Политика обработки персональных данных

1. Общие положения

1.1. Настоящей Политикой определяется порядок обработки и защиты персональных данных, установленный у Оператора: **Общество с ограниченной ответственностью «Гравитация», ОГРН: 1152468030098, ИНН: 2465127797, КПП: 246301001, 660100, Красноярский край, г. Красноярск, ул. Чкалова 41, пом. 142** (далее – Оператор).

1.2. Настоящая политика определяет порядок обработки персональных данных на материальных и электронных носителях, а также с использованием средств автоматизации, в том числе посредством обработки персональных данных на Сайта Оператора, размещенном в сети Интернет по адресу (включая все страницы, размещенные на указанном домене): **online.gravity24.ru**.

1.3. Обращения Оператору по вопросам обработки и защиты персональных данных могут быть направлены по адресу места нахождения Оператора, указанному выше, а также по адресу электронной почты **online@gravity24.ru**.

1.4. Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и интересов Оператора, его работников, контрагентов и третьих лиц в связи с необходимостью обработки сведений, составляющих персональные данные.

1.5. Обработка персональных данных осуществляется в соответствии с Федеральным законом от 27.07.2006. №152-ФЗ «О персональных данных» (далее – Закон), иными законами и подзаконными актами Российской Федерации, а также настоящей Политикой.

1.6. Оператор вправе принимать иные локальные нормативные акты (далее – ЛНА), регулирующие порядок обработки и защиты персональных данных Оператором, его работниками и уполномоченными лицами.

1.7. Политика о персональных данных должна быть опубликована на Сайте Оператора, а также может быть доступна для ознакомления неограниченному кругу лиц иными способами, согласованными с Оператором.

1.8. В связи с тем, что приложения к настоящей Политике содержат сведения о технических мерах защиты персональных данных, а также иные сведения, раскрытие которых может снизить уровень защиты персональных данных, доступ к таким приложениям предоставляется

исключительно лицам, в обязанности которых входит работа с соответствующими информационными системами персональных данных.

2. Принципы обработки персональных данных

2.1. Информация, получаемая Оператором, может иметь как материальную, так и электронную форму.

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

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

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

2.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

2.6. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого или выгодоприобретателем, по которому является субъект персональных данных.

2.7. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.8. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

2.8.1. После того как в отношении определенного набора персональных данных будут выполнены требования Закона о локализации, повторная

иди дополнительная локализация таких персональных данных не требуется, в связи с достижением целей, установленных Законом.

2.8.2. Если персональные данные были записаны в базу данных, расположенную на территории Российской Федерации, то впоследствии такие персональные данные могут вноситься Оператором в принадлежащую ему электронную базу данных, находящуюся за пределами Российской Федерации.

2.9. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, включая невозможность использования сервисов Сайта, а также заключения и исполнения сделок с Оператором.

2.10. Работники и/или представители Оператора обязаны соблюдать конфиденциальность обрабатываемых персональных данных, предпринимать все необходимые меры для соблюдения правил обработки персональных данных, предусмотренных настоящей Политикой, а также для обеспечения необходимого уровня защиты персональных данных от неправомерного доступа и иных угроз. В случае возникновения внештатной ситуации или отсутствии информации о необходимых действиях по защите персональных данных, работник обязан обратиться к своему непосредственному руководителю для получения необходимых инструкций и/или пояснений.

3. Основания обработки персональных данных

3.1. Информация об источниках персональных данных указывается в положениях об отдельных информационных системах персональных данных (ИСПД).

3.1.1. Источниками персональных данных могут являться субъект персональных данных, общедоступные источники персональных данных и иные источники, если иное не предусмотрено в положениях об отдельных ИСПД.

3.1.2. Обработка персональных данных, источником которых не является непосредственно субъект персональных данных должна осуществляться в строгом соответствии с действующим законодательством Российской Федерации в области защиты персональных данных.

3.1.3. При получении информации о персональных данных от третьих лиц Оператор должен предпринять возможные меры, а также получить

заверения и гарантии от третьих лиц, предоставляющих информацию, о том, что обработка персональных данных такими лицами осуществляется в строгом соответствии с действующим законодательством.

3.2. Оператор не имеет права получать и обрабатывать персональные данные о расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни субъекта персональных данных, за исключением случаев, когда субъект персональных данных дал свое прямое согласие в письменной форме на обработку указанных персональных данных, а также в случае, если такие персональные данные сделаны общедоступными субъектом персональных данных.

3.3. Обработка персональных данных возможна при наличии согласия субъекта персональных данных на обработку его персональных данных либо без такого согласия в следующих случаях:

3.3.1. Обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей.

3.3.2. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем, 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.

