УТВЕРЖДЕНО
приказом генерального директора
ООО «Боржоми Тех»
от «27» декабря 2021 г.
№2712/21-06/ОД

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Первая редакция

г. Москва

ОГЛАВЛЕНИЕ

Оглавление

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1.Настоящее Положение об обработке и защите персональных данных в ООО «Боржоми Тех» (далее – Положение) определяет порядок сбора, учета, хранения, передачи и иных видов обработки персональных данных (далее – ПДн) в ООО «Боржоми Тех» (далее – Общество), а также меры по обеспечению конфиденциальности ПДн, выявлению и предотвращению нарушений законодательства Российской Федерации в сфере ПДн.

1.2.Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым Кодексом Российской Федерации, Налоговым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон), Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 08 февраля 1998 года № 14-ФЗ «Об обществах с ограниченной ответственностью» и иными нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обработкой ПДн и определяющими порядок получения, обработки, хранения, передачи и любого другого использования ПДн.

1.3.Целями настоящего Положения являются:

1.3.1.Определение порядка обработки персональных данных в Обществе;

1.3.2.Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

1.3.3.Обеспечение защиты ПДн от несанкционированного доступа и разглашения;

1.3.4.Установление ответственности должностных лиц Общества, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Основные термины и определения:

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

– *конфиденциальность персональных данных* – обязательное для соблюдения должностным лицом Общества, получившим доступ к персональным данным, требование не допускать их раскрытия и/или распространения ПДн без согласия субъекта ПДн или иного законного основания;

– *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;

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

– *неавтоматизированная обработка* (осуществляемая без использования средств автоматизации) – обработка ПДн, включающая как обработку без использования средств вычислительной техники, так и обработку с помощью средств вычислительной техники ПДн, 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 осуществляется без непосредственного участия человека;

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

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

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

– *уничтожение персональных данных* – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных Общества 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;

– *трансграничная передача персональных данных* – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

– *общедоступны персональные данные* – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

– *биометрические персональные данные* – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (например, фото, отпечатки пальцев);

– *специальные персональные данные* – сведения касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

– *информационная система персональных данных (ИСПДн)* – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

3.ЦЕЛИ И ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1.Обработка ПДн осуществляется исключительно в целях:

3.1.1.подбора кандидатов на трудоустройство, ведение кадрового резерва, проверка кандидатов на трудоустройство, ретроспективный анализ принятых кадровых решений;

3.1.2. ведения кадрового делопроизводства;

3.1.3. обработки персональных данных работников Общества для исполнения требований, предусмотренных Трудовым кодексом Российской Федерации, в том числе по выплате работникам Общества причитающейся им заработной платы, компенсаций, премий, по осуществлению налоговых и пенсионных отчислений, оформлению справок, расчетов с подотчетными лицами, оказания помощи в оформлении виз, в бронировании и приобретении гостиничных мест и транспортных билетов направляющимся в командировку работникам Общества;

3.1.4. осуществления договорной деятельности в рамках возникновения, изменения и прекращения правоотношений между Общества, заявителями, клиентами и прочими контрагентами;

3.1.5. обеспечения справочной и информационной поддержки деятельности Общества;

3.1.6. обеспечения пропускного режима Общества;

3.1.7. выполнения требований закона о воинском учёте;

3.1.8.осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

3.1.9. осуществления обработки персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами.

Полный перечень целей обработки ПДн содержится в документе «Перечень персональных данных, обрабатываемых в Обществе». Установленные цели обработки ПДн являются законными.

3.2.В Обществе обрабатываются ПДн следующих категорий субъектов ПДн:

3.2.1. соискатели вакантных должностей Общества;

3.2.2. штатные работники Общества;

3.2.3. физические лица, работающие по договорам гражданско-правового характера;

3.2.4. посетители Общества;

3.2.5. заявители, обращающиеся в Общество (далее – Заявители).

3.3.Обработка ПДн в Обществе осуществляется на основании следующих документов:

3.3.1. Конституция Российской Федерации (статьи 23 - 24, часть 1 статьи 26);

3.3.2. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

3.3.3.статьи 65, 85 – 90, 212, 213, 225, 230, 230.1 Трудового Кодекса Российской Федерации;

3.3.4.Налоговый Кодекс Российской Федерации;

3.3.5.постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

3.3.6.постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

3.3.7.Федеральный закон от 28 марта 1998 года № 53-ФЗ «О воинской обязанности и военной службе»;

3.3.8.Федеральный закон № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

3.3.9.Федеральный закон №125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»;

