"УТВЕРЖДАЮ"

Директор МУП «ВГЭС»

А.А.Ромашов

"08" 12 2011 г.

ПОЛОЖЕНИЕ МУП «ВГЭС»
об обработке и защите персональных данных

1. Общие положения

1.1. Настоящее положение принято в целях сохранения личной тайны и защиты персональных данных работников муниципального унитарного предприятия «Волгодонская городская электрическая сеть».

1.2. Положение определяет порядок обработки персональных данных на предприятии, права и обязанности руководителей и работников, а также порядок взаимодействия по поводу сбора, хранения, передачи и защиты персональных данных работников.

1.3. Настоящее положение разработано на основе и во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, положений главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работников», Кодекса об административных правонарушениях РФ, Гражданского кодекса Российской Федерации, Уголовного кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 25.07.2011) (далее – Закон), а также Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.4. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания.

1.5. Настоящее положение утверждается и вводится в действие приказом директора и является обязательным для исполнения всеми сотрудниками, уполномоченными на обработку персональных данных.

2. Понятие и состав персональных данных работников

2.1. Персональные данные работника – любая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся прямо или косвенно конкретного работника.

2.2. Персональные данные работника составляют:

1) сведения о фактах, событиях и обстоятельствах частной жизни работника, позволяющие идентифицировать его;

2) служебные сведения, а также иные сведения, связанные с профессиональной деятельностью работника, в том числе сведения о поощрениях и о дисциплинарных взысканиях.

2.3. Документами, содержащими персональные данные являются:

1) паспорт или иной документ, удостоверяющий личность;

2) трудовая книжка;

3) страховое свидетельство государственного пенсионного страхования;

4) свидетельство о постановке на учёт в налоговый орган и присвоения ИНН;

5) документы воинского учёта;

6) документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;

7) карточка Т-2;

8) автобиография;

9) личный листок по учёту кадров;

10) медицинское заключение о состоянии здоровья;

11) документы, содержащие сведения о заработной плате, доплатах и надбавках;

12) приказы о приёме лица на работу, об увольнении, а также о переводе лица на другую должность;

13) другие документы, содержащие сведения, предназначенные для использования в служебных целях.

3. Обработка персональных данных работников

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

Обработка персональных данных работника осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов, содействия работнику в трудоустройстве, обучении, продвижении по службе, обеспечения личной безопасности работника, контроля качества и количества выполняемой работы и обеспечения сохранности имущества, оплаты труда, пользования льготами, предусмотренными законодательством РФ и локальными актами предприятия.

3.2. Обработка персональных данных допускается только с письменного согласия работника на обработку его персональных данных. (Приложение 1)

Работник отдела кадров в соответствии с установленными должностными обязанностями:

- обеспечивает получение согласия на обработку персональных данных работника на срок действия заключённого с ним трудового договора;
- знакомит работника под подпись с содержанием настоящего Положения.

Заявления о согласии на обработку персональных данных и лист ознакомления работников с настоящим Положением хранится в отделе кадров.

3.3. Работник обязан сообщать в установленном порядке в отдел кадров об изменении ранее переданных персональных данных в срок не позднее 10 рабочих дней с момента произошедших изменений.

Изменения в документы, содержащие персональные данные, вносятся сотрудниками, уполномоченными на обработку персональных данных, на основании официальных документов, предоставляемых работником.

3.4. В случаях, когда необходимые персональные данные работника можно получить только у третьего лица, сотрудник, уполномоченный на обработку персональных данных, должен уведомить об этом работника и получить от него письменное согласие по установленной форме. (Приложение 2)

При этом необходимо сообщить работнику о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работника дать письменное согласие на их получение.

3.5. Обработка специальных категорий персональных данных работника касающихся расовой, национальной принадлежности, политических взглядов,

религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных Законом.

3.6. Обработке подлежат только те персональные данные, которые отвечают достижению конкретных, заранее определенных и законных целей их обработки.

При обработке персональных данных работника должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

3.7. При утверждении настоящего Положения, приказом директора назначается лицо, ответственное за организацию обработки персональных данных работников на предприятии.

Лицо, ответственное за организацию обработки персональных данных обязано:

1) осуществлять внутренний контроль за соблюдением работодателем и его работниками законодательства о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников положения законодательства о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать приём и обработку обращений и запросов о персональных данных и (или) осуществлять контроль за приёмом и обработкой таких обращений и запросов.

3.8. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных федеральными законами.

3.8.1. При передаче персональных данных работника должны соблюдаться следующие требования:

1) не предоставлять персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральными законами;

2) не предоставлять персональные данные работника в коммерческих целях без его письменного согласия;

3) предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

4) разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по предприятию, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

5) не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

6) предоставлять персональные данные работника представителям работников в порядке, установленном Трудовым кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.9.2. Передача персональных данных от сотрудников предприятия внешнему потребителю может допускаться в минимальных объёмах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

3.9.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника (Приложения 5, 6), за

исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных Законом.

3.10. Все меры конфиденциальности при сборе, обработке и хранении персональных данных работника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

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

3.12. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

3.13. При принятии решений, затрагивающих интересы работника, сотрудники предприятия не имеют права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. При этом необходимо учитывать личные качества работника, его добросовестный и эффективный труд.

4. Доступ к персональным данным работников

4.1. Внутренний доступ (доступ внутри предприятия).

