

ПРИЛОЖЕНИЕ № 1
УТВЕРЖДЕНА
приказом директора учреждения
от «06» октября 2015г. № 227

ПОЛИТИКА
безопасности персональных данных в Тамбовском областном
государственном казенном учреждении
«Пожарно-спасательный центр»

1. ВВЕДЕНИЕ

Политика безопасности персональных данных (далее - Политика) определяет стратегию защиты персональных данных, обрабатываемых в Тамбовском областном государственном казенном учреждении «Пожарно-спасательный центр» (далее - учреждение) и формулирует основные принципы и механизмы защиты персональных данных.

Персональные данные являются конфиденциальной, строго охраняемой информацией.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, 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.

Настоящий документ разработан в соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных», Постановлений Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и других определяющих случаи и особенности обработки персональных данных нормативных правовых актов.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сведениями, составляющими персональные данные, обрабатываемые в учреждении является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), за исключением не обрабатываемых в учреждении персональных данных, касающихся расовой принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

В зависимости от субъекта персональных данных, учреждение обрабатывает персональные данные следующих категорий:

- а) иные категории персональных данных субъектов, являющихся работниками учреждения;
- б) иные категории персональных данных субъектов, не являющихся работниками учреждения;
- в) специальные категории персональных данных субъектов, не являющихся работниками учреждения;
- г) биометрические категории персональных данных субъектов, являющихся работниками учреждения.

3. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных должна осуществляться на основе следующих принципов:

обработка персональных данных должна осуществляться на законной и справедливой основе;

обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;

не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

обработке подлежат только персональные данные, которые отвечают целям их обработки;

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;

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;

хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором,

стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

обрабатываемые 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;

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;

обязанность лица, осуществляющего обработку персональных данных по поручению оператора, соблюдения принципов и правил обработки персональных данных;

соблюдение принципов и правил обработки персональных данных при поручении такой обработки другому лицу;

соблюдение конфиденциальности персональных данных;

обработка персональных данных (в том числе при обработке общедоступных персональных данных, специальных категорий персональных данных, биометрических персональных данных, при принятии решений на основании исключительно автоматизированной обработки персональных данных, при трансграничной передаче персональных данных) с письменного согласия субъектов персональных данных либо на ином законном основании;

соблюдение законности при осуществлении трансграничной передачи персональных данных;

соблюдением обязанностей, возлагаемых на оператора персональных данных, действующим законодательством и иными нормативными актами по обработке персональных данных;

принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством в области персональных данных;

принятие необходимых правовых, организационных и технических мер или обеспечении их принятия для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

недопустимость ограничения прав и свобод человека и гражданина по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в информационных системах персональных данных, конкретному субъекту персональных данных;

недопустимость использования оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в информационных системах персональных данных, конкретному субъекту персональных данных;

личная ответственность должностных лиц, осуществляющих обработку персональных данных;

документальное оформление всех принятых решений по обработке и обеспечению безопасности персональных данных.

4. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Учреждение, являясь оператором персональных данных, должно определять цели обработки персональных данных в своих информационных системах персональных данных.

Цели обработки персональных данных в информационных системах персональных данных должны быть четко определены и соответствовать:

заявленным основным полномочиям и правам учреждения;
перечням задач или функций структурных подразделений (должностных лиц) учреждения, указанным в положениях о таких структурных подразделениях (должностных обязанностях).

Определение целей обработки персональных данных в информационных системах персональных данных производится в Правилах обработки персональных данных конкретных информационных систем персональных данных учреждения.

Цели обработки персональных данных определяют:
содержание и объем 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.

Цели обработки персональных данных должны быть:
конкретны;
заранее определены;
законны;
заявлены.

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

Совместимость целей определяется по наличию общей цели, связанной с заявленными в Положении основными полномочиями и правами учреждения или по наличию общей цели, определяемой действующим законодательством Российской Федерации.

5. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сроки обработки указанных выше персональных данных определяются согласием субъекта на обработку персональных данных, сроком исковой давности, а также иными требованиями законодательства Российской Федерации и документов учреждения. Обработка персональных данных прекращается с ликвидацией учреждения.

6. ПРАВА И ОБЯЗАННОСТИ

Права и обязанности учреждения.

Учреждение как оператор персональных данных, вправе:

отстаивать свои интересы в суде;

предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;

использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством.

