Стандарт предприятия

Защита персональных данных

УТВЕРЖДАЮ
Генеральный директор
АО «Волгаэнергосбыт»
_____А.Г. Рачковский

Приказ № ВЭС-П-26-150 от 06.05.2026 г.

Наименование подразделения - разработчика: управление

Содержание

Введение

Настоящий стандарт предприятия (СТП) разработан для описания принципов, правил и иных вопросов обработки персональных данных в АО «Волгаэнергосбыт» (далее – Общество) в соответствии с нормами действующего законодательства Российской Федерации, в том числе Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных», Федеральным законом «Об информации, информационных технологиях и о защите информации».

1. Область применения

1.1. Настоящий стандарт устанавливает основные правила и условия обработки персональных данных, задачи, функции и права подразделений и ответственных лиц, в обязанности которых входит проведение мероприятий по организации работы с персональными данными, общие требования к обеспечению безопасности персональных данных, обрабатываемых с использованием средств автоматизации или без использования таких средств.

1.2. Настоящий стандарт распространяется на все структурные подразделения Общества. Работники Общества, осуществляющие обработку персональных данных, должны быть ознакомлены с настоящим стандартом.

1.3. Настоящий стандарт входит в состав нормативных документов системы управления Общества.

1.4. Участниками бизнес-процесса являются: структурные подразделения Общества и организации, осуществляющие функции: организации мероприятий по защите персональных данных, ИТ обеспечения, контроля обеспечения ИБ, руководители и работники структурных подразделений Общества.

2. Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие документы:

- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);
- Постановление Правительства Российский Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российский Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- СТП «Политика в области информационной безопасности»;
- СТП «Система управления информационной безопасностью»;
- СТП «Управление доступом к информационным ресурсам ИС»;
- СТП «Аудит информационной безопасности»;
- Локальные нормативные акты Общества по вопросам обработки и защиты персональных данных.

3. Определения и сокращения

В настоящем стандарте используются следующие сокращения и определения:

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

персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для

распространения в порядке, предусмотренном Федеральным законом «О персональных данных»;

биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных *(в частности, к биометрическим данным относится цветное цифровое фотографическое изображение лица владельца заграничного паспорта гражданина РФ, соответствующее ГОСТ Р ИСО/МЭК 19794-5-2013, дактилоскопические данные, данные радужной оболочки глаза, данные сетчатки глаза, генетическая информация, геометрия лица, геометрия руки/ладони, данные о голосе);*

специальные персональные данные - данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта персональных данных;

субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;

оператор персональных данных, 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;

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), блокирование, удаление, уничтожение персональных данных;

сбор персональных данных - действия, направленные на получение персональных данных о субъекте (субъектах) персональных данных;

запись персональных данных - фиксация персональных данных на каком-либо носителе ручным или машинным способом

накопление персональных данных - действия, направленные на сохранение персональных данных без их изменения;

систематизация персональных данных - расположение персональных данных в порядке, облегчающем их обработку;

хранение персональных данных - комплекс реализуемых оператором мер, направленных на обеспечение сохранности и защищенности информации, при помощи которой можно осуществить идентификацию того или иного физического лица;

уточнение персональных данных - обновление или изменение персональных данных для обеспечения их достоверности и актуальности;

извлечение персональных данных - обработка, предполагающая выявление из общего массива информационной системы (базы данных) конкретных персональных данных в соответствии с заданными критериями, с последующим их переносом на другой информационный носитель любым способом и в любой форме или без такого переноса;

использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

передача персональных данных - вид обработки персональных данных, в результате которой доступ к ним получает третье лицо (третьи лица);

предоставление персональных данных - действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц;

доступ к персональным данным - возможность получения и использования персональных данных;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (например, размещение

персональных данных на общедоступном ресурсе, включая Доски почета в общедоступных местах);

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

удаление персональных данных - процесс изъятия персональных данных из информационных систем с возможностью последующего восстановления;

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;

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека;

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу; передача персональных данных в подразделение (филиал) российского юридического лица, находящегося на территории иностранного государства, трансграничной передачей персональных данных не является;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их раскрытия и распространения без согласия субъекта персональных данных или наличия иного законного основания;

