Открытое акционерное общество
«Межрегиональная распределительная сетевая компания Северо-Запада»

УТВЕРЖДЕНО
приказом
ОАО «МРСК Северо-Запада»
от «01» 04 2013 №171

Система менеджмента качества

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в ОАО «МРСК Северо-Запада»

Санкт-Петербург
2013

Содержание

1 Назначение и область применения

1.1 Положение об обработке и защите персональных данных в ОАО «МРСК Северо-Запада» (далее – Положение) определяет цели обработки персональных данных, устанавливает общие требования к обеспечению безопасности персональных данных, обрабатываемых в ОАО «МРСК Северо-Запада» (далее – Общество) с использованием средств автоматизации или без использования таких средств, и регламентирует отношения по использованию персональных данных работниками Общества и лицами (контрагентами), состоящими в гражданско-правовых отношениях с Обществом.

1.2 Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15.09.2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3 Действие настоящего Положения распространяется на исполнительный аппарат и филиалы ОАО «МРСК Северо-Запада» и обязательно для исполнения всеми работниками Общества.

1.4 Настоящее Положение должно быть доведено под роспись до каждого работника Общества, осуществляющего обработку персональных данных.

2 Нормативные ссылки

В настоящем Положении использованы ссылки на следующие нормативные документы:

Конституция Российской Федерации

Гражданский кодекс Российской Федерации

Трудовой кодекс Российской Федерации

Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»

Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных»

Постановление Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Постановление Правительства РФ от 15.09.2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

Порядок проведения классификации информационных систем персональных данных, утв. приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13.02.2008 г. №55/86/20

П р и м е ч а н и е - При пользовании настоящим Положением целесообразно проверить действие ссылочных документов в информационной системе общего пользования. Если ссылочный документ заменен (изменен), то при пользовании настоящим Положением следует руководствоваться замененным (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем Положении применены следующие термины с соответствующими определениями:

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

3.2 *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.

3.3 *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.

3.4 *Автоматизированная обработка персональных данных* – обработка персональных данных с помощью средств вычислительной техники.

3.5 *Распространение персональных данных* – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

3.6 *Предоставление персональных данных* – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

3.7 *Блокирование персональных данных* – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

3.8 *Уничтожение персональных данных* – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3.9 *Обезличивание персональных данных* – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

3.10 *Информационная система персональных данных* – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3.11 *Контрагент* – сторона гражданско-правового договора, которой обладатель информации, составляющей персональные данные, передал эту информацию.

4 Обозначения и сокращения

В настоящем Положении используются следующие обозначения и сокращения:

Общество – ОАО «МРСК Северо-Запада», включая исполнительный аппарат и филиалы;

ИСПДн – информационная система персональных данных;

Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных» – Федеральный закон №152-ФЗ.

5 Общие положения

5.1 Принципы обработки персональных данных

При обработке персональных данных необходимо соблюдать следующие принципы:

5.1.1 Обработка персональных данных должна осуществляться на законной и справедливой основе.

5.1.2 Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

5.1.4 Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5.1.5 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.

5.1.6 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. Должны приниматься необходимые меры по удалению или уточнению неполных или неточных данных.

5.1.7 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.

5.1.8 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 законодательством.

5.2 Способы обработки и перечень действий с персональными данными

5.2.1 Общество может осуществлять обработку персональных данных с использованием средств автоматизации, а также без использования таких средств.

5.2.2 Перечень действий с персональными данными, которые могут осуществляться Обществом при обработке персональных данных субъектов:

- сбор;
- запись;
- систематизация;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передача (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

5.3 Необходимость уведомления уполномоченного органа по защите прав субъектов персональных данных

5.3.1 Общество обязано уведомить уполномоченный орган по защите прав субъектов персональных данных об обработке персональных данных, согласно требованиям Федерального закона №152-ФЗ по установленной форме.

6 Категории и субъекты персональных данных, цели обработки

6.1 Категории субъектов персональных данных

6.1.1 Обществом может осуществляться обработка персональных данных следующих категорий субъектов персональных данных:

- работников, состоящих или состоявших в трудовых отношениях с Обществом (далее – работники), а также членов их семей и близких родственников;
- физических лиц (контрагентов), состоящих или состоявших в договорных и иных гражданско-правовых отношениях с Обществом, акционеров в том числе членов их семей и близких родственников;
- физических лиц (посетителей) для однократного пропуска на территорию, на которой находятся объекты Общества.