3.3.10.Положение о воинском учете, утвержденное постановлением Правительства Российской Федерации от 27.11.2006 № 719;

3.3.11.Устав Общества;

3.3.12.согласие субъекта персональных данных;

3.3.13.Гражданский Кодекс Российской Федерации;

3.3.14.Федеральный закон от 27 августа 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3.3.15. Федеральный закон от 22 октября 2004 года № 125-ФЗ «Об архивном деле в Российской Федерации»;

3.3.16. Приказ Минздравсоцразвития России от 12.04.2011 № 302н;

3.3.17. иные законодательные акты, предусматривающие исполнение Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

4.ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Допускается осуществлять обработку только ПДн, необходимых для достижения целей обработки ПДн, указанных в Перечне персональных данных, обрабатываемых в Обществе, утверждаемом Генеральным директором Общества.

4.2. Состав и объем (содержание) персональных данных определяется целями их обработки, заявленными при их сборе, и указаны в Перечне персональных данных, обрабатываемых в Обществе.

4.3. Согласие на обработку персональных данных допускается собирать только в форме, позволяющей подтвердить факт его получения (если иное не установлено Федеральным законом).

4.4. Обработка ПДн в Обществе производится только с согласия субъектов ПДн в письменной форме. Без согласия субъектов ПДн обработка ПДн производится в следующих случаях:

–ПДн являются общедоступными;

–обработка ПДн осуществляется в целях исполнения договора, одной из сторон которого является субъект ПДн;

–для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение его согласия невозможно;

–по требованию полномочных государственных органов в случаях, предусмотренных федеральным законодательством;

–в иных случаях, предусмотренным законодательством Российской Федерации.

4.5. Для сбора письменных согласий на обработку ПДн допускается применять только утвержденные в Обществе формы согласий, соответствующие целям обработки.

4.6. Формы согласий на обработку персональных данных и анкеты, предназначенные для внесения в них ПДн, предусмотрены Перечнем форм согласий на обработку персональных данных и анкет, утверждаемым локальным нормативным актом Общества.

4.7. Организация сбора и хранения письменных согласий на обработку ПДн возлагается на структурное подразделение Общества, в функции которого входит обработка соответствующих ПДн в соответствии с Перечнем должностей работников Общества, замещение которых предусматривает осуществление обработки ПДн или осуществление доступа к ПДн (далее – Перечень должностей), утверждаемым локальным нормативным актом

Общества. Форма Перечня должностей приведена в Приложении №2 к настоящему Положению.

4.8. В случаях, если обязанность предоставления ПДн установлена Федеральным законом, работник Общества, осуществляющий сбор согласия субъекта ПДн, обязан разъяснить субъекту ПДн юридические последствия отказа предоставить свои ПДн. Обязанность предоставления ПДн установлена федеральными законами для следующих субъектов ПДн, чьи ПДн обрабатываются в Обществе:

–для работников Общества – Трудовым кодексом Российской Федерации;

–для физических лиц, состоящих в договорных и иных гражданско-правовых отношениях с Обществом, – Гражданским кодексом Российской Федерации;

–для членов органов управления Общества – Федеральным законом от 08 февраля 1998 года № 14-ФЗ «Об обществах с ограниченной ответственностью».

4.9. Перед началом обработки ПДн Общество уведомляет субъекта ПДн (лично или посредством направления заказного письма) о целях и способах обработки ПДн, невозможности прекращения.

4.10. Перед началом обработки ПДн Общество уведомляет субъекта ПДн (лично или посредством направления заказного письма) о целях и способах обработки ПДн, невозможности прекращения обработки (блокирования, уничтожения) ПДн субъекта до истечения, предусмотренного действующим законодательством Российской Федерации срока хранения данных.

4.11.Основным источником персональных данных субъекта ПДн является непосредственно сам субъект. Если ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть заранее в письменной форме уведомлен об этом, и от него должно быть получено письменное согласие. Ответственность за направление такого уведомления субъекту ПДн несет лицо, ответственное за сбор ПДн, осуществляемый в Обществе.

5. ЛИЦО, ОТВЕТСТВЕННОЕ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПДн

5.1. Лицо, ответственное за организацию обработки ПДн, назначается приказом Генерального директора Общества.

