Приложение №1
к Приказу №494/п
от «07» августа 2017 г.

ПОЛИТИКА

В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ОАО «ТЕПЛОЭНЕРГО»

Нижний Новгород, 2017г

Оглавление

1. Общие положения

1.1. Настоящая политика (далее – Политика) в отношении обработки и защиты персональных данных (далее – ПДн) определяет политику открытого акционерного общества «Теплоэнерго» (далее – Общество) в отношении обработки и обеспечения безопасности ПДн.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Обществе.

1.3. Положения Политики распространяются на отношения по обработке ПДн, полученных Обществом как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Политика обязательна для ознакомления и исполнения всеми лицами, допущенными к Обработке ПДн в информационных системах ПДн.

1.5. Политика разработана в соответствии с требованиями действующего законодательства Российской Федерации, в том числе с использованием следующих документов:

- Конституции Российской Федерации;
- Трудового кодекса Российской Федерации;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Иных нормативных правовых актов Российской Федерации, регулирующих вопросы обработки ПДн.

1.6.В Политике использованы следующие термины с соответствующими определениями:

Автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники;

Администратор информационной безопасности (АИБ) – должностное лицо, которое назначается приказом генерального директора Общества, наделенное определенными полномочиями и ответственностью, согласно инструкции и другим нормативным актам об администраторе информационной безопасности, для выполнения работ по обеспечению безопасности ПДн.

Блокирование - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

Информационная система ПДн (ИСПДн) - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

Обезличивание - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

Обработка ПДн/Обработка - любое действие (операция) или совокупность действий (операций), совершаемых с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (Распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

Ответственный за организацию обработки ПДн - должностное лицо, которое назначается приказом генерального директора Общества, организующее принятие правовых, организационных и технических мер в целях обеспечения надлежащего выполнения функций по организации обработки ПДн в Обществе в соответствии с положениями законодательства Российской Федерации в области ПДн;

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

Предоставление - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

Распространение - действия, направленные на раскрытие ПДн неопределенному кругу лиц;

Субъект ПДн - физическое лицо, прямо или косвенно определенное или определяемое на основании относящихся к нему ПДн;

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

2. Цели и состав персональных данных, обрабатываемых в Обществе

2.1. Цели обработки ПДн в Обществе:

Подбор соискателей, кадровое администрирование, обучение работников, осуществление воинского учета, установление доплат и надбавок, организация выпуска зарплатных карт, выдача зарплатных карт, расчет и выдача заработной платы, оформление договоров, сдача отчетности в Пенсионный фонд Российской Федерации, Федеральную налоговую службу Российской Федерации, учет налоговых льгот при начислении заработной платы, услуги теплоснабжения: заключение договоров с физическими и юридическими лицами, расчет и начисление оплаты за предоставленные услуги, уведомление потребителя, выдача справок потребителям, учет льгот и денежных компенсаций потребителей за предоставленные услуги в соответствии с законодательством РФ, прием платежей, контрольно-пропускной и внутри объектовый режим: оформление, выдача, пропусков для доступа на территорию Общества и их уничтожение и прочие цели в рамках законодательства Российской Федерации.

2.1.5. Охрана труда: исполнение обязанностей работодателя при возникновении несчастного случая и проведения медицинских осмотров.

2.3. Состав ПДн, обрабатываемых в Обществе:

- Адрес личной электронной почты (e-mail)
- Адрес места жительства
- Адрес по прописке и дата регистрации
- Владение иностранными языками и языками народов Российской Федерации
- Водительское удостоверение
- Выполняемая работа с начала трудовой деятельности (включая военную службу)
- Гражданство
- График работы
- Дата и место рождения
- Должностной оклад, часовая тарифная ставка
- Зарплатный счет
- ИНН
- Кадры видеосъемки