6.2 Категории обрабатываемых персональных данных

6.2.1 В Обществе выделяются следующие категории персональных данных:

- специальные категории персональных данных согласно Федеральному закону №152-ФЗ;
- персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к специальным категориям персональных данных;
- персональные данные, позволяющие идентифицировать субъекта персональных данных;
- обезличенные и/или общедоступные персональные данные.

6.2.2 Вышеуказанные категории персональных данных классифицированы Обществом с учетом степени тяжести последствий потери свойств безопасности персональных данных для субъекта персональных данных.

6.3 Цели обработки персональных данных

6.3.1 Обработка персональных данных работников Общества, а также членов их семей и близких родственников может осуществляться с целью:

- выполнения требований Трудового кодекса РФ, Налогового кодекса РФ, Устава Общества, а также на основании целей, определенных федеральным законодательством;
- оценки психологического состояния работников и выявления их профессиональной пригодности;
- контроля состояния здоровья работников для выполнения требований Трудового кодекса РФ в части охраны труда;
- создания информационно-справочной базы работников;
- обеспечения внутрипропускного режима на объекты Общества.

6.3.2 Обработка персональных данных физических лиц, состоящих или состоявших в договорных и иных гражданско-правовых отношениях с Обществом, акционеров в том числе членов их семей и близких родственников осуществляется с целью:

- выполнения заявок на технологическое присоединение энергопринимающих устройств потребителей электрической энергии;
- выполнения расчета оплаты за потребляемую электроэнергию;
- выполнения и контроля выполнения условий договоров, соглашений и иных видов гражданско-правовых отношений.

6.3.3 Обработка персональных данных физических лиц (посетителей) осуществляется с целью однократного пропуска на территорию, на которой находятся объекты Общества.

6.4 Объем и содержание персональных данных

6.4.1 Объем и содержание персональных данных работников Общества, а также членов их семей и близких родственников:

- фамилия, имя, отчество;

- дата рождения;
- место рождения;
- адрес регистрации;
- данные о паспорте гражданина РФ (серия, номер, кем и когда выдан, код подразделения);
- данные о заграничном паспорте гражданина РФ (серия, номер, кем и когда выдан, код подразделения);
- данные о водительском удостоверении;
- гражданство, национальность;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства обязательного пенсионного страхования;
- семейное положение;
- данные о состоянии здоровья;
- полис медицинского страхования (серия, номер, наименование страховой компании);
- данные об имуществе и обязательствах имущественного характера;
- данные об образовании, квалификации, профессии;
- данные о военной обязанности;
- данные о допуске к сведениям, составляющим государственную тайну;
- данные о наличии судимости;
- данные о наличии наград;
- контактная информация;
- табельный номер;
- почтовый адрес;
- информация о доходах работников;
- фотография;
- трудовая деятельность (период, место работы, должность);
- банковские реквизиты;
- иная информация, необходимая для достижения вышеуказанных целей обработки персональных данных.

6.4.2 Объем и содержание персональных данных физических лиц, состоящих или состоявших в договорных и иных гражданско-правовых отношениях с Обществом, акционеров и членов их семей и близких родственников:

- фамилия, имя, отчество;
- дата рождения;
- место рождения;
- адрес регистрации;
- данные о паспорте гражданина РФ (серия, номер, кем и когда выдан, код подразделения);
- гражданство;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства обязательного пенсионного страхования;
- данные об имуществе и обязательствах имущественного характера;
- данные об образовании, квалификации, профессии;
- контактная информация;
- почтовый адрес;
- информация об эмиссионных ценных бумагах;
- трудовая деятельность (период, место работы, должность);
- банковские реквизиты;
- иная информация, необходимая для достижения вышеуказанных целей обработки персональных данных.

6.4.3 Объем и содержание персональных данных физических лиц (посетителей) территории, на которой находятся объекты Общества:

- фамилия, имя, отчество;

- данные о паспорте гражданина РФ (серия, номер, кем и когда выдан, код подразделения);
- данные о водительском удостоверении.

6.5 Сроки обработки персональных данных

6.5.1 Сроки обработки персональных данных должны определяться в соответствии со сроками действия договоров с субъектами персональных данных, указанными в п. 6.1 настоящего Положения, законодательства Российской Федерации в области сроков хранения архивных документов, а также иными требованиями законодательства и нормативными документами Министерства энергетики.