5.2. В должностные обязанности лица, ответственного за организацию обработки ПДн, входит:

- осуществление внутреннего контроля за соблюдением Обществом и работниками Общества законодательства Российской Федерации о персональных данных и требований по защите ПДн;

- доведение до сведения работников Общества положений законодательства Российской Федерации и локальных нормативных актов Общества в области обработки и защиты ПДн и/или организация мероприятий по повышению осведомленности работников Общества в области обработки и защиты ПДн;

- организация соблюдения прав субъектов ПДн и организация обеспечения безопасности ПДн;

- организация приема и обработки обращений и запросов субъектов ПДн или их представителей и/или осуществление контроля за приемом и обработкой таких обращений и запросов;

- осуществление контроля за приемом и организацией направления в адрес уполномоченного органа по защите прав субъектов персональных данных уведомления об обработке ПДн, а также своевременное уведомление об изменении условий обработки.

5.3. В случае нахождения в отпуске, отсутствия по болезни или по иной причине лица, ответственного за организацию обработки ПДн, его обязанности выполняет работник Общества, назначенный приказом Генерального директора Общества.

6.ДЕЙСТВИЯ (ОПЕРАЦИИ), СОВЕРШАЕМЫЕ С ПДн

6.1. Общество осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (в том числе распространение, предоставление, трансграничную передачу), блокирование, обезличивание, уничтожение ПДн, а также иные действия, предусмотренные законодательством Российской Федерации о персональных данных.

6.2. Допустимые действия с ПДн определяются и ограничиваются целями, указанными при их сборе.

6.3. Работникам Общества запрещается осуществлять сбор, обработку и хранение ПДн субъектов ПДн, не указанных в Перечне персональных данных, обрабатываемых в Обществе, предусмотренном пунктом **Ошибка! Источник ссылки не найден.** настоящего Положения.

6.4. ПДн субъектов обрабатываются в Обществе как на бумажных носителях (без использования средств автоматизации), так и в электронном виде (с помощью средств вычислительной техники).

6.5. При неавтоматизированной обработке ПДн запрещается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. При неавтоматизированной обработке для разных категорий ПДн должны использоваться отдельные материальные носители.

6.6. Обработка ПДн в электронном виде допускается только с применением ИСПДн, соответствующих целям обработки и содержащихся в утверждаемом Генеральным директором Общества Перечне ИСПДн Общества.

6.7. Перечень ИСПДн Общества составляется лицом, ответственным за организацию обработки ПДн, на основе сведений об информационных системах Общества, предоставляемых ИТ специалистом Общества. Полнота Перечня ИСПДн Общества подтверждается визой (подписью) ИТ специалиста Общества.

6.8. При создании новых баз данных, реестров, таблиц, анкет, книг, журналов, предусматривающих занесение в них персональных данных, а также внедрении новых ИСПДн порядок обработки и защиты персональных данных в них согласовывается с лицом, ответственным за организацию обработки ПДн.

6.9. При внедрении новых ИСПДн, изменении объема (содержания), порядка и целей обработки ПДн лицо, ответственное за организацию обработки ПДн, инициирует внесение изменений в уведомление уполномоченного органа по защите прав субъектов персональных данных - федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере информационных технологий и связи (п. 1 ст. 23 Федерального закона) - об обработке ПДн в Обществе.

6.10.Сбор персональных данных.

6.10.1.Сбор персональных данных осуществляется после или совместно с получением согласия на обработку персональных данных путем:

– внесения ПДн субъектом ПДн в утвержденные в Обществе или предусмотренные законодательством Российской Федерации формы и анкеты, соответствующие целям обработки;

– внесения ПДн субъектом ПДн в ИСПДн Общества самостоятельно (в случае, если такая возможность предусмотрена в ИСПДн и утверждена локальными нормативными актами Общества);

– копирования оригиналов документов работниками структурного подразделения Общества, в функции которого входит обработка соответствующих ПДн в соответствии с Перечнем должностей;

– получения оригиналов документов;

– внесения предоставленных сведений работниками структурного подразделения Общества, в функции которого входит обработка соответствующих ПДн в соответствии с Перечнем должностей, в соответствующие целям обработки ИСПДн;

– получения письменных обращений субъектов ПДн, содержащих ПДн;

– получения ПДн из общедоступных источников.

6.10.2.Во всех информационно-телекоммуникационных сетях, с помощью которых организуется сбор персональных данных, должна быть опубликована Политика в отношении обработки и защиты ПДн в Обществе.

6.10.3.Во всех существующих и/или разрабатываемых ИСПДн Общества (в том числе веб-сайтах), в которых реализована подсистема самостоятельной регистрации субъектов ПДн (в том числе подсистема сбора ПДн), субъекту ПДн должна быть предоставлена возможность до окончания регистрации ознакомиться и выразить свое согласие с условиями использования данной ИСПДн, включающими порядок обработки и защиты персональных данных, вносимых субъектом ПДн.