- Наличие или отсутствие судимости
- Номер избирательного участка
- Номер свидетельства пенсионного страхования
- Паспортные данные (серия, номер, кем и когда выдан, номер подразделения)
- Подразделение
- Пол
- Послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов)
- Прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения)
- Профессия/должность
- Сведение об имуществе (наличие личного автомобиля) и данных документа (ПТС, свидетельство о регистрации автомобиля)
- Сведения о воинском учете
- Сведения о допуске к работам (вид допуска, дата получения, срок действия)
- Сведения о доходах с предыдущего места работы
- Сведения о наградах, поощрениях
- Сведения о наличии/отсутствии дисквалификации
- Сведения о наличии/отсутствии инвалидности
- Сведения о начисленной заработной плате
- Сведения о планируемом отпуске (ежегодном оплачиваемом и дополнительном).
- Сведения о повышении квалификации (период, вид повышения квалификации, наименование образовательного учреждения, наименование документа, подтверждающего повышение квалификации, номер и серия документа)
- Сведения о профессиональной переподготовке (период, вид профессиональной переподготовки, наименование специальности, наименование документа, подтверждаемого профессиональную переподготовку, номер и серия документа)
- Сведения о прохождении медицинских осмотров (периодичность прохождения, дата последнего медосмотра, состояние здоровья)
- Сведения о составе семьи (степень родства, фамилии, имена, отчества, даты рождения близких родственников)
- Сведения о страховом стаже
- Сведения о трудовом стаже, сведения о трудовой деятельности, занимаемых должностях
- Сведения об образовании (когда и какие образовательные учреждения закончил(а); наименование документа об образовании; номер, серия документа об образовании, направление подготовки или специальность, квалификация по документу об образовании)
- Сведения об отпусках, командировках и других причинах отсутствия на работе (дата начала, дата окончания, количество дней, вид отсутствия)
- Семейное положение
- Система оплаты
- Состояние здоровья (по результатам предварительного и периодических медицинских осмотров)
- Табельный номер
- Телефонный номер (домашний/мобильный)
- Условия налоговых вычетов (личный вычет, вычеты на детей, имущественные, статус налогоплательщика, льготы как подвергшимся воздействию радиации)

- Фамилия, имя, отчество
- Фотографии

2.4. Кроме того, обработка ПДн в Обществе осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Общество выступает в качестве работодателя, и в связи с реализацией Обществом своих прав и обязанностей как юридического лица.

2.5. ПДн получаются и обрабатываются Обществом на основании федеральных законов и иных нормативных правовых актов Российской Федерации, а в необходимых случаях - при наличии письменного согласия субъекта ПДн.
2.6. В целях исполнения возложенных на Общество функций Общество в установленном порядке вправе поручить обработку ПДн третьим лицам. В договоры с лицами, которым Общество поручает обработку ПДн, включаются условия, обязывающие таких лиц соблюдать предусмотренные законодательством требования к обработке и защите ПДн.
2.7. Общество предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.
2.8. В Обществе не производится обработка ПДн, несовместимая с целями их обработки. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн уничтожаются.
2.9. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Общество принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

3. Принципы обеспечения безопасности и порядок обработки персональных данных

3.1. Целью обеспечения безопасности ПДн при их обработке в Обществе является предотвращение несанкционированного доступа и обеспечение целостности и доступности обрабатываемых ПДн.
3.2. Для обеспечения безопасности ПДн Общество руководствуется следующими принципами:

- системность: обработка ПДн в Обществе осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;
- комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Общества и других имеющихся в Обществе систем и средств защиты;
- непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Обществе с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

- минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования ИСПДн Общества, а также объема и состава обрабатываемых ПДн;
- специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;
- эффективность процедур отбора кадров: кадровая политика Общества предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;
- наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

3.3. Обработка ПДн осуществляется:
- с согласия субъекта ПДн на обработку его ПДн;
- в случаях, когда Обработка ПДн необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется Обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом ПДн).

4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым в Обществе ПДн имеют лица, уполномоченные приказом Общества, лица, которым Общество поручило обработку ПДн на основании заключенного договора или поручения, а также лица, чьи ПДн подлежат обработке.
4.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой определенной функции Общества закрепляются за соответствующими структурными подразделениями Общества. Доступ к ПДн, обрабатываемым в ходе реализации полномочий, закрепленных за конкретным структурным подразделением Общества, могут иметь только Работники этого структурного подразделения. Работники допускаются к ПДн, связанным с деятельностью другого структурного подразделения, только в части вопросов, касающихся структурного подразделения этих Работников.
4.3. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних документов Общества. Работники, допущенные к обработке ПДн, под роспись знакомятся с документами Общества, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.
4.4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Обществом, определяется в соответствии с законодательством и определяется внутренними документами Общества.

