УТВЕРЖДЕНО
Приказом директора МУП «Теплоэнергия»
№ 219 от 7. 07. 16

ПОЛОЖЕНИЕ

по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МУП «Теплоэнергия»

(далее - Положение)

1. Термины и определения

1.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.2. Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

1.4. Информационная система персональных данных (далее - ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.5. Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.6. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

1.7. Конфиденциальность персональных данных - обязательное для соблюдения оператора или иных лиц, получивших доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2. Общие положения

2.1. Настоящее положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в ИСПДн, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и

технических средств, позволяющих осуществлять обработку таких персональных данных с использованием и без использования средств автоматизации, в МУП «Теплоэнергия».

2.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказом Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России) от 18.03.2013 № 21 «Об утверждении Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2.3. Обработка персональных данных в МУП «Теплоэнергия» осуществляется на основе принципов:

законности целей и способов обработки персональных данных; соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

недопустимости объединения созданных для несовместимых между собой целей баз данных ИСПДн.

3. Порядок определения защищаемой информации

3.1. МУП «Теплоэнергия» создает в пределах своих полномочий, установленных в соответствии с федеральными законами, ИСПДн, в целях обеспечения реализации прав субъектов персональных данных.

3.2. В МУП «Теплоэнергия» на основании перечня сведений конфиденциального характера, утвержденного Указом Президента Российской Федерации от 06.03.97 № 18, определяется и утверждается перечень сведений ограниченного доступа, не относящихся к государственной тайне (далее - конфиденциальной информации), и перечень информационных систем персональных данных. Доступ к персональным данным имеют следующие должностные лица, непосредственно использующие их в служебных целях по своим направлениям:

- Руководитель МУП «Теплоэнергия» и его заместители;
- Работники отдела кадров;
- Работники юридического отдела;
- Работники отдела реализации;
- Работники бухгалтерии;
- Работники службы корпоративной защиты.
- Работники отдела АСУП

3.3. На стадии проектирования каждой ИСПДн определяются цели и содержание обработки персональных данных, утверждается перечень обрабатываемых персональных данных.

4. Основные условия проведения обработки персональных данных

4.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, составленного по форме согласно приложению 1 к настоящему Положению или сформированного в информационной системе персональных данных, за исключением случаев, указанных в пунктах 2-11 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Вологодской области за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

4.2 Операторами ИСПДн МУП «Теплоэнергия», организующими и осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных, являются отделы МУП «Теплоэнергия», непосредственно осуществляющие обработку персональных данных, ведение ИСПДн.

4.3. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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.

4.4. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним другими нормативными правовыми актами.

4.5. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в ИСПДн оператором назначается должностное лицо, ответственное за обеспечение безопасности персональных данных.

4.6. Директор МУП «Теплоэнергия», в чьем ведении находятся ИСПДн:

- определяет сотрудников, допущенных к обработке персональных данных;

- издает нормативные правовые акты: определяющие политику оператора в отношении обработки персональных данных: по вопросам обработки персональных данных: устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства в области защиты информации.

4.7. Проведение внутреннего контроля и (или) аудита соответствия обработки персональных данных в МУП «Теплоэнергия» требованиям по защите информации осуществляют:

- должностное лицо, назначенное ответственными за обеспечение безопасности персональных данных в МУП «Теплоэнергия»;

- члены комиссии по защите информации МУП «Теплоэнергия».

4.8. Сотрудники, непосредственно осуществляющие обработку персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением, нормативными правовыми актами МУП «Теплоэнергия» и инструкциями в области защиты информации и подписывают обязательство о неразглашении информации, содержащей персональные данные, по форме согласно приложению 2 к настоящему Положению. Должностные инструкции сотрудников, допущенных к обработке персональных данных, должны содержать сведения о допуске к персональным данным и основания, на которых данный допуск осуществлен (наименование, дата и № соответствующего федерального закона).

4.9. Оператором и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных. Оператор или иное лицо, получившее доступ к персональным данным, обязано не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

4.10. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные соответствующими федеральными законами по защите информации.

В поручении оператор:

- определяет перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки;

- устанавливает обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;

- указывает требования к защите обрабатываемых персональных данных.

В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор, а лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

5. Правила обработки и защиты персональных данных в информационных системах с использованием и без использования средств автоматизации

5.1. Обеспечение безопасности персональных данных достигается:

- определением угроз безопасности персональных данных при их обработке в ИСПДн;

- применением организационных и технических мер по обеспечению безопасности персональных данных;

- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;

- учетом машинных носителей персональных данных;

- использованием организационных мер, технических, аппаратно- программных средств обнаружения фактов несанкционированного доступа к персональным данным и принятием необходимых мер противодействия и защиты;

- наличием системы резервирования и восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним, технологических, аппаратных, программных сбоях;

- установлением правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИСПДн.

5.2. Обработка персональных данных в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработки в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

5.3. Обработка персональных данных без использования средств автоматизации (в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации) осуществляется в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств

интересов иных субъектов персональных данных;

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

6.3. При использовании внешних электронных носителей информации с персональными данными, к ним предъявляются следующие требования:

а) электронные носители информации, содержащие персональные данные, учитываются в журнале учета, выдачи и уничтожения машинных носителей данных, предназначенных для обработки и хранения информации ограниченного доступа, не относящейся к государственной тайне, персональных данных, в МУП «Теплоэнергия»;

б) к каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

6.4. Все документы, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы условия, обеспечивающие их сохранность.

7. Требования к обработке и защите персональных данных в информационных системах с использования средств автоматизации.