6.6 Условия обработки персональных данных

6.6.1 Обработка персональных данных допускается в следующих случаях:

- обработка персональных данных осуществляется с письменного согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора 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;
- обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 г. №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;
- 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 оператора 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 необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законодательством.

6.7 Права субъекта персональных данных

6.7.1 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые способы обработки персональных данных;
- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законодательством Российской Федерации;

- иные сведения, предусмотренные федеральным законодательством Российской Федерации в области обработки и защиты персональных данных.

6.7.2 Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

7 Условия и порядок обработки персональных данных

7.1 Назначение ответственных лиц

7.1.1 В Обществе приказом Генерального директора назначается лицо, ответственное за организацию защиты персональных данных как в информационных системах Общества, в которых обрабатываются персональные данные, так и при обработке без использования средств автоматизации (далее – Ответственный за организацию защиты персональных данных).

7.1.2 Ответственный за организацию защиты персональных данных, в частности обязан:

- осуществлять внутренний контроль, за соблюдением Обществом, как оператором персональных данных, а также его работниками, законодательства РФ о персональных данных, в том числе требований к защите персональных данных;

- доводить до сведения работников Общества положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- организовывать мероприятия, направленные на обеспечение безопасности обрабатываемых персональных данных.

7.1.3 На время отсутствия Ответственного за организацию защиту персональных данных его обязанности исполняет замещающий его работник.

7.1.4 Контроль выполнения установленных требований по информационной безопасности при обработке персональных данных, а также непосредственное участие в мероприятиях по защите информационных систем персональных данных в исполнительном аппарате и филиалах Общества осуществляют администраторы безопасности информационных систем персональных данных из числа работников подразделений безопасности Общества.

7.1.5 Ответственность за администрирование баз данных, общесистемного и прикладного программного обеспечения, входящего в состав информационных систем персональных данных, возлагается на специально назначенных приказами администраторов информационных систем персональных данных из числа работников подразделений информационных технологий Общества.

7.1.6 Ответственными за обработку персональных данных в подразделениях, работники которых в соответствии со своими должностными обязанностями уполномочены обрабатывать персональные данные, являются руководители этих подразделений. На время отсутствия этих руководителей ответственными являются замещающие их лица. В компетенцию ответственных за обработку персональных данных входит:

- организация и обеспечение выполнения требований локальных актов при обработке персональных данных работниками подразделений Общества;

- организация приема и обработки обращений и запросов субъектов персональных данных или их представителей, осуществление контроля за приемом и обработкой таких обращений и запросов.

7.1.7 Ответственными за выполнение требований локальных актов Общества по вопросам обработки персональных данных и их защите на своих рабочих местах в рамках определенных соответствующими должностными инструкциями полномочий являются лица, уполномоченные обрабатывать в Обществе персональные данные.

7.1.8 Ответственными за организацию выполнения требований локальных актов Общества по вопросам обработки персональных данных и их защите в филиалах Общества являются руководители филиалов. На время отсутствия этих руководителей ответственными являются замещающие их лица.

7.2 Порядок допуска до обработки персональных данных

7.2.1 Допуск работников Общества до обработки персональных данных осуществляется на основании списка допущенных до обработки персональных данных. Внесение изменений в данный список осуществляется на основании соответствующего приказа Общества, инициатором которого выступают ответственные за обработку персональных данных.

7.2.2 Лица, уполномоченные обрабатывать в Обществе персональные данные, как с использованием средств автоматизации, так и без использования таковых, должны быть ознакомлены с настоящим Положением, законодательством РФ о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами Общества по обработке и защите персональных данных. Для этого разрабатывается соответствующий материал для обучения работников и далее проводится, в установленном порядке, их инструктаж.

7.2.3 С работниками, непосредственно осуществляющими обработку персональных данных, должны быть, в установленном порядке, оформлены обязательства о выполнении требований локальных актов Общества по обработке, защите и неразглашении сведений конфиденциального характера (в том числе персональных данных) (далее – Обязательство), а также в трудовых договорах и должностных инструкциях этих работников должны быть прописаны основные принципы работы с персональными данными.