6.11.Хранение ПДн.

6.11.1.Персональные данные хранятся на бумажных носителях, отчуждаемых (съемных) носителях информации (дискеты, CD-диски, съемные накопители) работниками структурного подразделения Общества, в функции которого входит обработка соответствующих ПДн в соответствии с Перечнем должностей.

6.11.2.Хранение носителей ПДн должно осуществляться способом, не допускающим несанкционированное использование, распространение и уничтожение ПДн, находящихся на этих носителях (сохранность ПДн), а также позволяющим обнаружить факт несанкционированного доступа.

6.11.3.Хранение ПДн в Обществе должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, если иной срок не установлен законодательством Российской Федерации о персональных данных.

6.11.4.Сроки хранения ПДн на бумажном носителе определяются в соответствии с требованиями законодательства Российской Федерации, локальными нормативными актами Общества, регламентирующими порядок их сбора, обработки и хранения.

6.11.5.Срок хранения ПДн в электронном виде должен соответствовать сроку хранения бумажных оригиналов.

6.11.6.Хранение ПДн, обработка которых осуществляется в различных целях, должны храниться на различных носителях ПДн.

6.11.7.За организацию хранения и использования носителей ПДн, своевременное предоставление сведений для регистрации мест хранения ПДн несет ответственность руководитель структурного подразделения, в функции которого входит обработка соответствующих ПДн в соответствии с Перечнем должностей.

6.12.Использование и уточнение (изменение, дополнение) ПДн.

6.12.1.Использование ПДн осуществляется в соответствии с федеральными законами, на основании которых они обрабатываются.

6.12.2.Вывод на печать документов, содержащих ПДн, допускается в связи с исполнением должностных обязанностей, в том числе в целях передачи печатных копий субъектам ПДн либо работникам, допущенным к обработке ПДн в соответствии с утвержденным Перечнем должностей.

6.12.3.Вынос работником документов на бумажных носителях и/или отчуждаемых носителей, содержащих ПДн, за пределы контролируемой зоны (офис Общества) допускается исключительно для исполнения договоров, соглашений, инструкций, регламентов, положений и иных локальных нормативных актов Общества.

6.12.4.Уточнение (изменение, дополнение) ПДн при осуществлении их обработки без использования средств вычислительной техники может производиться путем обновления (в том числе частичного) или изменения данных на материальном носителе. Если это не допускается техническими особенностями материального носителя, то путем фиксации на том же материальном носителе сведений об изменениях, вносимых в ПДн, либо путем изготовления нового материального носителя с уточненными ПДн.

6.13.Передача (предоставление, распространение и трансграничная передача ПДн).

6.13.1.Предоставление ПДн осуществляется в соответствии с федеральными законами, на основании которых они обрабатываются в порядке, предусмотренном настоящим Положением.

6.13.2.Трансграничная передача ПДн, обрабатываемых в Обществе, без согласия на то субъекта ПДн в письменной форме, не допускается.

6.13.3.Распространение ПДн допускается только при условии предварительного получения письменного согласия субъекта ПДн.

6.14.Прекращение обработки ПДн (блокирование, обезличивание, уничтожение).

6.14.1.После достижения цели обработки, утраты необходимости в ее достижении или отзыве согласия на обработку ПДн субъектом ПДн, если иное не предусмотрено законодательством Российской Федерации, ПДн подлежат обезличиванию или уничтожению в соответствии с Регламентом уничтожения персональных данных в Общества, утверждаемым органом управления Общества.

6.14.2.Допустимыми способами уничтожения являются механическое нарушение целостности носителя, не позволяющее произвести считывание или восстановление персональных данных и/или удаление с электронных носителей методами и средствами гарантированного удаления остаточной информации.

7.ДОПУСК РАБОТНИКОВ ОБЩЕСТВА К ОБРАБОТКЕ ПДн

7.1. В отношении ПДн, обрабатываемых в Обществе, на весь срок их обработки в Обществе устанавливается режим конфиденциальности. При этом любые ПДн, обрабатываемые в Обществе, считаются конфиденциальными, но применение грифа конфиденциальности в отношении документов, содержащих персональные данные, не обязательно.

7.2. Обработка ПДн и доступ к ним разрешены только работникам, получившим допуск к обработке ПДн в соответствии с утвержденным Перечнем должностей.

7.3. Все работники, получившие допуск к обработке ПДн, должны обеспечивать конфиденциальность ПДн, обрабатываемых в Обществе, за исключением обезличенных и общедоступных ПДн.