целостность персональных данных – способность средства вычислительной техники или информационной системы обеспечивать неизменность персональных данных в условиях случайного и/или преднамеренного их искажения (разрушения).;

общедоступные источники персональных данных - источники данных, в которые с письменного согласия субъекта персональных данных могут включаться персональные данные, сообщаемые субъектом персональных данных. Общедоступный источник персональных данных содержит заранее определенную администратором, преимущественно контактную или иную справочную информацию о соответствующем субъекте персональных данных;

общедоступные персональные данные - персональные данные, размещенные в общедоступных источниках персональных данных, с письменного согласия субъекта персональных данных;

Общество – Акционерное Общество «Волгаэнергосбы» (АО «Волгаэнергосбыт»);

Группа компаний ЭН+ /Группа ЭН+ – совокупность юридических лиц, связанных отношениями экономической и/или корпоративной зависимости;

безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств; информационная система персональных данных включает в себя базы данных, АРМ, каналы связи, сетевое оборудование, сервера, средства защиты информации, пользователей информационных систем, используемое программное обеспечение и т.п.

пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения);

базовый корпоративный перечень ИСПДн – утвержденный приказом по Группе компаний ЭН+ перечень информационных систем персональных данных, используемых компаниями Группы ЭН+;

уполномоченный орган по защите прав субъектов персональных данных – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, Роскомнадзор;

ООО «ЭН+ ДИДЖИТАЛ» – организация, осуществляющая функции ИТ обеспечения по договору оказания услуг.

АРМ – автоматизированное рабочее место;

ИБ – информационная безопасность;

ИСПДн – информационная система персональных данных;

ПДн – персональные данные.

Департамент ПДн – Департамент мониторинга и защиты персональных данных АО «ЭН+ ГЕНЕРАЦИЯ».

4. Общие положения

4.1. Принципы обработки персональных данных

Обработка персональных данных осуществляется Обществом в соответствии со следующими принципами:

4.1.1. обработка персональных данных осуществляется на законной и справедливой основе;

4.1.2. обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей; не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

4.1.3. не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

4.1.4. обработке подлежат только персональные данные, которые отвечают целям их обработки;

4.1.5. содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки; обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;

4.1.6. при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Общество принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;

4.1.7. хранение персональных данных осуществляется 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; обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.2. Условия обработки персональных данных

4.2.1. Обработка специальных категорий персональных данных осуществляется Обществом с соблюдением следующих условий:

субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

обработка персональных данных осуществляется в иных случаях, предусмотренных Федеральным законом «О персональных данных».

4.2.2. Общество не обрабатывает биометрические персональные данные.

4.2.3. Обработка иных категорий персональных данных осуществляется Обществом с соблюдением следующих условий:

обработка персональных данных осуществляется с 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 Общество функций, полномочий и обязанностей;

обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

обработка персональных данных необходима для 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 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. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных;

обработка персональных данных необходима для осуществления прав и законных интересов Общества или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.3. Способы обработки и перечень действий с персональными данными

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

4.3.2. 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), блокирование, удаление, уничтожение.

4.4. Конфиденциальность персональных данных

4.4.1. Сотрудники Общества, получившие доступ к персональным данным, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

4.4.2. Сотрудники Общества, получившие доступ к персональным данным, подписывают обязательство о неразглашении персональных данных, ставших им известными при выполнении должностных обязанностей.

5. Субъекты и категории персональных данных, цели обработки

5.1. Категории субъектов персональных данных

В Обществе может осуществляться обработка персональных данных следующих категорий субъектов персональных данных:

- работники
- близкие родственники работников
- уволенные работники
- родственники уволенных работников
- представители контрагентов
- выгодоприобретатели по договорам
- практиканты
- представители контрагентов
- посетители сайта
- граждане, заполнившие на сайте форму обратной связи
- соискатели
- физические лица, ПДн которых необходимы для организации пропускного режима

- контрагенты
- потребители
- законные представители граждан, персональные данные которых необходимы для осуществления возложенных функций, полномочий и обязанностей
- представители потребителей

5.2. Категории персональных данных субъектов персональных данных

5.2.1. В соответствии с Федеральным законом «О персональных данных» в Обществе выделяются следующие категории персональных данных:

– персональные данные, отнесенные к специальным категориям персональных данных;

– персональные данные, которые не могут быть отнесены к вышеуказанным категориям персональных данных (иные).