3.3.3. Обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

3.3.4. Обработка персональных данных осуществляется в статистических или иных исследовательских целях (за исключением обработки персональных данных, в целях продвижения товаров, работ и услуг), при условии обязательного обезличивания персональных данных.

3.3.5. Обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

3.3.6. В иных случаях, предусмотренных Законом.

3.4. Соглашаясь с политикой обработки персональных данных, субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

3.4.1. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным.

3.4.2. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

3.5. Обработка персональных данных в целях продвижения товаров, работ и услуг путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта персональных данных. Оператор ведет учет сведений о дате и форме получения согласия субъекта персональных данных на обработку своих данных в вышеназванных целях.

3.6. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных. Требования субъекта персональных данных о прекращении обработки его персональных данных могут быть направлены Оператору посредством запроса в письменной или электронной форме.

3.7. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, прямо указанных в Законе.

4. Обработка куки-файлов (Cookies)

4.1. Настоящее положение также определяет порядок обработки и хранения файлов Cookie (далее – Данные), установленный у Оператора. Данное положение применяется ко всем интернет-страницам, расположенным в домене Сайта.

4.2. Обработка Данных осуществляется с помощью сервисов интернет статистики Яндекс.Метрика https://metrika.yandex.ru, Google Analytics https:// analytics.google.com, рекламных сетей Facebook https://facebook.com и ВКонтакте, https://vk.com, а также иных сервисов.

4.3. Акцептом условий использования Данных являются любые действия Пользователя по использованию Сайта, в том числе первое открытие любой страницы Сайта в браузере на любом устройстве Пользователя.

4.4. Использование Сайта, в том числе его просмотр, поиск информации возможно только при условии полного и безоговорочного принятия условий использования Данных. При несогласии Пользователя с условиями использования данных, Пользователь обязан немедленно прекратить использование Сайта.

4.5. Оператор вправе по своему усмотрению обновлять Положение в отношении файлов cookie. Все изменения будут применяться после публикации новой редакции Положения в отношении файлов cookie на Сайте.

4.6. Обработка данных

4.6.1. Cookie представляет собой файл, который содержит текстовую информацию и сохраняется веб-браузером при посещении Сайта, что позволяет веб-сайту, открытому в браузере, сохранять и определять интернет-активность Пользователя.

4.6.2. Данные используются для обеспечения работы Сайта, отслеживания перемещения Пользователей по Сайту и сохранения аутентификационных данных. На Сайте могут быть использованы следующие типы cookie-файлов:

- Прямые cookie-файлы, которые создаются непосредственно Сайтом, а также сторонние cookie-файлы, которые создаются иными веб-сайтами.
- Обязательные cookie-файлы, которые необходимы для технического обеспечения корректной работы веб-сайта.
- Мониторинговые cookie-файлы, в которых сохраняется информация о работе веб-сайта, включая количество посетителей, проведенное на Сайте время, сообщения об ошибках.
- Функциональные cookie-файлы, которые улучшают работу веб-сайта путем запоминания предпочтений Пользователя, включая языковые, региональные или иные параметры.
- Рекламные cookie-файлы, которые позволяют предлагать персонализированную рекламу.
- Сессионные cookie-файлы являются временными и удаляются при закрытии браузера, а постоянные cookie-файлы остаются на устройстве до тех пор, пока они не будут удалены вручную или автоматически удалены устройством Пользователя.

4.6.3. Сайт может содержать и использовать веб-маячки и аналогичные технологии, которые представляют собой прозрачное изображение размером 1x1 пиксель, которое размещается на Сайте или в электронном письме и помогает анализировать поведение Пользователей.

4.6.4. Файлы cookie могут использоваться для определения Пользователя, при этом Данные ни при каких обстоятельствах не используются для определения личности пользователя и не являются персональными данными.

4.6.5. Некоторые файлы cookie, могут обрабатываться с участием сторонних сервисов и третьих лиц (информационными, рекламными, аналитическими партнёрами), которые могут обрабатывать и объединять файлы cookie, собранные на Сайте, с другой информацией, предоставленной Пользователем и/или собранной с других веб-сайтов.

4.7. Использование Сайта подразумевает полное и информированное согласие Пользователя на обработку Данных Оператором в порядке и на условиях, установленных Положением. Сбор и обработка Данных осуществляются автоматически при использовании Сайта.

4.8. В случае отказа Пользователя от предоставления права использования Данных Оператором, Пользователь вправе в любое время самостоятельно отключить возможность использования файлов Cookie и иных данных о Пользователе, используемом браузере, устройстве, с которого осуществляется использование Сайта, настроить иные параметры использования данных на своем браузере и/или устройстве, а также вправе отказаться от использования Сайта.