7.4. Работники Общества должны быть ознакомлены под подпись с документами Общества, устанавливающими порядок обработки и защиты ПДн, а также со своими правами и обязанностями, возникающими при осуществлении обработки и защиты ПДн.

7.5. Допуск к обработке ПДн может быть оформлен только для работников Общества, имеющих достаточные основания для обработки ПДн или осуществления доступа к ним.

7.6. К достаточным основаниям обработки ПДн или осуществления доступа к ним относится необходимость исполнения работником трудовых обязанностей, предусмотренных должностными инструкциями, а также необходимость исполнения требований законодательства Российской Федерации, в том числе для реализации прав субъектов персональных данных в соответствии со статьей 14 Федерального закона. Права и обязанности работника Общества относительно соблюдения правовых актов, касающихся обработки и защиты ПДн в Обществе, в том числе обязательство прекратить обработку ПДн в случае расторжения трудового договора, должны быть включены в Обязательство о неразглашении ПДн работником Общества (далее – Обязательство, Обязательство о неразглашении ПДн). Форма Обязательства о неразглашении приведена в Приложении №1 к настоящему Положению. Обязательство приобщается к личному делу работника, подписавшего такое Обязательство и получившего допуск к обработке ПДн.

7.7.Допуск к обработке ПДн работника Общества считается оформленным с момента предоставления работником подписанного им Обязательства о неразглашении ПДн.

7.8.Информация о наличии или отсутствии оснований обработки ПДн или доступа к ним предоставляется структурное подразделение Общества, в функции которого входит обработка соответствующих ПДн в соответствии с Перечнем должностей, лицом, ответственным за организацию обработки ПДн. Для этих целей лицо, ответственное за организацию обработки ПДн, формирует Перечень должностей, предусмотренный п. 3.7 настоящего Положения.

7.9.Перечень должностей формируется, дорабатывается и пересматривается по мере необходимости (изменение организационно-штатной структуры, введение новых должностей, изменении должностных обязанностей работников, функций структурных подразделений и т.п.) лицом, ответственным за организацию обработки ПДн, на основании копий приказов, представляемых сотрудниками отдела по работе с персоналом, и утверждается Генеральным директором Общества.

7.10.Информация о наличии или отсутствии оформленного допуска у работника Общества представляется сотрудниками отдела по работе с персоналом Общества по запросу работников Общества.

7.11.Доступ работников Общества к ПДн предоставляется только для исполнения должностных обязанностей при условии наличия должности работника в Перечне должностей, после оформления допуска. Любые действия с ПДн, обрабатываемыми в Обществе, работниками, чьи должности не предусмотрены Перечнем должностей, запрещены.

7.12.Доступ работников Общества к ПДн, зафиксированным на бумажных носителях или отчуждаемых электронных носителях, организуется и предоставляется лицом, ответственным за организацию обработки ПДн, либо структурным подразделением Общества, в функции которого входит обработка соответствующих ПДн в соответствии с Перечнем должностей.

7.13.Руководитель структурного подразделения, включенного в Перечень должностей, в котором обрабатываются ПДн, осуществляет контроль за соблюдением правил разграничения доступа к ПДн и требований по обеспечению конфиденциальности ПДн в рамках своих полномочий.

8.ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Не допускается предоставление ПДн государственному органу, его территориальному органу, органу местного самоуправления или организации, подведомственной государственному органу, органу местного самоуправления, а также физическому или юридическому лицу, за исключением случаев, предусмотренных федеральными законами.

8.2. В соответствии со статьей 6 Федерального закона Общество может поручать обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации о персональных данных, на основании договора (далее – Договор-поручение на обработку ПДн). В Договоре-поручении на обработку ПДн указываются порядок предоставления ПДн, перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку персональных данных, обязательства сторон по соблюдению конфиденциальности и обеспечению безопасности персональных данных при их обработке, цели обработки, а также требования к защите обрабатываемых ПДн.

8.3. В случае, когда при закупке товаров, работ, услуг требуется (подразумевается) предоставление Обществом ПДн, инициатор закупки обеспечивает включение в проект договора, заключаемого с единственным поставщиком, а также в проект договора, являющего частью документации о закупке, условий Договора-поручения на обработку ПДн, указанных в п.8.2 настоящего Положения.