5.2.2. В информационных системах Общества обработка персональных данных, относящихся к специальным категориям персональных данных, может осуществляться при соблюдении условий, предусмотренных Федеральным законом «О персональных данных» и настоящим СТП.

5.3. Цели обработки персональных данных

5.3.1. В Обществе определены следующие базовые цели обработки персональных данных:

– ведение кадрового учета и расчетов с персоналом;
– обеспечение соблюдения трудового законодательства РФ;
– обеспечение соблюдения пенсионного законодательства РФ;
– обеспечение соблюдения страхового законодательства РФ;
– обеспечение соблюдения налогового законодательства РФ;
– обеспечение соблюдения законодательства РФ об исполнительном производстве;
– обеспечение соблюдения требований законодательства в области охраны труда;
– подготовка, заключение и исполнение гражданско-правового договора с физическим лицом;
– ведение официального сайта организации, предоставление посетителю сайта информации об организации и оказываемых услугах;
– подбор персонала (соискателей) на вакантные должности оператора;
– обеспечение прохождения ознакомительной, производственной или преддипломной практики на основании договора с учебным заведением;
– обеспечение пропускного режима на территорию оператора;
– реализация программы добровольного медицинского страхования;
– ведение документооборота;
– ведение договорной работы (кроме ГПХ);
– организация санаторно-курортного лечения и детских оздоровительных лагерей;
– реализация программ обучения персонала;
– сопровождение управленческих процессов;
– ведение бухгалтерского и управленческого учета;
– оценка качества оказываемых услуг клиентами компании;
– обеспечение соблюдения корпоративной этики;
– обеспечение соблюдения законодательства в области защиты персональных данных;
– контроль учета рабочего времени;
– формирование сводной отчетности по направлениям деятельности;
– организация командировок;
– рассмотрение обращений граждан, подготовка ответов на обращения;
– оценка по 9 боксам;
– осуществление псих.проверок/псих.тестирования;
– исполнение обязательств в рамках оказания услуг в сфере жилищно-коммунального хозяйства и энергетики (исполнение требований жилищного законодательства Российской Федерации, законодательства Российской Федерации в области электроэнергетики, теплоснабжения, водоснабжения и водоотведения) заключение, сопровождение, расторжение договоров ресурсоснабжения и поставки коммунальных услуг

(теплоснабжения, электроснабжения, горячего-, холодного водоснабжения и водоотведения и др.), осуществление расчетов с потребителями в рамках заключенных договоров);
– ведение расчетно-информационного обслуживания потребителей по вопросам поставки и оплаты энергоресурсов, по вопросам начислений и оплаты оказываемых оператором коммунальных услуг (ресурса), включая расчет и начисление платы за коммунальные услуги (ресурс), печать и рассылку платежных документов по оплате коммунальных услуг (ресурса), консультации специалистов по вопросам поставки и оплаты энергоресурсов, по вопросам начисления и оплаты коммунальных услуг (ресурса);
– обеспечение надлежащего исполнения потребителями обязательств по заключенным с Обществом договорам оказания услуг в сфере жилищно-коммунального хозяйства и энергетики (осуществление проверок надлежащего исполнения договорных обязательств потребителями, в том числе расчет задолженности по оплате оказанных услуг; направление требований о надлежащем исполнении обязательств, взыскание задолженности потребителей по оплате услуг в досудебном и судебном порядке, предъявление к исполнению исполнительных документов, применение иных мер, предусмотренных договорами и нормами законодательства).

5.4. Сроки обработки персональных данных

5.4.1. Сроки обработки персональных данных определяются в соответствии с целями обработки, сроками действия договоров с субъектами персональных данных, а также требованиями законодательства и внутренних документов Общества.