4.9. Согласие распространяется на любое действие (операцию) или совокупность действий (операций) включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, распространение, передачу (в том числе трансграничную), блокирование, удаление и уничтожение.

4.10. В настройках браузера Пользователь может установить уведомления об обработке Данных или полностью запретить их обработку. При этом, отключение cookie-файлов может повлиять на корректную работу Сайта.

4.11. Сайт использует сеансовые и постоянные файлы cookie. Сеансовые файлы cookie хранятся временно и удаляются после закрытия браузера. Постоянные файлы cookie сохраняются после завершения сеанса и обрабатываются до момента отзыва согласия Пользователя на обработку Данных.

4.12. Пользователь имеет право получать информацию об обработке Оператором файлов cookie на Сайте; требовать исправления неточных файлов cookie Пользователя; требовать удаления файлов cookie Пользователя; ограничивать обработку файлов cookie при наличии технической возможности и в случае, если это допускается в соответствии с действующим законодательством.

4.13. Данные используются для контроля трафика, анализа использования Сайта и улучшения его работы.

4.14. Пользователям следует принимать во внимание, что третьи лица могут использовать файлы cookie, собранные на Сайте, для иных целей, в частности для настройки предпочтений Пользователя при использовании других сайтов, отображения наиболее релевантной рекламы, оценки активности рекламных кампаний и отслеживания действий Пользователя на других сайтах. Оператор не несет ответственности за действия третьих лиц при использовании Данных на сторонних сайтах.

4.15. Оператор не использует системы автоматического принятия решений при обработке файлов cookie на Сайте.

4.16. Обработка файлов cookie на Сайте может также предполагать обработку таких файлов третьими лицами в случае интеграции сервисов Сайта с сервисами и сайтами третьих лиц.

4.17. Для определения порядка и условий обработки Данных сторонними сайтами и сервисами Пользователю необходимо напрямую связаться с соответствующими операторами данных.

4.18. Оператор вправе осуществлять интеграцию сторонних сервисов на Сайт, в результате чего, обработка собранных cookie-файлов будет осуществляться третьими лицами в порядке и на условиях, определяемых такими лицами.

4.19. В связи с вышеизложенным обработка файлов cookie может осуществляться за пределами страны Пользователя.

5. Передача персональных данных

5.1. При передаче персональных данных Оператор должен соблюдать следующие требования:

5.1.1. Не сообщать персональные данные субъекта персональных данных в коммерческих целях без согласия субъекта персональных данных.

5.1.2. Предупредить лиц, получивших персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц заверений о том, что это правило соблюдено. Лица, получившие персональные данные субъекта персональных данных, обязаны соблюдать режим конфиденциальности.

5.1.3. Разрешать доступ к персональным данным субъекта персональных данных только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

5.2. Оператор вправе поручить обработку персональных данных другому лицу на основании заключаемого с этим лицом договора.

5.2.1. Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом.

5.2.2. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных.

5.3. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5.4. В случае, если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед Оператором.

6. Порядок обработки персональных данных

6.1. Обработка персональных данных, содержащихся в ИСПД либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), 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. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в ИСПД либо были извлечены из нее.

6.2. При обработке персональных данных Оператором не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6.3. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных.

6.4. Уничтожение и/или блокирование персональных данных может производиться любым способом, исключающим дальнейшую обработку этих персональных данных, в том числе путем физического уничтожения материальных носителей и безвозвратного удаления данных с электронного носителя без возможности восстановления таких данных.

6.5. Уничтожение и/или блокирование персональных данных осуществляются лицом, ответственным за защиту соответствующей ИСПД.

6.6. Уточнение персональных данных производится путем обновления или изменения данных на соответствующем носителе. Если такой порядок не допускается техническими особенностями носителя, то уточнение персональных данных осуществляется путем фиксации на том же носителе сведений о вносимых изменениях либо путем изготовления нового носителя с уточненными персональными данными.

6.7. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Оператором.

7. Защита персональных данных

7.1. Оператор принимает необходимые правовые, организационные и технические меры и обеспечивает их обновление 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.

7.1.1. Осуществление организационных и правовых мер по защите персональных данных и установлению порядка обработки персональных данных Оператором осуществляется лицом, уполномоченным руководителем Оператора.

7.1.2. Осуществление технических и иных мер по защите персональных данных, содержащихся в отдельных ИСПД, осуществляется лицом, уполномоченным руководителем Оператора соответствующим приказом.

7.1.3. Перечень лиц, имеющих право доступа к отдельным ИСПД устанавливается в журналах учета (перечнях) лиц, имеющих соответствующий доступ.