8.4. В случае, когда при закупке товаров, работ, услуг требуется получение Обществом ПДн, инициатор закупки обеспечивает включение в проект договора, заключаемого с единственным поставщиком, а также в проект договора, являющего частью документации о закупке, условий, способствующих снижению количества административных процедур, подлежащих исполнению Обществом в соответствии с законодательством о персональных данных (например, получение Обществом обезличенных ПДн; получение Обществом ПДн лиц, давших согласие на предоставление доступа к их ПДн неограниченного круга лиц; возложение на контрагента по договору, передающего ПДн Обществу, обязательств по предварительному получению согласия субъектов ПДн на обработку их ПДн, включая согласие на передачу ПДн Обществу и/или его контрагенту, уведомлению субъекта ПДн о предстоящей обработке его ПДн Обществом и/или его контрагентом).

8.5. Проекты договоров, заключаемых с единственным поставщиком, а также проекты договоров, являющихся частью документации о закупке, подразумевающих передачу или получение Обществом ПДн, дополнительно подлежат согласованию лицом, ответственным за организацию обработки ПДн. В целях соблюдения требований настоящего пункта инициатор закупки при направлении указанных в настоящем пункте документов на рассмотрение и предварительное согласование сопровождает их информацией о планируемой обработке ПДн. Указанная информация предоставляется в электронном виде.

8.6. Общество предоставляет персональные данные субъекта ПДн государственному органу, его территориальному органу, органу местного самоуправления или организации, подведомственной государственному органу, органу местного самоуправления, а также физическому или юридическому лицу на основании запроса о предоставлении персональных данных (далее − Запрос) в случаях, предусмотренных законодательством.

8.7. Запрос оформляется в письменном виде и должен быть подписан уполномоченным лицом или субъектом ПДн, содержать указание цели и правового основания затребования

персональных данных и срок предоставления этой информации, если иное не установлено законодательством.

8.8. Запрос подлежит рассмотрению Обществом, в процессе которого определяются положения федеральных законов, устанавливающие право обратившегося государственного органа, его территориального органа, органа местного самоуправления или организации, подведомственной государственному органу, органу местного самоуправления, а также физического или юридического лица на получение запрашиваемых ПДн.

8.9. Обоснованием (мотивом) Запроса является конкретная цель, связанная с реализацией гражданином своих прав или исполнением субъектом обращения определенных законодательством федеральным законом обязанностей, для достижения которых ему необходимо использовать запрашиваемые ПДн, например, находящееся в производстве суда, правоохранительного органа дело (в Запросе указывается номер), проведение правоохранительным органом оперативно-розыскных мероприятий или проверки по поступившей в этот орган информации (в Запросе указывается дата и номер документа, на основании которого проводится оперативно-розыскное мероприятие) и т.д. Запросы, по форме и содержанию не отвечающие требованиям п.8.7 настоящего Положения, исполнению не подлежат.

8.10. Запрос субъекта ПДн о предоставлении его ПДн в соответствии со статьей 14 Федерального закона должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Обществом, либо сведения, иным образом подтверждающие факт обработки ПДн Обществом, подпись субъекта ПДн или его представителя.

8.11. Право субъекта ПДн на доступ к своим ПДн может быть ограничено в случаях, предусмотренных законодательством Российской Федерации.

8.12. При получении Запроса субъекта ПДн или его законного представителя по вопросам получения сведений, предусмотренных законодательством Российской Федерации, должностное лицо Общества, получившее такой Запрос, обязано проинформировать лицо, ответственное за организацию обработки ПДн, и передать ему оригинал обращения в течение дня, когда был получен Запрос или на следующий рабочий день.

8.13. Лицо, ответственное за организацию обработки ПДн, обязано зарегистрировать поступивший Запрос (в том числе в Журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки ПДн, оформленном по форме, приведенной в Приложении №3 к настоящему Положению), принять меры по предоставлению субъекту ПДн требуемой информации или мотивированного отказа в предоставлении такой информации, а также принять меры по уточнению, блокированию или уничтожению ПДн субъекта ПДн в случае законности соответствующих требований субъекта ПДн.

8.14. Лицо, ответственное за организацию обработки ПДн, имеет право запросить у любого работника Общества информацию, необходимую для ответа на Запрос, а работник Общества обязан её предоставить (в том числе в письменной форме) в течение одного рабочего дня.

8.15. Ответ на Запрос субъекта ПДн формируется лицом, ответственным за организацию обработки ПДн, в письменном виде, подписывается Генеральным директором Общества в течение одного рабочего дня, а затем в срок, не превышающий одного рабочего дня, отправляется в адрес субъекта ПДн государственной почтовой службой заказным письмом с уведомлением о вручении или курьером (непосредственно в руки адресату под подпись).

8.16. При реализации прав субъекта ПДн его персональные данные должны предоставляться ему таким образом, чтобы не нарушалась конфиденциальность персональных данных других субъектов ПДн.

