



**МАРИЙ ЭЛ РЕСПУБЛИКЫН
ЧОНГЫМАШ,
АРХИТЕКТУР ДЕН
ИЛЕМ-КОММУНАЛ
ОЗАНЛЫК
МИНИСТЕРСТВЫЖЕ**

**МИНИСТЕРСТВО
СТРОИТЕЛЬСТВА,
АРХИТЕКТУРЫ И ЖИЛИЩНО-
КОММУНАЛЬНОГО
ХОЗЯЙСТВА
РЕСПУБЛИКИ МАРИЙ ЭЛ**

П Р И К А З

от 15 сентября 2016 г. № 417

Об утверждении Положения об обработке персональных данных в информационных системах персональных данных в Министерстве строительства, архитектуры и жилищно- коммунального хозяйства Республики Марий Эл

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

п р и к а з ы в а ю:

1. Утвердить прилагаемое Положение об обработке персональных данных в информационных системах персональных данных в Министерстве строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл.

2. Приказ Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл от 31 октября 2008 г. № 420 «Об утверждении Положения об обработке персональных данных в информационных системах персональных данных в Министерстве строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл» признать утратившим силу.

Министр

Э.В.Варенова

УТВЕРЖДЕНО
приказом Министерства строительства,
архитектуры и жилищно-коммунального
хозяйства Республики Марий Эл
от 15 сентября 2016 г. № 417

ПОЛОЖЕНИЕ
об обработке персональных данных
в информационных системах персональных данных
в Министерстве строительства, архитектуры и жилищно-
коммунального хозяйства Республики Марий Эл

1. Настоящим Положением в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятые в соответствии с ним иные правовые документы.

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 (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 т.п.), средства защиты информации, применяемые в информационных системах.

2. Список должностных лиц, отвечающие за безопасность персональных данных, обрабатываемых в информационных системах и должностных лиц, осуществляющие обработку персональных данных, либо имеющих доступ к ним утверждается приказом Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Марий Эл.

3. При обработке персональных данных должны быть соблюдены следующие требования:

а) обработка персональных данных осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, Конституции Республики Марий Эл, федеральных законов, законов Республики Марий Эл и иных нормативных правовых актов Российской Федерации и Республики Марий Эл;

б) обработка персональных данных осуществляется оператором с согласия субъектов персональных данных, за исключением следующих случаев:

обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

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

обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности;

в) в случае, если на основании договора требуется поручить обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке;

г) при принятии решений, затрагивающих интересы гражданского служащего или лица, замещающего государственную должность Республики Марий Эл, запрещается основываться на их персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

д) защита персональных данных от неправомерного их использования или утраты обеспечивается за счет средств министерства в порядке, установленном федеральными законами.

4. В целях обеспечения защиты персональных данных, хранящихся в личных делах, лица, замещающие государственные должности Республики Марий Эл, и гражданские служащие имеют право:

а) получать полную информацию о своих персональных данных и обработке этих данных;

б) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;

в) требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона, в случае отказа в исключении или исправлении персональных данных заявлять в письменной форме о своем несогласии с обоснованием такого несогласия. Персональные данные оценочного

характера лицо, замещающее государственную должность Республики Марий Эл, или гражданский служащий имеет право дополнить заявлением, выражающим его собственную точку зрения;

г) обжаловать в суд любые неправомерные действия или бездействие представителя нанимателя или уполномоченного им лица при обработке и защите персональных данных гражданского служащего.

5. 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 информационных системах 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-технических 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.

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.

6. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

7. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

8. Информационные системы классифицируются в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

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

10. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа

с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

11. При обработке персональных данных в информационной системе должно быть обеспечено:

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

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

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

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

12. 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.