Эти лица предупреждаются о том, что обрабатываемые ими персональные данные могут быть использованы лишь в целях, установленных законодательством РФ и локальными актами Общества, и они имеют право доступа только к тем персональным данным, обработка которых предусмотрена их должностными обязанностями.

7.2.4 Обязательство подлежит оформлению со всеми лицами, уполномоченными в Обществе обрабатывать персональные данные.

7.2.5 Ознакомление с фактом предстоящей обработки персональных данных, а также с документами по вопросам обработки и защиты персональных данных в Обществе производится при оформлении трудовых отношений физического лица с Обществом под роспись и является приложением к трудовому договору.

7.2.6 Ответственным за организацию и выполнение процедуры ознакомления является работник структурного подразделения Общества, уполномоченный на оформление трудовых отношений.

7.3 Порядок получения персональных данных

7.3.1 Персональные данные работников и контрагентов предоставляются субъектом персональных данных лично.

7.3.2 В случае, когда персональные данные возможно получить только у третьей стороны, субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

7.3.3 Субъект персональных данных обязан предоставлять Обществу достоверную персональную информацию. При изменении персональных данных должен письменно уведомить об этом Общество в срок, не превышающий 7 (семи) дней.

7.3.4 Общество имеет право запрашивать у субъекта персональных данных дополнительные сведения и документы, подтверждающие их достоверность.

7.3.5 Общество не имеет права получать и обрабатывать персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских

убеждений, состояния здоровья, интимной жизни субъекта персональных данных, за исключением следующих случаев:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных.

7.4 Порядок хранения и уничтожения персональных данных

7.4.1 Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

7.4.2 Общество должно прекратить обработку персональных данных и уничтожить собранные персональные данные, если иное не установлено законодательством РФ, в следующих случаях и в сроки, установленные законодательством РФ:

- по достижению целей обработки или при утрате необходимости в их достижении;
- по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных – если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такое согласие требуется в соответствии с законодательством РФ;
- при невозможности устранения допущенных нарушений при обработке персональных данных.

7.5 Порядок передачи персональных данных

7.5.1 Общество обязуется не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ.

7.5.2 Передача персональных данных работников, а также членов их семей и контрагентов в пределах Общества осуществляется в соответствии с должностными инструкциями и локальными нормативными актами Общества.

7.5.3 Работники Общества, в обязанности которых входит работа с персональными данными работников и контрагентов обеспечивают защиту персональных данных от несанкционированного доступа и копирования.

7.5.4 Передача персональных данных субъектов разрешена только специально уполномоченным лицам и организациям, при этом указанные лица и организации должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

7.5.5 Общество имеет право передавать персональные данные субъекта его законным, полномочным представителям в порядке, установленном законодательством РФ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции и достижения определенной цели.

7.5.6 Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и/или применения технических средств, если иное не регламентировано соответствующими нормативно-методическими и организационно-распорядительными документами в Обществе.

7.5.7 Подключение информационной системы к информационной системе другого класса или к информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) осуществляется с использованием межсетевых экранов.

7.5.8 Передача бумажных документов, содержащих персональные данные, осуществляется курьерской службой или заказным отправлением. При отправлении пакетов с грифом «Персональные данные» через почтовое отделение связи, курьерскую службу их целесообразно

помещать в другие конверты, на которые наносятся только реквизиты, предусмотренные почтовыми правилами для открытых заказных отправлений.

8 Мероприятия по обеспечению безопасности персональных данных

8.1 Мероприятия по обеспечению безопасности персональных данных при автоматизированной обработке

8.1.1 Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

8.1.2 Безопасность персональных данных при их обработке в информационных системах персональных данных обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, прошедшие в установленном порядке процедуру соответствия, а также используемые в информационных системах персональных данных информационные технологии.

8.1.3 На всех автоматизированных рабочих местах и серверах, где осуществляется обработка персональных данных, должны быть установлены средства защиты информации от несанкционированного доступа, а также антивирусное программное обеспечение.

8.1.4 Все информационные системы персональных данных Общества подлежат обязательной классификации.

8.1.5 Классификация информационных систем персональных данных проводится комиссией, назначенной приказом Генерального директора Общества.

8.1.6 Классификация информационных систем персональных данных должна осуществляться Обществом в соответствии с порядком проведения классификации информационных систем персональных данных.

