопасности защищаемой информации при ее обработке в информационной системе;

в) при обновлении информации или добавлении новых угроз безопасности информации в Банк данных угроз безопасности информации (bdu.fstec.ru) или при их добавлении в иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации;

г) при изменении требований законодательства Российской Федерации в области защиты информации, нормативно-правовых актов и методических документов;

д) при появлении сведений и фактов о новых возможностях нарушителей, выявлении новых источников угроз безопасности информации, развитии способов и средств реализации угроз безопасности информации;

е) при изменении порядка обработки защищаемой информации в сегментах ГИСОГД РК.

В Министерстве строительства и архитектуры Республики Крым запрещается обработка ПДн в целях, не соответствующих целям создания ГИСОГД РК, эксплуатация ГИСОГД РК в составе, отличном от указанного при создании информационной системы.

В целях обеспечения управления информационной безопасностью ПДн в Министерстве строительства и архитектуры Республики Крым создается система защиты ПДн (далее – СЗПДн).

Объектами защиты СЗПДн являются информация, обрабатываемая Оператором и содержащая ПДн, а также инфраструктура, содержащая и поддерживающая указанную информацию.

СЗПДн реализуется комплексом правовых, организационных и технических мер, которые включают:

1) подготовку локальных актов Оператора по вопросам обработки и обеспечения безопасности ПДн, контроль за исполнением в Министерстве строительства и архитектуры Республики Крым требований нормативных правовых актов и локальных актов Оператора в области обработки и обеспечения безопасности ПДн, а также внесение соответствующих изменений в имеющиеся локальные акты Оператора;

2) письменное оформление обязательств сотрудников Оператора о неразглашении ПДн;

3) доведение до сведения сотрудников Оператора информации об установленной законодательством Российской Федерации ответственности за нарушения, связанные с обработкой и обеспечением безопасности ПДн;

4) обеспечение наличия в положениях о структурных подразделениях Оператора и должностных обязанностях требований по соблюдению установленного порядка обработки и обеспечения безопасности ПДн;

5) разработку и введение в действие локальных актов Оператора по обеспечению безопасности информационной системы;

6) регламентацию процедур создания и осуществление документирования действующих инженерных и информационных систем, программных комплексов, порядка внесения в них изменений и своевременной актуализации эксплуатационной документации;

7) ознакомление сотрудников Оператора с положениями нормативных правовых актов Российской Федерации и локальных актов Оператора в области обработки и обеспечения безопасности ПДн и(или) организацию обучения их правилам обработки и обеспечения безопасности ПДн;

8) проведение мероприятий в форме утверждения планов проверки и контроля по регламентации, установлению, поддержанию и осуществлению контроля за состоянием:

8.1) контрольно-пропускного режима, а также за перемещением технических средств и машинных носителей информации;

8.2) защиты технологических процессов, информационных ресурсов, информации и поддерживающей их инфраструктуры от угроз техногенного характера и внешних неинформационных воздействий;

9) регламентацию в форме инструкций сотрудникам Оператора, участвующим в обработке ПДн, а также отвечающим за организацию обработки и обеспечение безопасности ПДн правил обработки ПДн, в том числе хранение и передачу информации внутри Министерства строительства и архитектуры Республики Крым при взаимодействии с контрагентами Оператора, государственными органами и организациями, обращения с документами (включая электронные документы) и машинными носителями, порядка их учета, хранения и уничтожения;

10) установление в форме инструкций и перечней сотрудникам Оператора правил доступа на объекты, в помещения, в информационную систему, применения в этих целях систем охраны и управления доступом;

11) формирование участков (например, выделение в отдельные виртуальные локальные компьютерные сети технических средств)

администрирования безопасности, мониторинга и аудита, управление доступом к защищаемым ресурсам;

12) организацию технического оснащения объектов и информационной системы в соответствии с существующими требованиями к информационной безопасности;

13) формирование условий и технологических процессов обработки, хранения и передачи информации в Министерстве строительства и архитектуры Республики Крым (включая условия хранения документов в архивах), обеспечивающих реализацию требований нормативных правовых актов, методических документов уполномоченных государственных органов и локальных актов Оператора в области обработки и обеспечения безопасности ПДн;