7.1 Обработка персональных данных, осуществляемая с использования средств автоматизации, должна осуществляться таким образом, чтобы обеспечивались следующие требования:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них.

7.2 Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

- определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;
- адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или

автоматизации», утвержденным Постановлением Правительства Российской Федерации 15.09.2008 № 687.

5.4. Мероприятия по обеспечению безопасности персональных данных проводятся в соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах », утвержденных приказом ФСТЭК Росси от 18.02.2013 № 21.

5.5. Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации ИСПДн, инструкции пользователя, администратора по организации антивирусной защиты, парольной защиты автоматизированных систем, и других нормативных и методических документов;
- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;
- охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

6. Требования к обработке и защите персональных данных в информационных системах без использования средств автоматизации

6.1 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы отдельным приказом по Предприятию в отношении каждой категории персональных данных были:

- определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- введен контроль за соблюдением указанных выше условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ.

6.2. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, 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;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) 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

структурно-функциональными характеристиками, не свойственными информационной системе);

- уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

- дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

7.3 При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

8. Порядок привлечения специализированных сторонних организаций к разработке ИСПДн и средств защиты информации МУП «Теплоэнергия»

8.1. Порядок привлечения специализированных сторонних организаций к разработке и эксплуатации новых ИСПДн, их задачи и функции на различных стадиях создания и эксплуатации ИСПДн определяются руководителем МУП «Теплоэнергия», исходя из особенностей автоматизированных систем.

8.2 Выбор и реализация методов и способов защиты информации в ИСПДн МУП «Теплоэнергия», контроль за эксплуатацией ИСПДн осуществляется должностным лицом, назначенным ответственным за обеспечение безопасности персональных данных в МУП «Теплоэнергия». При необходимости привлекаются специалисты по защите информации Муниципального бюджетного учреждения "Центр муниципальных информационных ресурсов и технологий".

8.3 Для проведения мероприятий по обеспечению безопасности персональных данных для ИСПДн 1 класса привлекаются специализированные сторонние организации, имеющие лицензии ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

9. Ответственность должностных лиц

Сотрудники, допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 1
к положению

СОГЛАСИЕ на обработку персональных данных

Я, _____,
(Ф.И.О)
_____ серия _____№_____ выдан _____
(вид документа, удостоверяющего личность)
_____,
(когда и кем)
проживающий (ая) по адресу : _____*
_____ ,
настоящим даю свое согласие на обработку _____**
(наименование и адрес оператора) моих персональных данных и
подтверждаю, что, давая такое согласие, я действую своей волей и в своих интересах.

Согласие дается мною для целей _____
(цель обработки персональных данных)
и распространяется на следующую информацию: _____

(перечень персональных данных)

С вышеуказанными персональными данными могут быть совершены следующие действия: сбор, систематизация, накопление, автоматизированная обработка, хранение, уточнение (обновление, изменение), использование, предоставление вышеуказанных данных по запросу руководителей органов мэрии города или по письменному запросу сторонних организаций (только в целях реализации полномочий органов местного самоуправления), обезличивание, блокирование, уничтожение персональных данных, а также осуществление действий с моими персональными данными в соответствии с федеральным законодательством.1

Персональные данные могут обрабатываться с помощью средств вычислительной техники, а также в письменной форме без использования средств автоматизации.2

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

Данное согласие действует до «_____» _____ _____ г.

---

1 - Перечисляются только те действия, которые будут осуществляться с персональными данными.
(фамилия, инициалы лица, давшего согласие)

СОГЛАСИЕ на получение персональных данных у третьего лица

В _____
(Наименование отдела, управления)

Я, _____
(Фамилия, имя, отчество)

_____
(занимаемая должность)

даю свое согласие на получение моих персональных данных, а именно:

_____

_____

_____

У (в) _____
(указать источник - третье лицо, у которого могут быть получены сведения о работнике)

с целью _____

_____
(указать цель получения персональных данных)

в документальной, электронной, устной (по телефону) форме (нужное подчеркнуть) в течение _____
(указать срок действия согласия)

Настоящее согласие может быть отозвано мной в письменной форме.

(фамилия, инициалы лица, давшего согласие) (подпись)

Приложение 2 к
положению

ОБЯЗАТЕЛЬСТВО о неразглашении информации, содержащей персональные данные

Я,_____
(Ф.И.О.)
исполняющий (ая) должностные обязанности по замещаемой должности

(должность, наименование структурного подразделения)

предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному руководителю.
3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.
4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.
5. После прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

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

(фамилия, инициалы) (подпись)

« » г.
(фамилия, инициалы имени, отчества лица, давшего согласие) (подпись)

« _____» _____ г.

СОГЛАСИЕ

на передачу персональных данных третьему лицу

В _____
(Наименование отдела, управления)

Я, _____
(Фамилия, имя, отчество)

_____
(занимаемая должность)

даю свое согласие на передачу моих персональных данных, а именно:

_____

_____

_____

в _____
(указать третье лицо, которому передаются сведения о работнике)

с целью _____

_____
(указать цель передачи персональных данных)

в документальной, электронной, устной (в т.ч. по телефону) форме (нужное подчеркнуть) в течение _____
(указать срок действия согласия)

Настоящее согласие может быть отозвано мной в письменной форме.

(подпись)

* - Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем. В этом случае в согласии указывается фамилия, имя.отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этогопредставителя

** - Если обработка персональных данных поручается третьему лицу, в согласии дополнительно указывается наименование или фамилия, имя.отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора.

**** - Указываются способы обработки персональных данных, используемые оператором