9.ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Мероприятия по обеспечению безопасности ПДн в ИСПДн определяются Политикой в области обработки и защиты персональных данных Общества, утвержденной приказом генерального директора Общества.

10.ОРГАНИЗАЦИЯ ВНУТРЕННЕГО КОНТРОЛЯ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДн

10.1.Внутренний контроль обработки ПДн в Обществе осуществляется в целях предотвращения и выявления нарушений законодательства Российской Федерации, принятых в соответствии с ним нормативных правовых актов Российской Федерации и локальных нормативных актов Общества.

10.2.Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

- обеспечение соблюдения работниками Общества порядка обработки и защиты ПДн;
- оценку знаний работников, задействованных в обработке ПДн;
- обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн;
- внедрение методов контроля и проведение проверок, направленных на выявление нарушений установленного порядка обработки ПДн;
- разработка и выполнение корректирующих мер, направленных на устранение выявленных нарушений порядка обработки ПДн;
- разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий;
- контроль исполнения рекомендаций и указаний по устранению указанных нарушений;
- отслеживание законодательства, регламентирующего требования работы с ПДн.

10.3.Лицо, ответственное за организацию обработки ПДн, не реже 1 раза в 3 года организует проведение внутреннего контроля соблюдения порядка обработки и обеспечения безопасности ПДн силами соответствующей постоянно действующей комиссии, состав которой утверждается приказом Генерального директора Общества (далее – Комиссия).

10.4.Проведение внутреннего контроля соблюдения порядка обработки и обеспечения безопасности ПДн включает:

- проверку деятельности работников Общества, допущенных к работе с ПДн и связанной с обработкой ПДн;
- проверку состояния защищенности ПДн, обрабатываемых в ИСПДн, включая выполнение требований по защите для каждой конкретной ИСПДн, корректности работы системы защиты ПДн и т.д.

10.5.Все результаты контрольных мероприятий представляются Генеральному директору Общества в виде отчетов проведения внутреннего контроля, подписанных членами

Комиссии, указанной в п. 9.3 настоящего Положения. Форма отчета проведения внутреннего контроля приведена в Приложении № 4 к настоящему Положению.

10.6.При выявлении нарушений порядка обработки и обеспечения безопасности ПДн (далее – Нарушение), сведения о них фиксируются в Журнале учета выявленных нарушений, оформленном по форме, приведенной в Приложении № 5 к настоящему Положению, и прилагаются к акту.

10.7.В отношении выявленных нарушений по распоряжению Генерального директора Общества инициируется проведение служебной проверки.

10.8.Лицо, ответственное за организацию обработки ПДн, организует принятие мер по нейтрализации угроз, приведших к возникновению нарушений, а также по устранению последствий таких нарушений.

11.ОТВЕСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИЩ ОБРАТОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1.Лица, виновные в нарушении норм, регулирующих получение, учет, обработку, хранение и защиту ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 1

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных работником ООО «Боржоми Тех», включенным в Перечень должностей работников ООО «БОРЖОМИ ТЕХ», замещение которых предусматривает осуществление обработки персональных данных или осуществление доступа к ним

Я, _____,

(фамилия, имя, отчество полностью)

с Положением об обработки и защите персональных данных в ООО «БОРЖОМИ ТЕХ» (далее – Положение) ознакомлен(а), о предоставлении мне допуска к обработке персональных данных в соответствии с Положением оповещен(а), понимаю, что получаю доступ к персональным данным, обрабатываемым в ООО «БОРЖОМИ ТЕХ», и обязуюсь:

- соблюдать порядок обработки и защиты персональных данных, установленный в ООО «БОРЖОМИ ТЕХ» указанным Положением, а также иными локальными нормативными актами Общества по вопросам обработки и защиты персональных данных, с которыми я ознакомлен(а);
- не разглашать (в том числе устно, письменно и/или с применением средств вычислительной техники) персональные данные работников ООО «БОРЖОМИ ТЕХ» и иных лиц, ставшие мне известными в связи с исполнением моих должностных обязанностей;
- информировать своего непосредственного руководителя и лицо, ответственное за организацию обработки персональных данных, об утрате документов и/или носителей персональных данных, о фактах нарушения порядка обращения с ними, о попытках несанкционированного доступа к персональным данным;
- использовать персональные данные лишь в целях, для которых они сообщены;
- по прекращении трудового договора с ООО «БОРЖОМИ ТЕХ» вернуть все носители персональных данных (документы, машинные носители, черновики, распечатки и др.), которые находились в моем распоряжении в связи с выполнением должностных обязанностей, передать их непосредственному руководителю или иному, специально назначенному для этой цели лицу.

