УТВЕРЖДЕНО

Приказом №
От «22» 12 2010г.

№_____

Директор МУП «Тепловые сети»

_____В. И. Фомин

П О Л О Ж Е Н И Е №1

О защите персональных данных работников

1. Общие положения

Настоящее положение устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников муниципального унитарного предприятия «Тепловые сети».

Под сотрудниками подразумеваются лица, имеющие трудовые отношения с муниципальным унитарным предприятием «Тепловые сети».

1.1. Цель

Настоящее Положение является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся у работодателя, посредством планомерных действий по совершенствованию организации труда.

1.2. Основания

Основанием для разработки данного Положения являются:

- Конституция Российской Федерации от 12.12.1993г.
- Гражданский кодекс РФ;
- Трудовой кодекс РФ;
- Кодекс РФ об административных правонарушениях №195-ФЗ от 30.12.2001г.;
- Федеральный закон №24-ФЗ от 20.02.1995 «Об информации, информационных технологиях и защите информации»;
- Указ Президента РФ №188 от 06.09.1997 «Об утверждении перечня сведений конфиденциального характера»;
- Правила внутреннего трудового распорядка.

1.3. Порядок ввода в действие Положения о защите персональных данных и изменений к нему

Положение о защите персональных данных и изменениях к нему вводятся приказом по общей деятельности МУП «Тепловые сети» и утверждаются директором предприятия. Все сотрудники предприятия должны быть ознакомлены под расписку с данным Положением и изменениями к нему.

2. Понятие и состав персональных данных

2.1. Под персональными данными сотрудников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией. К персональным данным относятся:
-все биографические данные сотрудника;
-образование;
-специальность;
-занимаемая должность;
-наличие судимостей;
-адрес места жительства;
-домашний телефон;
-состав семьи;
-место работы или учебы членов семьи и родственников;
-характер взаимоотношений в семье;
-размер заработной платы;
-содержание трудового договора;
-состав декларируемых сведений о наличии материальных ценностей;
-содержание декларации, подаваемой в налоговую инспекцию;
-подлинники и копии приказов по личному составу;
-личные дела, личные карточки (форма Т-2) и трудовые книжки сотрудников;
-основания к приказам по личному составу;
-дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
-копии отчетов, направляемые в органы статистики;
-анкета;
-копии документов об образовании;
-результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
-фотографии и иные сведения, относящиеся к персональным данным сотрудника.

2.2. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения – соответствующий гриф ограничения на них не ставится.

2.3. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.
Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал сотрудником) или изъявил желание вступить

в трудовые отношения с работодателем. Субъект персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных.
Держателем персональных данных является работодатель, которому сотрудник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

2.4. Права и обязанности работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным работодателем. Указанные права и обязанности он может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

2.5.Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

3. Принципы создания, обработки и хранения персональных данных.

3.1. Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.
Получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.
3.2. Все персональные данные сотрудника получаются у него самого. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Работодатель должен сообщить сотруднику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа сотрудника дать письменное согласие на их получение.
3.3. Не допускается получение и обработка персональных данных сотрудника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.
3.4. Пакет анкетно-биографических и характеризующих материалов сотрудника обязательно содержит личную карточку формы Т-2, а также может содержать документы, содержащие персональные данные сотрудника, в порядке, отражающем процесс приема на работу: заявление сотрудника о приеме на работу, результат медицинского обследования на предмет годности к осуществлению трудовых обязанностей, приказ о приеме на работу, расписка сотрудника об ознакомлении с документами организации, устанавливающими порядок обработки персональных данных работников, а также об его правах и обязанностях в этой области, расписка сотрудника об ознакомлении его с локальными нормативными актами организации.
При заполнении личной карточки Т-2 используются следующие документы:
-паспорт;
-трудовая книжка;
-военный билет;
-документы об образовании.

Изменения, вносимые в карточку Т-2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).
Сотрудник отдела кадров, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу сотрудника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.
3.6. При обработке персональных данных сотрудников работодатель в лице директора вправе определять особые способы обработки, документирования, хранения и защиты персональных данных сотрудников МУП «Тепловые сети» на базе современных информационных технологий.

Сотрудник обязан:
-передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом.
-своевременно сообщать работодателю об изменении своих персональных данных.

Сотрудник имеет право на:
-полную информацию о своих персональных данных и обработке этих данных;
-свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника за исключением случаев, предусмотренных действующим законодательством Российской Федерации;
-доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;
-требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия.

4. Доступ к персональным данным работников

Персональные данные добровольно передаются сотрудником непосредственно держателю этих данных и потребителям внутри предприятия МУП «Тепловые сети» исключительно для обработки и использования в работе.
4.1.Внешний доступ. К числу массовых потребителей персональных данных вне предприятия МУП «Тепловые сети» можно отнести государственные и негосударственные функциональные структуры:
-налоговые инспекции;
-правоохранительные органы;
-органы статистики;
-страховые агентства;
-органы социального страхования;
-пенсионные фонды;
-подразделения муниципальных органов управления.
4.2. Внутренний доступ. Внутри предприятия МУП «Тепловые сети» к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:
-все сотрудники отдела кадров;
-все сотрудники бухгалтерии;
-руководители структурных подразделений.

В отделе кадров хранятся личные карточки сотрудников, работающих в настоящее время. Для этого используются специально оборудованные шкафы или сейфы, которые запираются. Личные карточки располагаются в алфавитном порядке по структурным подразделениям. После увольнения документы по личному составу хранятся в архиве предприятия.

5. Передача персональных данных

При передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

5.1. Передача внешнему потребителю.

• Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

• При передаче персональных данных сотрудника потребителям (в том числе и в коммерческих целях) за пределы МУП «Тепловые сети» работодатель не должен сообщать эти данные третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, или в случаях, установленных законодательством Российской Федерации.

• Ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения Директора предприятия и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений.

• Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

• Сведения передаются в письменной форме и должны иметь гриф конфиденциальности.

• По возможности персональные данные обезличиваются.

5.2. Передача внутреннему потребителю.

• Работодатель вправе разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, перечисленным в п. 2 гл. 4.

• Потребители персональных данных должны подписать обязательство о неразглашении персональных данных сотрудников (Приложение 1).

6. Защита персональных данных

6.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

6.2. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности предприятия.

1.«Внутренняя защита».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами предприятия. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками требований нормативно-методических документов по защите информации;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных карточек Т-2 сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочее место только директору предприятия;
- персональные компьютеры, на которых содержатся персональные данные, должны быть защищены паролями доступа.

2.«Внешняя защита».

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности предприятия, посетители, сотрудники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим предприятия;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Персональная ответственность — одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Каждый сотрудник предприятия, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

Начальник отдела кадров  Т. Л. Ерохина

Приложение

к Положению о защите персональных данных работников

от « ____ » _____ 20_ г.

Обязательство о неразглашении персональных данных сотрудников

Отдел кадров:

Бухгалтерия:

Отдел АСУ:

Руководители подразделений:

Юридический отдел:

~

лист
ознакомления с Положением о защите
персональных данных работников

№п/п	Фамилия, имя, отчество работника	Дата и подпись работника после ознакомления с Положением