4.1.1. Право доступа к персональным данным работника имеют:

- директор предприятия;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным работника может иметь руководитель нового подразделения;
- сам работник, носитель данных;
- другие работники предприятия при выполнении ими своих служебных обязанностей.

4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом директора предприятия. (Приложение 3)

4.1.3. Сотрудник, имеющий доступ к персональным данным работников в связи с исполнением своих трудовых обязанностей, обеспечивает хранение информации, содержащей персональные данные работника, исключающее доступ к ним третьих лиц.

Документы, содержащие персональные данные работников, хранятся в помещении отдела кадров и бухгалтерии где обеспечено наличие сигнализации. Доступ к электронным базам данных, содержащим персональные данные работников, обеспечивается системой паролей.

В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные работников (соблюдение "политики чистых столов").

При уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своём рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные работников лицу, на которое локальным актом (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей.

При увольнении сотрудника, имеющего доступ к персональным данным работников, документы и иные носители, содержащие персональные данные работников, передаются другому сотруднику, имеющему доступ к персональным данным работников по указанию руководителя структурного подразделения.

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне предприятия можно отнести государственные и негосударственные функциональные структуры:

- налоговые службы;
- правоохранительные органы;
- страховые агентства;

- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

4.2.2. Надзорно- контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного согласия.

4.2.4. Сведения о работающем или уже уволенном работнике могут быть предоставлены другой организации только по письменному запросу на фирменном бланке организации, с приложением копии заявления работника.

Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.

В случае развода бывшая супруга (супруг) имеют право обратиться с письменным запросом о размере заработной платы работника без его согласия. (Уголовный кодекс РФ).

5. Обеспечение безопасности персональных данных работников

5.1. Под угрозой безопасности персональных данных при их обработке понимается совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных.

5.2. Обеспечение безопасности персональных данных представляет собой технологический процесс предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий достаточно надёжную безопасность информации в процессе деятельности предприятия.

5.3. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена за счёт собственных средств предприятия.

5.4. «Внутренняя защита».

5.4.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, сотрудник, работающий с документами и базами данных. Регламентация доступа сотрудника к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами предприятия.

5.4.2. Для обеспечения внутренней безопасности персональных данных работников необходимо соблюдать ряд мер:

1) ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;

2) строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

3) рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;

4) знание и соблюдение сотрудником требований по защите информации и сохранении тайны персональных данных работников (Приложение 4);

5) наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

6) определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором производится работа с информационной системой персональных данных или хранение электронных баз данных персональных данных;

7) управление доступом пользователей к информационной системе персональных данных;

8) регистрация входа (выхода) пользователей информационной системы персональных данных;

9) учет всех защищаемых электронных носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

10) обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды;

11) физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

12) периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы;

13) организация порядка уничтожения персональных данных;

14) своевременное выявление нарушения требований разрешительной системы доступа сотрудниками;

15) воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты сведений при работе с конфиденциальными документами;

16) не допускается выдача личных дел сотрудников на рабочие места руководителей структурных подразделений. Личные дела могут выдаваться на рабочие места только директору, работникам отдела кадров и в исключительных случаях, по письменному разрешению директора, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

5.5. «Внешняя защита».

5.5.1. 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, подмена, фальсификация содержания реквизитов документа, заражение вирусным или вредоносным программным обеспечением и др.

5.5.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности предприятия, посетители, работники других структурных подразделений. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров.

5.5.3. Для обеспечения внешней защиты персональных данных работников необходимо соблюдать ряд мер:

1) порядок приёма, учёта и контроля деятельности посетителей;

2) технические средства охраны, сигнализации;

3) порядок охраны территории, зданий, помещений, транспортных средств;

4) требования к защите информации при интервьюировании и собеседованиях.

5.6. Все лица, связанные с обработкой персональных данных, согласно Перечню должностей, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия работника, если иное не предусмотрено Законом.

5.7. По возможности персональные данные обезличиваются.

6. Права и обязанности работника

6.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нём.

6.2. Работники и их представители должны быть ознакомлены под расписку с документами предприятия, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

6.3. В целях обеспечения безопасности персональных данных работник имеет право:

1) требовать уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

2) на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

3) определять своих представителей для защиты своих персональных данных;

4) на сохранение и защиту своей личной и семейной тайны.

6.4. Работник обязан:

1) передавать сотрудникам, уполномоченным на обработку персональных данных, комплекс необходимых, достоверных, документированных персональных данных;

2) своевременно, в срок не позднее 10 рабочих дней с момента произошедших изменений, сообщать новые персональные данные.

6.5. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

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

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

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие её, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

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

7.4. Каждый сотрудник предприятия, получающий для работы конфиденциальный документ, несёт единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Сотрудники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение сотрудником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера руководитель вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

7.5.2. Сотрудники, в обязанность которых входит ведение персональных данных работника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не

предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации, а также разглашение информации с ограниченным доступом – влечёт наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершённые лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с Уголовным кодексом Российской Федерации.

7.5.4. Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки его персональных данных, а также требований к защите персональных данных, установленных в соответствии с Законом, подлежит возмещению в соответствии с Гражданским кодексом Российской Федерации.

7.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

Составил:
Юрисконсульт
_____ М.А.Лобачева

Согласовано:
Начальник ПТЭО
_____ А.Н.Журба

Начальник ИВГ
_____ Д.Н.Полетавкин

Ст. инспектор ОК
_____ Н.А.Мусиец