5.4.2. Хранение персональных данных должно осуществляться 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.

5.5. Передача и поручение обработки персональных данных

5.5.1. Общество вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом «О персональных данных», на основании заключаемого с этим лицом договора.

5.5.2. В случае, если Общество на основании договора поручает обработку персональных данных третьему лицу (другому оператору), существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке, а также обязанность соблюдения требований к защите обрабатываемых персональных данных, указанных в соответствии со статьей 19 Федерального закона «О персональных данных».

5.5.3. Лицо, осуществляющее обработку персональных данных по поручению Общества, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных» и(или) договором на поручение обработки персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».

5.5.4. Передача или поручение обработки персональных данных может выполняться на основе федерального закона, в этом случае согласие субъекта персональных данных не требуется.

5.5.5. Общество вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

5.6. Общедоступные источники персональных данных

5.6.1. Общество не создает общедоступные источники персональных данных.

6. Согласие субъекта персональных данных на обработку его персональных данных

6.1. При необходимости обеспечения условий обработки персональных данных субъекта может предоставляться согласие субъекта персональных данных на обработку его персональных данных.

6.2. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1. фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2. фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
3. наименование и адрес Общества;
4. цель обработки персональных данных;
5. перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
6. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка будет поручена такому лицу;
7. перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Обществом способов обработки персональных данных;
8. срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
9. подпись субъекта персональных данных.

6.3. Персональные данные могут быть получены Обществом от лица, не являющегося субъектом персональных данных, при условии предоставления подтверждения наличия оснований, указанных в пунктах 2 – 11 части 1 статьи 6, пунктах 2 – 10 части 2 статьи 10 и части 2 статьи 11 Федерального закона «О персональных данных».

6.4. Формы согласий разрабатываются Обществом в соответствии с требованиями Федерального закона «О персональных данных». При необходимости методическое сопровождение разработки и согласование форм согласий на обработку персональных данных осуществляется Департаментом мониторинга и защиты персональных данных АО «ЭН+ ГЕНЕРАЦИЯ».

В случае утверждения в Группе компаний ЭН+ форм согласий на обработку персональных данных для определенных случаев обработки, Общество использует утвержденные формы.

7. Разработка и утверждение локальных нормативных документов, регламентирующих вопросы обработки персональных данных в Обществе

7.1. Общество совместно с Департаментом ПДн при необходимости разрабатывает и утверждает либо актуализирует базовые локальные нормативные документы, регламентирующие вопросы обработки персональных данных, в том числе:

7.1.1. Политику в отношении обработки персональных данных;

7.1.2. Приказ о назначении ответственного за организацию обработки персональных данных и инструкцию ответственного за организацию обработки персональных данных;

7.1.3 Приказ об уничтожении персональных данных;

7.1.4. Приказ об утверждении форм документов, необходимых в целях выполнения требований законодательства РФ в области персональных данных;

7.1.5. Приказ об утверждении перечней сотрудников (должностей сотрудников), осуществляющих обработку ПДн и имеющих доступ к обрабатываемым ПДн;

7.1.6. Приказ о внутреннем контроле соответствия обработки персональных данных;

7.1.7. Приказ об оценке вреда, который может быть причинен субъектам персональных данных;

7.1.8. Приказ об обеспечении безопасности материальных носителей персональных данных.

7.2. В отношении информационных систем персональных данных, используемых в Обществе, при необходимости разрабатываются и утверждаются либо актуализируются следующие локальные регламентирующие документы:

7.2.1. Приказ об утверждении перечня ИСПДн и перечня персональных данных, обрабатываемых в ИСПДн;

7.2.2. Акты определения уровня защищенности персональных данных при их обработке в ИСПДн;

7.2.3. Модель угроз безопасности персональных данных в ИСПДн;

7.2.4. Приказ об ответственном за обеспечение безопасности ПДн в ИСПДн (для 2 и 3 уровней защищенности персональных данных);

7.2.5. Приказ о системе разграничения доступа в ИСПДн;

7.2.6. Приказ о контролируемых зонах.