5. Реализуемые требования к защите персональных данных

5.1. Общество принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Законом о ПДн и принятыми в соответствии с ним нормативными правовыми

актами, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.
5.2. Состав указанных в пункте 5.1 Политики мер, включая их содержание и выбор средств защиты ПДн, определяется, а внутренние регулятивные документы об обработке и защите ПДн утверждаются (издаются) Обществом исходя из требований нормативных актов РФ в части защиты ПДн.
5.3. Обществом производится устранение выявленных нарушений законодательства об обработке и защите ПДн.
5.4. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше чем этого требуют цели обработки ПДн, если срок хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн.
5.5. Обществом осуществляется ознакомление работников Общества, непосредственно осуществляющих обработку ПДн, с положениями законодательства о ПДн, в том числе требованиями к защите ПДн, Политикой и иными внутренними регулятивными документами по вопросам обработки ПДн, и (или) обучение указанных работников по вопросам обработки и защиты ПДн.
5.6. При обработке ПДн с использованием средств автоматизации Обществом, в частности, применяются следующие меры:

- назначается Ответственный за организацию обработки ПДн, из числа Работников, которые получают указания непосредственно от генерального директора Общества и подотчетных ему работников;
- утверждаются (издаются) внутренние регулятивные документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;
- применяются технические меры и решения для защиты ПДн;
- осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн Закону о ПДн и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике и внутренним регулятивным документам Общества;
- проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Закона о ПДн, определяется соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение исполнения обязанностей, предусмотренных Законом о ПДн.

5.7. Обеспечение безопасности ПДн в Обществе при их обработке в ИСПДн достигается в Обществе, в частности, путем:

1) определения угроз безопасности ПДн. Тип актуальных угроз безопасности ПДн и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;

2) определения в установленном порядке состава и содержания мер по обеспечению безопасности ПДн, выбора средств защиты информации. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности Обществом могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности ПДн. В этом случае в ходе разработки системы защиты ПДн проводится обоснование применения компенсирующих мер для обеспечения безопасности ПДн;

3) применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших

процедуру оценки соответствия, когда применение таких средств необходимо для нейтрализации актуальных угроз. В Обществе, в том числе, осуществляются:

- оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;
- учет машинных носителей ПДн, обеспечение их сохранности;
- аудит и контроль с целью обнаружения фактов несанкционированного доступа к ПДн и принятие соответствующих мер;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к обрабатываемым ПДн, а также обеспечение регистрации и учета действий, совершаемых с ПДн;
- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- контроль принимаемых мер по обеспечению безопасности ПДн, уровня защищенности ИСПДн.

5.8. Обеспечение защиты ПДн в Обществе при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

1) обособления ПДн от иной информации;

2) недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо различны;

3) использования отдельных материальных носителей для обработки каждой категории ПДн;

4) соблюдения требований:

- к раздельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;
- уточнению ПДн;
- уничтожению или обезличиванию части ПДн;
- определению мест хранения носителей ПДн;
- использованию типовых форм документов, характер информации в которых предполагается или допускается включение в них ПДн;
- ведению журналов, содержащих ПДн, необходимых для выдачи однократных пропусков субъектам ПДн в занимаемые Обществом здания и помещения;
- хранению ПДн, в том числе к обеспечению раздельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

6. Права субъектов персональных данных

6.1 Права субъектов ПДн определяются в соответствии с гл. 3, Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

6.2 Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Обществом;
- правовые основания и цели обработки ПДн;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- иной информации в соответствии с Федеральным законом «О персональных данных».

6.3. Субъект ПДн имеет право требовать от Общества уточнения своих ПДн, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными либо не являются необходимыми для заявленной цели обработки.

6.4. Субъект ПДн имеет право обращаться с требованием о прекращении неправомерной обработки его ПДн.

6.5. Субъект ПДн имеет право отозвать свое согласие на обработку ПДн способом, указанным в согласии на обработку ПДн, или иным способом, предусмотренным действующим законодательством

7. Заключительные положения

7.1 Политика является внутренним документом Общества, она общедоступна и подлежит размещению на официальном сайте Общества.

7.2 Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите ПДн, но не реже одного раза в три года.

7.3 Контроль исполнения требований настоящей политики осуществляется ответственным за обеспечение безопасности ПДн Общества.

7.4 Ответственность должностных лиц Общества, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн, определяется в соответствии с законодательством Российской Федерации и внутренними документами Общества.