



АДМИНИСТРАЦИЯ  
Муромского сельского поселения  
Белогорского района  
Республики Крым  
ПОСТАНОВЛЕНИЕ

15 сентября 2020

с.Муромское

№ 177

**Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных Администрации Муромского сельского поселения**

В соответствии с Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», 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» **ПОСТАНОВЛЯЮ:**

1. Утвердить Требования к защите персональных данных при их обработке в информационных системах персональных данных Администрации Муромского сельского поселения согласно приложению.

2. Заместителю главы администрации ознакомить с настоящим постановлением работников Администрации Муромского сельского поселения под роспись.

3. Настоящее постановление вступает в силу со дня, следующего за днем официального опубликования.

Глава Администрации  
Муромского сельского поселения

А.Х.Хамитов

УТВЕРЖДЕНО  
постановлением Администрации  
Муромского сельского поселения  
от 15.09.2020 г. № 177  
Приложение № 1

## **Требования к защите персональных данных при их обработке в информационных системах персональных данных Администрации Муромского сельского поселения**

1. Настоящие документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных Администрации Муромского сельского поселения (далее - информационные системы) представляющих собой совокупность персональных данных, содержащихся в базах данных, а также технических средств, позволяющих осуществлять обработку персональных данных с использованием средств автоматизации (далее - информационные системы).

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

2. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные Администрации Муромского сельского поселения (далее - оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора (далее - уполномоченное лицо).

3. Безопасность персональных данных достигается путем 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.

Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей угрозы. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах. Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и 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. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором.

5. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

6. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.

7. Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в пункте 6, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора или уполномоченного лица.

8. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) 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;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

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

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

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) 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;

к) описание системы защиты персональных данных.

9. При обнаружении нарушений порядка предоставления персональных данных оператор или уполномоченное лицо незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.