8.1.7 Результаты классификации информационных систем персональных данных должны быть оформлены соответствующим актом.

8.1.8 Для каждой информационной системы персональных данных должны быть определены:

- цель обработки персональных данных;
- объем и содержание обрабатываемых персональных данных;
- перечень действий с персональными данными и способы их обработки.

8.1.9 Объем и содержание персональных данных, а также перечень действий и способы обработки персональных данных должны соответствовать целям обработки. Если нет необходимости в обработке определенных персональных данных, эти персональные данные должны быть удалены.

8.1.10 Размещение информационных систем персональных данных, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

8.1.11 Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает администратор безопасности ИСПДн. Обязанность администратора безопасности ИСПДн обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе персональных данных.

8.1.12 Данные о работе с электронными носителями информации регистрируются в соответствующих журналах работы с электронными носителями информации, составляющей персональные данные согласно приложению 1. Ответственность за надлежащее ведение журналов

возлагается на соответствующих работников структурных подразделений, отвечающих за обработку персональных данных.

8.1.13 Лица, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка работников, допущенных до обработки персональных данных в Обществе.

8.1.14 Устанавливаются правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивается регистрация и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется уполномоченными работниками Общества, администратором ИСПДн и администратором безопасности ИСПДн.

8.1.15 Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных осуществляется администратором безопасности ИСПДн.

8.1.16 При обнаружении нарушений порядка предоставления персональных данных администратор ИСПДн и администратор безопасности ИСПДн незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин. Обо всех инцидентах информационной безопасности в ИСПДн сообщается ответственному за обработку персональных данных соответствующего структурного подразделения и Ответственному за организацию защиты персональных данных.

8.2 Мероприятия по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации

8.2.1 При обработке в Обществе персональных данных на бумажных носителях, в частности, при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться требования, установленные Постановлением Правительства РФ №687.

8.2.2 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждого материального носителя персональных данных можно было определить места хранения материальных носителей персональных данных и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

8.2.3 Необходимо обеспечивать раздельное хранение персональных данных, обработка которых осуществляется в различных целях, при этом документы содержащие персональные данные группируются в дела отдельно от документов открытого характера.

8.2.4 При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

8.2.5 Приказом Генерального директора Общества утверждается перечень мест хранения персональных данных, обрабатываемых без использования средств автоматизации. Инициаторами данного приказа выступают ответственные за организацию обработки персональных данных.

8.2.6 Допускается передача материальных носителей персональных данных на хранение сторонней организации на основании договора, при этом, существенным условием договора является обязанность обеспечения указанной организацией конфиденциальности персональных данных и безопасности персональных данных при их обработке и хранении.

8.2.7 Работники Общества, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств

автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

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

- типовая форма должна содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя 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 его 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.

8.2.9 Материальные носители персональных данных, по достижении целей обработки содержащихся на них персональных данных, подлежат уничтожению, если иное не предусмотрено законодательством РФ (полное физическое и не восстановимое уничтожение материальных носителей персональных данных). Работник, у которого находятся материальные носители персональных данных, подлежащие уничтожению, инициирует комиссионное уничтожение таких носителей с обязательным присутствием уполномоченных работников подразделений безопасности и делопроизводства Общества.

8.2.10 Данные о работе с бумажными носителями информации регистрируются в электронной базе подразделения делопроизводства. Ответственность за ведение данной базы возлагается приказом Генерального директора Общества на заместителя генерального директора по соответствующему направлению деятельности.

8.3 Порядок работы с материальными носителями информации, содержащими персональные данные

8.3.1 Порядок учета материальных носителей информации, содержащей персональные данные (далее – носители информации):

8.3.1.1 На бумажные носители информации наносятся следующие реквизиты:

- Гриф «Персональные данные» проставляется исполнителем в правом верхнем углу бланка документа.

Пример:

Персональные данные Экз. №_____

- На оборотной стороне последнего листа каждого экземпляра документа в левом нижнем углу проставляется учетный номер, количество отпечатанных экземпляров, учетный номер носителя, с которого печатался документ, фамилия и инициалы исполнителя, его телефон и дата подготовки документа.