14) установление полномочий пользователей и форм представления информации пользователям информационной системы;

15) организацию непрерывного процесса контроля (мониторинга) событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к ПДн;

16) организацию необходимых мероприятий с сотрудниками Оператора, а также собеседование с лицами, претендующими на работу в Министерстве строительства и архитектуры Республики Крым, изучение их биографии и проверку предоставляемых сведений; обучение сотрудников Оператора требованиям информационной безопасности;

17) осуществление контроля эффективности организационных мер защиты;

18) разработку защитных технических решений:

18.1) при стратегическом планировании архитектуры информационной системы;

18.2) при выборе технических средств обработки информации;

18.3) при разработке и(или) приобретении программного обеспечения;

19) применение следующих компонентов технических мер защиты:

19.1) защищенных средств (систем) обработки информации, содержащей ПДн;

19.2) межсетевых экранов для логического разделения подсетей и защиты от несанкционированного доступа из внешних (открытых) информационных систем;

19.3) аппаратных и программных средств защиты и контроля, устройств, технических систем и средств, используемых для обеспечения информационной безопасности, в том числе для обнаружения и нейтрализации попыток несанкционированного доступа к информации.

Сотрудники Оператора ознакамливаются с локальными актами Оператора, регламентирующими необходимые действия по обеспечению целостности и доступности ПДн в нештатных ситуациях.

По окончанию сроков обработки ПДн создается комиссия из сотрудников Оператора для уничтожения ПДн. Данные ПДн уничтожаются и

составляется акт об уничтожении, форма которого приведена в приложении 4 к настоящему Регламенту.

5. Правила допуска, хранения и пересылки ПДн

Допуск сотрудников Оператора к обработке ПДн в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

Пересылка ПДн без использования специальных средств защиты информации по общедоступным сетям связи, в том числе сети «Интернет», запрещается.

Пересылка ПДн разрешается только в соответствии с целями обработки ПДн по каналам связи, расположенным в пределах контролируемой зоны, либо по защищенным каналам связи с помощью средств защиты информации, прошедших оценку соответствия в ФСБ России и/или ФСТЭК России.

6. Ответственность за нарушение норм, регулирующих обработку ПДн

Сотрудники Оператора, виновные в нарушении норм, регулирующих обработку и обеспечение безопасности ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

7. Заключительные положения

Настоящий Регламент вступает в силу с момента его подписания.

Настоящий Регламент доводится до всех сотрудников Оператора персонально под подпись, осуществляющих работу с ГИСОГД РК.

Приложение 1 к Регламенту обработки и обеспечения безопасности персональных данных, содержащихся в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым Министерства строительства и архитектуры Республики Крым

ОБЯЗАТЕЛЬСТВО

о неразглашении информации

Я, _____
(фамилия, имя, отчество, адрес, документ, удостоверяющий личность)
_____
_____
_____,
Сотрудник Министерства строительства и архитектуры Республики Крым (далее – Оператор),

обязуюсь:

не разглашать персональные данные физических лиц и другую информацию, в отношении которой установлено требование об обеспечении ее конфиденциальности (далее – сведения ограниченного доступа), которые будут доверены мне Оператором или станут известны в период действия трудового договора, а также сведения ограниченного доступа сторонних предприятий и организаций, переданные мне в ходе служебной деятельности;

не сообщать устно или письменно кому бы то ни было сведения ограниченного доступа без соответствующего разрешения имеющих на то право лиц;

в случае попытки посторонних лиц получить сведения ограниченного доступа немедленно сообщать об этом своему непосредственному руководителю;

не использовать знание сведений ограниченного доступа для занятий любой деятельностью, которая в качестве конкурентного действия может нанести ущерб Оператору;

при прекращении действия служебного контракта все машинные носители сведений ограниченного доступа (документы, электронные носители, черновики, распечатки на принтерах и пр.), которые находились в моем распоряжении в связи с выполнением должностных обязанностей, передать своему непосредственному руководителю;

об утрате или недостаче машинных носителей сведений ограниченного доступа, удостоверений, пропусков, ключей от сейфов (хранилищ), личных

печатей и других фактах, которые могут привести к разглашению сведений ограниченного доступа, а также о причинах и условиях возможной утечки этих сведений немедленно сообщать непосредственному руководителю;

использовать переданные мне Оператором и установленные на рабочем месте технические средства обработки и передачи информации исключительно для выполнения обязанностей, предусмотренных служебным контрактом.