Разрешаю ООО «БОРЖОМИ ТЕХ» осуществлять контроль за соблюдением мной Положения и иных локальных нормативных актов Общества по вопросам обработки и защиты персональных данных, с которыми я ознакомлен(а), в том числе использования мной технических средств обработки, передачи и защиты персональных данных.

Об ответственности за разглашение персональных данных предупрежден(а). Мне известно, что нарушение этих требований может повлечь уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

Настоящее обязательство действует в течение всего срока конфиденциальности персональных данных, но не менее 5 лет с момента прекращения трудовых отношений с

ООО «БОРЖОМИ ТЕХ».

« »_____20___г. _____/_____

ФИО (подпись)

Приложение № 2

ПЕРЕЧЕНЬ

должностей работников ООО «БОРЖОМИ ТЕХ», замещение которых предусматривает осуществление обработки персональных данных или осуществление доступа к ним

Структурное подразделение	**Должность работника**
1	2

«_____»______________ 20___ г.

____

(подпись, фамилия лица, ответственного за организацию обработки ПДн)

Приложение № 3

ЖУРНАЛ

учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных ООО «БОРЖОМИ ТЕХ»

№ п/п	Дата поступления обращения	Регистрационный номер (если есть)	Сведения о запрашивающем лице	Цель краткое содержание обращения	Отметка о предоставлении/отказе в предоставлении информации	Дата передачи/отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8	9

Приложение № 4

Отчет
о результатах проведения внутреннего контроля обеспечения защиты персональных данных в информационных системах персональных данных в ООО «БОРЖОМИ ТЕХ»

1. Внутренняя проверка была произведена на основании (годового плана, приказа, распоряжения и т.п.) № __ от «__« __ 20__ года.
Проверка проводилась с «__« __ 20__ года по месту нахождения Общества с ограниченной ответственностью «БОРЖОМИ ТЕХ» по адресу:_____

Проверка проводилась в соответствии со следующими законодательными, нормативными и методическими актами:

Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных» (далее – Федеральный закон «О персональных данных»);

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3. В ходе проведения проверки решались следующие задачи:

определение перечня информационных систем, осуществляющих обработку персональных данных в (наименование организации, гос. органа, гос. органа субъекта, публично-правового образования);

определение границ информационных систем персональных данных;

установление мест и форматов хранения персональных данных;

проведение изучения существующего порядка обработки и защиты персональных данных в информационных системах персональных данных;

составление перечня персональных данных, обрабатываемых в информационных системах персональных данных в (наименование организации, гос. органа, гос. органа субъекта, публично-правового образования);

оценка степени участия сотрудников в обработке персональных данных;

составление перечня используемого оборудования и ПО;

определение состава используемых средств защиты персональных данных;

установление способов обработки персональных данных;

выявление нарушений требований к защите персональных данных.

4. В ходе проверки для каждой информационной системы персональных данных определялось:

состав и структура объектов защиты;

конфигурация и структура информационной системы;

режим обработки информационной системы;

перечень лиц, участвующих в обработке персональных данных;

права доступа лиц, допущенных к обработке персональных данных;

существующие меры защиты персональных данных;

необходимые меры защиты персональных данных.

5. Меры, принятые в (наименование организации, гос. органа, гос. органа субъекта, публично-правового образования) по обеспечению безопасности персональных данных.

6. Выявленные нарушения требований к защите персональных данных.

7. Рекомендации по устранению выявленных нарушений:

"__" _____ 20__ г.

_____

(*подпись, фамилия лица, ответственного за организацию обработки ПДн)*

Приложение № 5

Начат «___» _____ 20__ г.

Окончен «___» _____ 20__ г.

На _____ листах

ЖУРНАЛ

регистрации выявленных нарушений в ООО «БОРЖОМИ ТЕХ»

№	Дата выявления нарушения	Подразделение, где выявлено нарушение и допустившее нарушение лицо (ФИО, должность)	Кем и при каких обстоятельствах выявлено нарушение (жалоба, плановая проверка и т.д.)	Содержание нарушения	Требования, каких нормативных документов нарушены	Корректирующие и предупреждающие действия по устранению нарушения и предотвращению нарушения в дальнейшем	Ответственное за устранение лицо выявленного нарушения лицо (ФИО, должность и его подпись)	Срок устранения нарушения	Отметка о контроле за выполнением (дата, ФИО и должность проверяющего)
1	2	3	4	5	6	7	8	9	10