Пример:
Уч. №60-01/123пдн
Отп. 1 экз.
Отп. с НЖМД №123
Исп. и отп. Иванов И.И.
(812) 569-30-77
23.04.2012

8.3.1.2 Порядок нанесения реквизитов на бумажные носители информации, содержащие персональные данные:

а) При создании документа на компьютере:

1) исполнителем создается гриф в электронном документе;

2) при распечатке созданного документа – исполнителем печатается, с помощью принтера, учетный номер;

3) документ регистрируется в подразделении делопроизводства.

б) При получении документов в бумажном виде от субъекта персональных данных:

1) документ регистрируется в подразделении делопроизводства;

2) гриф и учетный номер проставляются с помощью печатей.

в) При получении документов в электронном виде от субъекта персональных данных:

1) полученный электронный документ распечатывается;

2) документ регистрируется в подразделении делопроизводства при этом гриф и учетный номер проставляются с помощью печатей.

г) При получении документов в электронном или бумажном виде от контрагента без грифа, указывающего наличие в данном документе персональных данных, вне зависимости от содержания документа, подразделением делопроизводства осуществляется учет и регистрация таких документов в том же порядке, что и общие документы.

8.3.1.3 На электронные носители информации, администраторами ИСПДн, наносятся следующие реквизиты:

- накопители на жестких магнитных дисках (далее – НЖМД) – НЖМД №__;
- флеш-накопители – ФН №__.

8.3.1.4 Материальные носители информации регистрируются администраторами ИСПДн в Журнале регистрации и учета электронных носителей информации, составляющей персональные данные по форме согласно приложению 2.

8.3.2 Порядок хранения носителей информации:

8.3.2.1 Хранение носителей информации разрешается только в сейфах или запираемых шкафах.

8.3.2.2 Бумажные носители информации с грифом «Персональные данные» запрещается выносить из служебных помещений для работы с ними за пределами территории Общества, если иное не регламентировано указанием Генерального директора Общества.

8.3.2.3 Срок хранения носителей информации определяется в соответствии с номенклатурой дел и законодательством РФ;

8.3.2.4 При работе с бумажными носителями информации, в целях исключения их хищения и ограничения доступа к ним посторонних лиц, работники обязаны не оставлять документы без присмотра и при выходе из кабинета – запирать их в сейф (запираемый шкаф).

8.3.2.5 При обращении с электронными носителями информации запрещается:

- снимать несанкционированные копии с электронных носителей информации;
- оставлять электронные носители без присмотра;
- записывать на электронные носители данные, не связанные с информацией, содержащей персональные данные;

- подключать к персональным электронно-вычислительным машинам (далее – ПЭВМ) дополнительные устройства и соединители без соответствующего предписания на возможность их совместного использования;

- оставлять не заблокированной ПЭВМ, при отсутствии визуального контроля за ней;

- вносить какие-либо изменения в программное обеспечение ПЭВМ;

- несанкционированно устанавливать, создавать и выполнять на ПЭВМ посторонние программы;

- осуществлять несанкционированное вскрытие системных блоков ПЭВМ;

- совершать иные действия, противоречащие Политике в области использования вычислительной техники и телекоммуникационных ресурсов Общества.

8.3.2.7 Ответственность в структурных подразделениях за надлежащее использование и хранение материальных носителей информации, содержащих персональные данные, возлагается на ответственных за обработку персональных данных, согласно пункту 7.1.6 настоящего Положения.

8.3.3 Порядок уничтожения носителей информации:

8.3.3.1 Носители информации, утратившие практическую ценность или сроки хранения которых истекли, подлежат уничтожению или стиранию.

8.3.3.2 Бумажные носители информации уничтожаются путем механического измельчения, сжигания химическим или термальным способом.

8.3.3.3 Уничтожение электронных носителей информации производится с помощью специальных аппаратных средств, либо любого другого способа надежного и гарантированного уничтожения. Перед уничтожением электронного носителя информации с него должна быть удалена информация, составляющая персональные данные, с помощью специальных программных или аппаратных средств.

8.3.3.4 О стирании информации, составляющей персональные данные на материальных носителях, а также об уничтожении самих носителей составляются соответствующие акты, которые подписываются:

- начальником подразделения безопасности;

- начальником подразделения информационных технологий;

- администратором безопасности ИСПДн;

- администратором ИСПДн;

- ответственным работником.

8.3.3.5 Акты утверждаются заместителем генерального директора по безопасности.

8.3.3.6 В журнале учета носителей информации делается отметка об уничтожении и/или стирании, с указанием даты и номера акта.