Оператор предоставил мне необходимые условия для выполнения требований по охране сведений ограниченного доступа, к которым я допущен: хранилища для документов, средства для доступа к информационным ресурсам (ключи, пароли и т.п.) и др., определяемые обязанностями, выполняемыми мною.

Оператор оставляет за собой право, но не принимает каких-либо обязательств контролировать надлежащее использование мною технических средств обработки и хранения информации, соблюдение мною мер по защите персональных данных.

Я предупрежден, что разглашение сведений ограниченного доступа, ставших мне известными в период действия трудового договора, может повлечь дисциплинарную, материальную, административную, гражданско-правовую, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации.

«____»_____20__г. _____

(подпись)

Проинструктировал:

«____»_____20__г. _____

(подпись)

Приложение 2 к Регламенту обработки и обеспечения безопасности персональных данных, содержащихся в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым Министерства строительства и архитектуры Республики Крым

ПИСЬМЕННОЕ СОГЛАСИЕ
субъекта персональных данных на обработку персональных данных

Я, _____,
(ФИО полностью)
проживающий по адресу _____,
(адрес)
паспорт _____, выдан _____
(серия и номер) (дата)
_____,
(название выдавшего органа)
в соответствии с требованиями статьи 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» даю свое согласие Министерству строительства и архитектуры Республики Крым, расположенному по адресу: Республика Крым, г. Симферополь, ул. Ленина, 17 (далее – Оператор), на обработку моих персональных данных, включающих:

_____
_____.
(список персональных данных)

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая _____
_____,
(список операций с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение)
с целью _____.
(цель обработки персональных данных)

Настоящее согласие дается на срок _____.
(срок обработки персональных данных)

Я оставляю за собой право отозвать свое согласие посредством
_____
(способ отзыва согласия на обработку персональных данных)

В случае получения моего заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан _____

_____.

(действия и период времени их выполнения)

Приложение 3 к Регламенту обработки и обеспечения безопасности персональных данных, содержащихся в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым Министерства строительства и архитектуры Республики Крым

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные Министерству строительства и архитектуры Республики Крым с целью _____

Мне, _____,
разъяснены юридические последствия отказа предоставить свои персональные данные в Министерство строительства и архитектуры Республики Крым (далее – Оператор).

Оператор осуществляет обработку персональных данных на основе законодательства Российской Федерации, регламентирующего правила обработки персональных данных, а также на основе принятой в Министерстве строительства и архитектуры Республики Крым Политики Министерства строительства и архитектуры Республики Крым в отношении обработки и обеспечения безопасности персональных данных.

Обработка персональных данных в Министерстве строительства и архитектуры Республики Крым осуществляется в связи с выполнением Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Мне как субъекту персональных данных разъяснено, что без предоставления данных, обязательных для _____ _____, мне будет отказано в _____.

«____»_____20__г. _____ /_____/
(дата) (Подпись) (Расшифровка подписи)

Разъяснение провел _____ /_____/
(Подпись) (Расшифровка подписи)

Приложение 4 к Регламенту обработки и обеспечения безопасности персональных данных, содержащихся в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым Министерства строительства и архитектуры Республики Крым

АКТ № _____

уничтожения персональных данных, находящихся в ГИСОГД РК

_____ «____»_____ 20___ г.
(Место уничтожения) (Дата уничтожения)

Комиссия в составе:
Председатель комиссии:

_____ _____
(Должность) (ФИО)

Члены комиссии:

