Общество с ограничесснной ответственностью «Лениногорские тепловые сети»

УТВЕРЖДАЮ
Генеральный директор
ООО «ЛТС»
_____ **А.А. Хисматуллин**
«_01_» _октября_ 20_15_ г.

ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Лениногорские тепловые сети»

СОГЛАСОВАНО
Начальник юридически-правового отдела
_____ Л.Х. Ялалова
«_01_» _октября_ 20_15_ г.

г. Лениногорск

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Лениногорские тепловые сети» (далее - Положение) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ«О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю 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» и другими нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

1.2. Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Лениногорские тепловые сети».

1.3. Безопасность персональных данных при их обработке в информационных системах персональных данных обеспечивается применением организационных мер и технических средств защиты информации (в том числе средств предотвращения несанкционированного доступа). Организационные меры и технические средства защиты информации должны удовлетворять требованиям, установленным нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

1.4. Термины и определения, используемые в Положении:

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

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

информационная система персональных данных (далее - ИС) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации

определить принадлежность персональных данных конкретному субъекту персональных данных;

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;

оператор персональных данных – ООО «Лениногорские тепловые сети», осуществляющее обработку персональных данных, а также определяющее цели обработки, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

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

распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

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.

1.5. Требования настоящего Положения являются обязательными для исполнения всеми лицами, получившими доступ к персональным данным.

1.6. Решение о необходимости изменения Положения принимается на основании:

результатов проведенных аудитов, мероприятий по контролю и надзору за обеспечением безопасности персональных данных, осуществляемых уполномоченными органами;

изменения нормативных правовых актов и (или) нормативных методических документов Российской Федерации в области защиты персональных данных;

изменения процессов обработки персональных данных в ИС персональных данных Главного управления имущественных отношений Алтайского края;

результатов анализа инцидентов информационной безопасности в ИС персональных данных;

жалоб субъектов персональных данных.

Изменение мероприятий по защите персональных данных при их обработке в ИС должны быть направлены на предотвращение инцидентов или устранения последствий уже реализованных инцидентов информационной безопасности.

Все предлагаемые изменения Положения подлежат предварительной оценке до их ввода в действие, на соответствие нормативным правовым актам и нормативным методическим документам Российской Федерации, регулирующим отношения, связанные с обеспечением безопасности персональных данных при их

обработке в информационных системах персональных данных.

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных осуществляется оператором персональных данных исключительно в целях реализации возложенных на него функций, определяемых законами и иными нормативными правовыми актами Российской Федерации, регулирующим отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИС персональных данных.

2.2. Объем и характер обрабатываемых персональных данных должен соответствовать целям их обработки. Недопустима обработка персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных. Недопустимо объединение созданных для несовместимых между собой целей баз данных ИС персональных данных.

2.3. Персональные данные оператор получает непосредственно от субъекта персональных данных, который принимает решение об их предоставлении и дает согласие на их обработку своей волей и в своем интересе. Согласие оформляется на бумажном бланке установленной формы и должно содержать собственноручную подпись субъекта персональных данных или его представителя.

2.4. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных, при их обработке в ИС персональных данных, оператором назначается ответственный за организацию обработки персональных данных.

2.5. Лица, доступ которых к персональным данным, обрабатываемым в ИС персональных данных, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка лиц, допущенных к сведениям, содержащим конфиденциальную информацию и персональные данные, с указанием помещений, в которых осуществляется обработка, и прав доступа к информационным и техническим ресурсам.

2.6. Персональные данные, используемые для обработки в ИС персональных данных, порядок использования, цель, периодичность и основания внесения изменений и дополнений, а также порядок хранения устанавливаются оператором с учетом специфики своей деятельности в утвержденных операторам инструкциях, регламентирующих работы в ИС персональных данных.

2.7. Оператор осуществляет обработку следующих категорий субъектов персональных данных:

кандидатов, работников, родственников работников, лиц, ранее состоявших в трудовых отношениях с Обществом;

физических лиц по договорам гражданско-правового характера, авторов результатов интеллектуальной деятельности;

контрагентов – физических лиц, представителей и работников контрагентов (юридических лиц).

2.8. Принятые в ООО «Лениногорские тепловые сети» организационно-распорядительные документы должны быть доведены до сведения всех лиц, участвующих в обработке персональных данных, в части, их касающейся.

3. ОБЯЗАННОСТИ И ПРАВА ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИС ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Оператор персональных данных обязан сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных либо его законного представителя.

3.2. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан 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.

3.3. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.4. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан

уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.5. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан 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.

3.6. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) 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 оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

3.7. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) 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 оператора) 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 оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия

субъекта персональных данных на основаниях, предусмотренных действующим законодательством Российской Федерации.

3.8. Оператор при передаче персональных данных физических лиц третьим лицам, в порядке, установленном Положением, ограничивает передаваемую информацию только теми персональными данными физических лиц, которые необходимы для выполнения третьими лицами своих функций. Передача персональных данных по телефону, факсимильной связи, электронной почте запрещается.

4. МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

4.2. В целях определения мер защиты персональных данных должна быть разработана модель угроз безопасности персональных данных, обрабатываемых в ИС персональных данных, проведена оценка актуальных угроз безопасности персональных данных.

Модель угроз безопасности персональных данных корректируется при изменении состава основных технических средств и условий эксплуатации ИС персональных данных ответственным за разработку и осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе Общества (системным администратором).