Права и обязанности субъекта персональных данных.

Субъект персональных данных имеет право:

требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

требовать перечень своих персональных данных, обрабатываемых учреждением и источник их получения;

получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;

требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;

на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

7. ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Персональные данные субъектов подлежат обработке с использованием средств автоматизации или без использования таких средств.

Обработка персональных данных в учреждении подразумевает действия по сбору, записи, систематизации, накоплению, хранению, уточнению (обновление, изменение), извлечению, использованию, передачи (предоставление), обезличивание, блокирование, удаление, уничтожение персональных данных субъектов, персональные данные которых обрабатываются в учреждении.

В целях координации действий по обеспечению безопасности персональных данных в учреждении назначены ответственные лица за организацию обработки персональных данных и за обеспечение безопасности персональных данных.

Обеспечение безопасности персональных данных, а также разработка и внедрение средств защиты персональных данных основывается на анализе угроз безопасности персональных данных.

Для обеспечения внутренней защиты персональных данных работников в помещения, в которых хранятся персональные данные, имеют право доступа только те сотрудники, перечень которых утвержден приказом директора учреждения.

Для защиты персональных данных соблюдается ряд мер организационно-технического характера:

ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные;

технические средства охраны, сигнализации;

защита паролями доступа персональных компьютеров, на которых содержатся персональные данные.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

Обработка персональных данных средствами автоматизации в учреждении допускается только в следующих случаях:

обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на учреждение функций, полномочий и обязанностей;

обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

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

обработка персональных данных необходима для осуществления прав и законных интересов учреждения или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

осуществляется обработка персональных данных, доступ неограниченного круга лиц, к которым предоставлен субъектом персональных

данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

8. ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

Обработка персональных данных средствами автоматизации в учреждении допускается только в следующих случаях:

обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на учреждение функций, полномочий и обязанностей;

обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

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

обработка персональных данных необходима для осуществления прав и законных интересов учреждения или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

осуществляется обработка персональных данных, доступ неограниченного круга лиц, к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Обработка персональных данных средствами автоматизации должна осуществляться на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки

информации, содержащих такие данные, определенные для выполнения конкретных операций с заранее определенными целями, с учетом требований принятых в учреждении положений по обработке персональных данных.

9. ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых, заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности, при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных, осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать:

сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации,

имя (наименование) и адрес оператора,

фамилию, имя, отчество и адрес субъекта персональных данных,

источник получения персональных данных,

сроки обработки персональных данных,

перечень действий с персональными данными, которые будут совершаться в процессе их обработки,

общее описание используемых оператором способов обработки персональных данных;

типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку

персональных данных, осуществляемую без использования средств автоматизации – при необходимости получения письменного согласия на обработку персональных данных;

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

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

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

10. ПОРЯДОК ОБРАБОТКИ ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ответственным за обработку обращений субъектов персональных данных является уполномоченное лицо, ответственное за организацию обработки персональных данных.

При поступлении обращения от субъекта персональных данных указанное лицо обязано:

убедиться, что обращение субъекта персональных данных зарегистрировано согласно процедурам, установленным в учреждение;

действовать в соответствии с Федеральным законом «О персональных данных» № 152-ФЗ;

уведомить директора учреждения о поступлении обращения субъекта персональных данных;

убедиться в отсутствии в обращении требования, нарушающего конституционные права и свободы других лиц;

подготовить ответ, удовлетворяющий запрос субъекта персональных данных, или мотивированный отказ (в случае если исполнение запроса может повлечь нарушение конституционных прав и свобод других лиц);

сделать соответствующую запись в Журнале учета обращений субъектов персональных данных при обработке персональных данных в ИСПДн учреждении;

направить соответствующий ответ в адрес субъекта персональных данных.

11. ОТВЕТСТВЕННОСТЬ

Работники учреждения, разгласившие персональные данные субъектов ПДн, а также работники, по вине которых произошло нарушение конфиденциальности ПДн, и работники, создавшие предпосылки к нарушению конфиденциальности персональных данных, несут ответственность, предусмотренную действующим законодательством Российской Федерации, внутренними документами учреждения.

12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящая Политика является внутренним документом учреждения, является общедоступной и подлежит размещению на официальном сайте учреждения.

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.

Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных учреждения.

Ответственность должностных лиц учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами учреждения.