_____ _____
(Должность) (ФИО)

_____ _____
(Должность) (ФИО)

_____ _____
(Должность) (ФИО)

_____ _____
(Должность) (ФИО)

составили настоящий акт о том, что «____»_____20____ г. произведено уничтожение персональных данных, находящихся на:

_____

_____

_____

(наименование АРМ по утвержденной конфигурации, ФИО ответственного пользователя АРМ, заводской или учетный номер системного блока ПЭВМ, носителя информации, способ уничтожения информации)

Уничтожены персональные данные в соответствии с таблицей:

№ п/п	Информация (наименование документа)	Учетный номер	Вид носителя	Количество	Срок хранения

Подписи членов комиссии:

Председатель комиссии:

_____	_____	« » 202 г.
(Подпись)	(ФИО)	(Дата)

Члены комиссии:

_____	_____	« » 202 г.
(Подпись)	(ФИО)	(Дата)
_____	_____	« » 202 г.
(Подпись)	(ФИО)	(Дата)
_____	_____	« » 202 г.
(Подпись)	(ФИО)	(Дата)
_____	_____	« » 202 г.
(Подпись)	(ФИО)	(Дата)

Приложение 5 к Регламенту обработки и обеспечения безопасности персональных данных, содержащихся в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым Министерства строительства и архитектуры Республики Крым

Исходная информация об ГИСОГД РК

№ п/п	Наименование информационной системы	Территориальное размещение компонентов информационной системы[2]	Исходные данные информационной системы		Класс защищенности государственной информационной системы[3] и(или) уровень защищенности информационной системы[4]
1	Государственная информационная система обеспечения градостроительной деятельности Республики Крым	Серверный сегмент: Россия, Республика Крым, г. Симферополь, ул. Козлова, 45А, в здании Акционерного общества «Крымтехнологии»; Сегмент привилегированных пользователей: стационарное автоматизированное рабочее место привилегированного пользователя ГИСОГД РК, 295001, Республика Крым,	Категория обрабатываемых персональных данных:	Иные и общедоступные персональные данные	К3 (в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в
			Количество субъектов персональных данных:	более 100 000	

[2] С указанием физических адресов размещения.
[3] Заполняется на основании акта классификации государственной информационной системы
[4] Заполняется на основании акта определения уровня защищенности информационной системы

№ п/п	Наименование информационной системы	Территориальное размещение компонентов информационной системы[2]	Исходные данные информационной системы		Класс защищенности государственной информационной системы[3] и(или) уровень защищенности информационной системы[4]
		г. Симферополь, ул. Ленина 17, кабинет 314; Сегмент непривилегированных пользователей: стационарное автоматизированное рабочее место непривилегированного пользователя ГИСОГД РК, 295001, Республика Крым, г. Симферополь, ул. Ленина, д. 17, кабинет 311.	Субъекты персональных данных:	Министерства строительства и архитектуры Республики Крым	государственных информационных системах») УЗ3 (в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»)
			Тип актуальных угроз:	3	
			Уровень значимости информации:	УЗ3	
			Масштаб:	региональный	

Приложение 3
к приказу Министерства
строительства и архитектуры
Республики Крым
от 08.11.2021 № 396

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым

1. Общие положения

Перечень персональных данных, обрабатываемых в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым, разработан на основании Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Сведения, подлежащие защите в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым, и сроки их обработки

В Государственной информационной системе обеспечения градостроительной деятельности Республики Крым (далее – ГИСОГД РК) обрабатываются следующие персональные данные:

- ФИО;
- Паспортные данные;
- Дата рождения;
- Пол;
- Адрес регистрации;
- Адрес фактического проживания;
- Номер телефона.

В соответствии с пунктом 5 Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» ГИСОГД РК относится к следующим типам:

а) информационная система, обрабатывающая общедоступные и иные категории персональных данных;

б) информационная система, обрабатывающая персональные данные субъектов персональных данных, не являющихся сотрудниками Оператора.

2. Цель обработки персональных данных

Цели и основание обработки персональных данных в ГИСОГД РК в таблице 1.