7.3. Разработка документации, предусмотренной пунктом 7.1. настоящего стандарта предприятия, осуществляется Обществом при сопровождении Департамента ПДн.

7.4. В целях разработки и утверждения документов, предусмотренных пунктом 7.1. настоящего стандарта предприятия, Общества определяет сотрудника, обеспечивающего взаимодействие с Департаментом ПДн при разработке документации.

7.5. Департамент ПДн сопровождает процесс сбора необходимой информации в Обществе и формирует проекты документов. В случае участия Общества в проекте автоматизации процессов обработки персональных данных с использованием специализированного программного продукта документы формируются в указанном программном продукте.

7.6. Ответственный сотрудник Общества направляет разработанные совместно с Департаментом ПДн документы на согласование и утверждение в установленном порядке; после утверждения ответственный сотрудник направляет скан-копии документов в Департамент ПДн.

7.7. Разработка документации, предусмотренной пунктом 7.2. настоящего стандарта предприятия, осуществляется Обществом совместно с Департаментом ПДн и подразделением ИБ.

Перечень ИСПДн, предусмотренный пунктом 7.2.1., утверждается в Обществе с учетом базового корпоративного перечня ИСПДн, утвержденного приказом по Группе компаний ЭН+.

Ответственный за обеспечение безопасности ПДн в ИСПДн назначается для ИСПДн 3-го и 2-го уровней защищенности.

7.8. Департамент ПДн контролирует актуальность базового пакета регламентирующей документации по Группе компаний ЭН+; в случае изменения законодательства инициирует внесение изменений в соответствующие регламентирующие документы.

7.9. Общество обеспечивает актуальность базового пакета регламентирующей документации с точки зрения организации внутренних процессов в Обществе (кадровые перестановки, изменение перечня помещений, в которых ведется обработка персональных данных, изменение составов комиссий, ответственных лиц и т.п.).

8. Уведомление о намерении осуществлять обработку персональных данных

8.1. Общество, за исключением случаев, предусмотренных Федеральным законом «О персональных данных», до начала обработки персональных данных уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

8.2. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление

содержит следующие сведения:

1) наименование (фамилия, имя, отчество), адрес Общества;

2) цель обработки персональных данных;

3) описание мер, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

4) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

5) дата начала обработки персональных данных;

6) срок или условие прекращения обработки персональных данных;

7) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

8) сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

9) фамилия, имя, отчество физического лица или наименование юридического лица, имеющих доступ и (или) осуществляющих на основании договора обработку персональных данных, содержащихся в государственных и муниципальных информационных системах;

10) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

8.3. В случае изменения указанных сведений Общество не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения, уведомляет уполномоченный орган по защите прав субъектов персональных данных обо всех произошедших за указанный период изменениях. В случае прекращения обработки персональных данных Общество уведомляет об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты прекращения обработки персональных данных.

8.4. В случае участия Общества в проекте автоматизации процессов обработки персональных данных с использованием специализированного программного продукта возможно формирование и выгрузка уведомления с использованием указанного программного продукта.

9. Взаимодействие с Департаментом ПДн

9.1. Департамент ПДн является структурным подразделением, ответственным за сопровождение процессов обработки и защиты ПДн в компаниях Группы ЭН+, включая:

9.1.1. обеспечение единых подходов к обработке и защите ПДн в Группе компаний;

9.1.2. контроль соответствия обработки и защиты персональных данных требованиям законодательства о персональных данных, в том числе при проведении внутренних аудитов компаний Группы ЭН+;

9.1.3. организация разработки документации по вопросам персональных данных;

9.1.4. организация обучения работников компаний Группы ЭН+ по вопросам персональных данных;

9.1.5. участие в согласовании технических решений при внедрении (доработке) новых ИСПДн в Группе компаний ЭН+;

9.1.6. методологическое и консультационное сопровождение компаний Группы ЭН+ по вопросам персональных данных, включая координацию взаимодействия с надзорными органами и субъектами персональных данных.