4.3. Для обеспечения принятого уровня защищенности персональных данных при обработке в ИС персональных данных необходимо выполнить следующие требования:

организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

обеспечение сохранности носителей персональных данных; утверждение документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для исполнения ими служебных (трудовых) обязанностей;

использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

4.4. Для обеспечения принятого уровня защищенности персональных данных при обработке в ИС персональных данных должны быть реализованы следующие мероприятия, входящие в состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных

данных, с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации; защита технических средств; защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

В ИС персональных данных подлежат регистрации события входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы. Срок хранения такой информации не менее 1 месяца. Анализ результатов событий безопасности проводится ответственным за разработку и осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе (системным администратором) Общества, в случае выявления фактов НСД, информация доводится до ответственного за организацию обработки персональных данных.

Лица, уполномоченные осуществлять обработку персональных данных, несут ответственность за защиту персональных данных в порядке, предусмотренном действующим законодательством Российской Федерации.

5. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ

5.1. Генеральный директор:

назначает ответственного за организацию обработки персональных данных в ООО «Лениногорские тепловые сети»;

назначает ответственного за разработку и осуществление мероприятий по обеспечению безопасности персональных данных при их обработке (системного администратора) в информационной системе Общества;

утверждает организационно-распорядительные документы по обеспечению безопасности и конфиденциальности персональных данных;

принимает решения о необходимости проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

5.2. Ответственный за разработку и осуществление мероприятий по обеспечению безопасности персональных данных при их обработке (системный администратор):

отвечает за соблюдение в ИС персональных данных требований по обеспечению безопасности информации и правильность применения средств защиты информации от несанкционированного доступа;

анализирует информацию, циркулирующую в технических средствах и системах, определяет возможные технические каналы ее утечки;

организует периодический контроль работоспособности систем защиты информации, применяемых на ИС персональных данных;

отвечает за своевременное обнаружение фактов несанкционированного доступа к ИС персональных данных;

участвует в проведение служебных расследований по фактам и попыткам несанкционированного доступа к ИС персональных данных;

организует работы по контролю эффективности технических (программно-технических, программных) мероприятий по защите (обеспечению безопасности) информации в ИС персональных данных;

проводит анализ причин выявленных нарушений и недостатков в организации защиты (обеспечении безопасности) ИС персональных данных;

разрабатывает предложения по составу общесистемных программных средств, обеспечивающих функционирование ИС персональных данных;

разрабатывает предложения по дальнейшему совершенствованию системы защиты информации, планирует мероприятия по защите ИС персональных данных;

отвечает за осуществление установки и ввода в эксплуатацию средств защиты информации ИС персональных данных в соответствии с эксплуатационной и технической документацией;

организует работы по проведению антивирусного контроля в ИС персональных данных;

осуществляет работы по организации резервного копирования персональных данных;

отвечает за регистрацию и учет защищаемых носителей информации;

отвечает за установку (обновление версий), обеспечение функционирования программного обеспечения ИС персональных данных;

разрабатывает проекты распорядительных документов по защите персональных данных при их обработке в ИС персональных данных в Главном управлении имущественных отношений Алтайского края;

подготавливает предложения о привлечении к проведению работ по защите персональных данных при их обработке в ИС персональных данных на договорной основе организаций, имеющих лицензию на соответствующий вид

деятельности.

5.3. Ответственный за организацию обработки персональных данных в ООО «Лениногорские тепловые сети»:

осуществляет координацию организационных мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИС персональных данных;

осуществляет методическое руководство сотрудников Общества, имеющих доступ к персональным данным, в вопросах обеспечения безопасности персональных данных;

отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИС персональных данных и ее ресурсов на этапах эксплуатации и модернизации;

осуществляет внутренний контроль за соблюдением требований законодательства Российской Федерации, организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИС и правил обработки персональных данных в ООО «Лениногорские тепловые сети», в том числе требований к защите персональных данных;

участвует в планировании мероприятий по защите информации, контролирует их выполнение и эффективность;

визирует организационно-методические документы по обеспечению безопасности и конфиденциальности персональных данных;

составляет список лиц, допущенных к сведениям, содержащим конфиденциальную информацию и персональные данные, с указанием помещений, в которых осуществляется обработка, и прав доступа к информационным и техническим ресурсам;

обеспечивает проведение служебных расследований по фактам и попыткам несанкционированного доступа к ИС персональных данных;

отвечает за организацию расследований причин и условий появления нарушений безопасности ИС персональных данных, разработку предложений по устранению недостатков и предупреждению подобного рода нарушений.

5.4. Пользователь ИС персональных данных:

отвечает за установленный порядок использования технического и программного обеспечения, а также применение технических и программных средств защиты информации;

соблюдает требования руководящих документов по обеспечению безопасности информации;

соблюдает утвержденную разрешительную систему доступа к техническим средствам и информации, обрабатываемой в ИС персональных данных;

немедленно докладывает администратору информационной безопасности и информирует ответственного за организацию обработки персональных данных о фактах и попытках несанкционированного доступа к обрабатываемой (хранящейся) информации в ИС персональных данных.

6. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Текущий контроль выполнения организационных мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИС персональных данных, осуществляется ответственным за организацию обработки персональных данных и администратором информационной безопасности ИС персональных данных.

6.3. Проверки соответствия обработки персональных данных установленным требованиям к защите персональных данных при их обработке в ИС персональных данных организуются и проводятся комиссией самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года на основании приказа генерального директора ООО «Лениногорские тепловые сети».

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Настоящее Положение вступает в силу с момента его утверждения.

7.2. Настоящее Положение не заменяет собой действующего законодательства Российской Федерации, регулирующего отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИС персональных данных.

7.3. В случае, если в результате изменений федеральных законов и иных нормативных правовых актов Российской Федерации отдельные требования настоящего Положения вступят в противоречие с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и нормативными правовыми актами Российской Федерации, соответствующие требования Положения не будут подлежать применению.