Таблица 1 – Цели обработки персональных данных

Перечень субъектов ПДн	Цели обработки ПДн	Правовое основание обработки ПДн
Персональные данные субъектов персональных данных, не являющихся сотрудниками Оператора (субъекты, обращающиеся для предоставления государственных (муниципальных) услуг в сфере градостроительной деятельности)	а) Осуществление государственных (муниципальных) функций и предоставление государственных (муниципальных) услуг в сфере градостроительной деятельности; б) Рассмотрение информации, направляемой для размещения в ГИСОГД РК.	а) Согласие субъекта ПДн на обработку его ПДн согласно подпункту 1 пункта 1 статьи 6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон №152-ФЗ); б) обработка ПДн необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей (подпункт 2 пункта 1 статьи 6 Федерального закона №152-ФЗ) Федеральный закон №59-ФЗ.

Приложение 4
к приказу Министерства
строительства и архитектуры
Республики Крым
от 08.11.2021 № 546

ПЕРЕЧЕНЬ

защищаемых ресурсов Государственной информационной системы обеспечения градостроительной деятельности Республики Крым

В Государственной информационной системе обеспечения градостроительной деятельности Республики Крым предусмотрены роли в соответствии с таблицей 1.

Таблица 1 – Роли Государственной информационной системы обеспечения градостроительной деятельности Республики Крым

№ п/п	Роль
1	Лицо, ответственное за обеспечение безопасности информации (Администратор безопасности информации)
2	Системный администратор
3	Пользователь ИС

Права на доступ к защищаемым ресурсам для каждой из ролей представлены в таблице 2.

Таблица 2 – Права на доступ к защищаемым ресурсам

№ п/п	Роль	Защищаемый ресурс	Права доступа к защищаемой информации				
			R	W	D	A	X
1	Администратор безопасности информации	Средства защиты информации	+	+	+	+	+
		Общесистемное и прикладное программное обеспечение	+	+	-	-	+
		База данных Государственной информационной системы обеспечения градостроительной деятельности Республики Крым	-	-	-	-	-
2	Системный администратор	Средства защиты информации	+	-	-	-	+
		Общесистемное и прикладное программное обеспечение	+	+	+	+	+
		База данных Государственной информационной системы обеспечения градостроительной деятельности Республики Крым	-	-	-	-	-
3	Пользователь ИС	Средства защиты информации	+	-	-	-	+
		Общесистемное и прикладное программное обеспечение	+	+	-	-	+
		База данных Государственной информационной системы обеспечения градостроительной деятельности Республики Крым	+	+	-	+	-

Где: R – право на чтение, W – право на запись, D – право на удаление, A – право на добавление объекта, X – право на исполнение объекта, «+» – есть права доступа, «–» – нет права доступа.

Приложение 5
к приказу Министерства
строительства и архитектуры
Республики Крым
от 08.11.2021 № 396

ПЛАН

мероприятий по контролю за обеспечением безопасности информации в Государственной информационной системе обеспечения градостроительной деятельности Республики Крым

Мероприятие	Периодичность	Исполнитель
Контроль за соблюдением режима обработки персональных данных	Один раз в квартал	Должностное лицо, ответственное за обеспечение безопасности информации (далее – Администратор безопасности информации)
Контроль за реализацией антивирусной защиты и обновлением базы данных признаков вредоносных компьютерных программ (вирусов)	Один раз в квартал	Администратор безопасности информации
Контроль состава технических средств, программного обеспечения и средств защиты информации	Один раз в квартал	Администратор безопасности информации
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты персональных данных	Ежегодно	Администратор безопасности информации
Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Один раз в квартал	Администратор безопасности информации
Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Один раз в квартал	Администратор безопасности информации
Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Ежегодно	Администратор безопасности информации
Мониторинг актуального состояния нормативно-организационных документов	Ежемесячно	Администратор безопасности информации
Контроль за знанием пользователями принятых мер по обеспечению безопасности персональных данных	Ежемесячно	Администратор безопасности информации

Мероприятие	Периодичность	Исполнитель
Организация контроля и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены	Один раз в квартал	Администратор безопасности информации