9.2. Взаимодействие Общества с Департаментом ПДн осуществляется в соответствии с Регламентом, утвержденным приказом по Группе компаний ЭН+, в рамках

реализации функций, предусмотренных Положением о Департаменте ПДн.

10. Уничтожение персональных данных

10.1. Под уничтожением персональных данных подразумеваются 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.

Уничтожение персональных данных осуществляется Обществом по основаниям и в сроки, установленные Федеральным законом «О персональных данных» с соблюдением требований приказа Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

10.2. Уничтожение персональных данных осуществляется Обществом в следующих случаях:

– по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей, истечении срока обработки и хранения персональных данных;

– в случае отзыва субъектом персональных данных согласия на обработку его персональных данных;

– в случае выявления неправомерной обработки персональных данных;

– в случае подтверждения незаконного получения персональных данных либо несоответствия обрабатываемых персональных данных заявленной цели обработки.

10.3. В случае достижения цели обработки персональных данных Общество обязуется прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Обществом и субъектом персональных данных либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

10.4. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Общество обязуется прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Обществом и субъектом персональных данных либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.

10.5. В случае выявления субъектом персональных данных, его представителем или уполномоченным органом по защите прав субъектов персональных данных неправомерной обработки персональных данных, осуществляемой Обществом или лицом, действующим по поручению Общества, и невозможности обеспечить правомерность обработки персональных данных, Общество в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязуется уничтожить такие персональные данные или обеспечить их уничтожение. Об уничтожении персональных данных Общество обязуется уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его

представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

10.6. В случае представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Общество в срок, не превышающий семи рабочих дней со дня представления таких сведений, обязана уничтожить такие персональные данные. Общество обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

10.7. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных в пунктах 10.3 – 10.6 настоящего стандарта предприятия, Общество осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Общества) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

11. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

11.1. Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных»

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн, реализуемых в рамках создаваемой системы защиты персональных данных (далее – СЗПДн).

11.2. СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн, уровня защищенности ПДн, который необходимо обеспечить, и информационных технологий, используемых в информационных системах.

11.3. Безопасность ПДн при их обработке в ИСПДн обеспечивает Общество или лицо, осуществляющее обработку ПДн по поручению Общества на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между Обществом и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность ПДн при их обработке в информационной системе.

11.4. Выбор средств защиты информации для СЗПДн осуществляется в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (далее – ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) во исполнение Федерального закона «О персональных данных».

11.5. Структура, состав и основные функции СЗПДн определяются исходя из уровня защищенности ПДн при их обработке в ИСПДн.

11.6. Общество на основании проведенной предварительной инвентаризации используемых информационных систем определяет и утверждает приказом перечень ИСПДн Общества и состав ПДн, обрабатываемых в ИСПДн.

Формирование перечня ИСПДн осуществляется ответственным за организацию обработки персональных данных (а при его отсутствии – иным определенным руководителем Общества ответственным работником) совместно с Департаментом ПДн и подразделением ИТ (*при его отсутствии – обслуживающей компанией ООО «ЭН+ ДИДЖИТАЛ»*) с учетом утвержденного базового корпоративного перечня ИСПДн. Перечень ИСПДн согласовывает подразделение информационной безопасности

(специалист по информационной безопасности), ответственное (ый) за сопровождение Общества.

11.7. Для каждой ИСПДн (группы ИСПДн) в Обществе должна быть разработана модель угроз безопасности ПДн при их обработке в ИСПДн с учетом требований 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» на основании Методики оценки угроз безопасности информации, утвержденной ФСТЭК России 05.02.2021.

11.8. Все информационные системы персональных данных Общества подлежат обязательной оценке в соответствии с постановлением Правительства Российский Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». По итогам оценки оформляется и утверждается акт определения уровня защищенности ПДн при их обработке в ИСПДн.

12. Ответственность

12.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, уголовную ответственность в соответствии с действующим законодательством.

12.2. Руководители структурных подразделений Общества несут ответственность за соблюдение работниками возглавляемых подразделений норм, регулирующих обработку персональных данных.

12.3. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы с персональными данными работодатель вправе применить предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.