8.4 Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации ИСПДн

8.4.1 Технические меры:

8.4.1.1 К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы жизнеобеспечения;

- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных;

- системы контроля физического доступа.

8.4.1.2 Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;

- системы вентиляции и кондиционирования;

- системы резервного питания.

8.4.1.3 Все помещения Общества, в которых размещаются элементы ИСПДн и средства защиты должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

8.4.1.4 Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

8.4.1.5 Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т.д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

8.4.1.6 К системам обеспечения отказоустойчивости относятся:

- кластеризация;
- технология избыточных массивов независимых жёстких дисков (далее – RAID).

8.4.1.7 Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

8.4.1.8 Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на электронном носителе (НЖМД и т.п.).

8.4.2 Организационные меры:

8.4.2.1 Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже 1 (одного) раза в неделю;
- для технологической информации – не реже 1 (одного) раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже 1 (одного) раза в 3 (три) месяца, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

8.4.2.2 Данные о проведении процедуры резервного копирования, должны отражаться в специально созданном журнале учета. Ответственным за ведение данного журнала является администратор ИСПДн.

8.4.2.3 Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

Носители должны храниться не менее 1 (одного) года, для возможности восстановления данных.

9 Ответственность работников, допущенных до обработки персональных данных

9.1 Лица, нарушающие или не исполняющие требования настоящего Положения, привлекаются к дисциплинарной, административной или уголовной ответственности в соответствии с законодательством РФ.

9.2 Работодатель имеет право обратиться в суд для привлечения к ответственности работника, причинившего ущерб Обществу путем разглашения информации, содержащей персональные данные.

10 Контроль за обработкой персональных данных

10.1 Контроль за обработкой персональных данных в Обществе осуществляет Ответственный за организацию защиты персональных данных.

10.2 При выявлении нарушений настоящего Положения, действующих локальных нормативных актов или федерального законодательства в области обработки и защиты персональных данных об этом немедленно следует сообщить ответственному за обработку персональных данных, либо Ответственному за защиту персональных данных в Обществе.

Должность	Подпись, дата	Ф.И.О.
РАЗРАБОТЧИК:		
Главный специалист сектора защиты информации департамента безопасности		Голубев А.А.
СОГЛАСОВАНО:		
Начальник департамента безопасности		Горбунов А.В.
Начальник департамента информационных технологий		Алексеев Е.Г.
Начальник департамента правового обеспечения	26.12.12	Горбунова Н.В.
Начальник отдела менеджмента качества управления менеджмента качества	27.12.2012 Мясников М.А.	Большаков И.А.

Приложение 1
(обязательное)

Форма журнала работы с электронными носителями информации, составляющей персональные данные

Открытое акционерное общество
«Межрегиональная распределительная сетевая компания Северо-Запада»

ЖУРНАЛ

работы с электронными носителями информации, составляющей персональные данные

Санкт-Петербург,
20__ г.

ЖУРНАЛ
работы с электронными носителями информации, составляющей персональные данные

_____ на _____ год

(наименование подразделения)

№ п/п	Регистрационный номер	Начало работы с носителем (время, дата)	Ф.И.О. работника	Подпись работника	Окончание работы с носителем (время, дата)	Ф.И.О. работника	Подпись работника	Примечание
1	2	3	4	5	6	7	8	9

Приложение 2
(обязательное)

Форма журнала регистрации и учета электронных носителей информации, составляющей персональные данные

Открытое акционерное общество
«Межрегиональная распределительная сетевая компания Северо-Запада»

ЖУРНАЛ

регистрации и учета электронных носителей информации, составляющей персональные данные

Санкт-Петербург,
20__ г.

ЖУРНАЛ
регистрации и учета электронных носителей информации, составляющей персональные данные

_____ на _____ год

(наименование подразделения)

№ п/п	Регистрационный номер	Серийный номер	Местонахождение (структурное подразделение)	Название ИСПДн	Отметка о постановке на учет (Ф.И.О., подпись, дата)
1	2	3	4	5	6

Отметка о снятии с учета (Ф.И.О., подпись, дата)	Сведения о стирании носителя информации (дата, № акта)	Сведения об уничтожении/выводе из эксплуатации носителя информации (дата, № акта)	Подпись администратора безопасности ИСПДн	Примечание
7	8	9	10	11