7.1.4. Право доступа к персональным данным также может быть предоставлено иным лицам, перечисленным в журнале лиц, имеющих доступ к персональным данным.

7.1.5. Порядок хранения материальных и электронных носителей персональных данных и ИСПД, а также перечень обрабатываемых персональных данных и цели обработки персональных данных устанавливаются в положениях об отдельных ИСПД.

7.2. Обработка персональных данных должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных и установить перечень лиц, осуществляющих обработку персональных данных и лиц, имеющих доступ к персональным данным.

7.3. Оператор ведет перечни действующих локальных нормативных актов, ИСПД, а также перечни лиц, ответственных за защиту персональных данных, и лиц, имеющих доступ к ИСПД, а также иные перечни, при наличии необходимости ведения соответствующего учета. Ведение перечней может осуществляться в электронном виде и/или на материальных носителях.

7.4. Лицо, ответственное за организацию обработки персональных данных обязано:

7.4.1. Организовывать работу Оператора по разработке и принятию организационно-распорядительных документов, регламентирующих деятельность по обработке и защите персональных данных, поддержанию их в актуальном состоянии;

7.4.2. Организовывать принятие Оператором правовых, организационных и технических мер для защиты персональных данных;

7.4.3. Проводить инструктаж работников в соответствии с Инструкцией по проведению инструктажа лиц, допущенных к работе с информационными системами персональных данных;

7.4.4. Осуществлять внутренний контроль за соблюдением работниками организации законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, а также инициировать проведение служебных расследований по фактам нарушения установленных правил обработки и защиты персональных данных;

7.4.5. Представлять интересы Оператора при проверках надзорных органов в сфере обработки персональных данных, а также организовывать прием и обработку обращений субъектов персональных данных.

7.5. Лицо, ответственное за обеспечение безопасности отдельной информационное системы персональных данных обязано:

7.5.1. Обеспечить применение технических мер защиты персональных данных, сохранность и резервное копирование данных, а также обеспечивать функционирование и безопасность средств защиты информации;

7.5.2. Контролировать выполнение установленных правил обеспечения защиты персональных данных лицами, допущенными к обработке персональных данных в соответствующей ИСПД;

7.5.3. Инициировать проведение служебных расследований по фактам нарушения установленных правил обеспечения защиты персональных данных, несанкционированного доступа к персональным данным;

7.5.4. Контролировать и обеспечивать правомерный доступ к ИСПД, контролировать доступ в помещения с носителями ИСПД, обеспечить доступ к защищаемой информации всем группам пользователей ИСПД согласно их правам доступа при получении оформленного

соответствующим образом разрешения, а также не допускать к работе на элементах ИСПД посторонних лиц.

8. Общие меры по защите персональных данных

8.1. Состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей Оператора по защите персональных данных включает следующие обязанности:

8.1.1. Утверждение перечня ИСПД и назначение лиц, ответственных за организацию обработки и защиты персональных данных;

8.1.2. Издание документов, определяющих политику Оператора в отношении обработки персональных данных, а также издание локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства и устранение последствий таких нарушений;

8.1.3. Применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

8.1.4. Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

8.1.5. Оценка вреда, который может быть причинен субъектам персональных данных, соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей по защите персональных данных;

8.1.6. Ознакомление и/или обучение лиц, непосредственно осуществляющих обработку персональных данных.

8.2. Обеспечение безопасности персональных данных достигается, в частности:

8.2.1. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

8.2.2. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение

которых обеспечивает установленные уровни защищенности персональных данных.

8.2.3. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, а также учетом носителей персональных данных.

8.2.4. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

8.2.5. Обнаружением фактов несанкционированного доступа к персональным данным и принятием мер.

8.2.6. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

8.2.7. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

8.2.8. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

8.3. Оператор обеспечивает неограниченный доступ к документам, определяющим его политику в отношении обработки персональных данных, а также к сведениям о реализуемых требованиях к защите персональных данных путем размещения таких документов на Сайте, в месте своего нахождения и/или иным образом.

9. Порядок применения мер по защите данных

9.1. 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.

9.2. Мероприятия по защите персональных данных осуществляются на регулярной и систематичной основе. Регулярность и систематичность подразумевает осуществление мероприятий по мере необходимости, но не реже одного раза в каждом календарном году.

9.3. Для защиты персональных данных и предотвращения несанкционированного доступа к персональным данным применяются следующие организационные меры защиты:

9.3.1. Доступ к носителям ИСПД допускается только для лиц, в обязанности которых входит обработка персональных данных, с обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПД.

9.3.2. Персональные данные, обрабатываемые при помощи материальных носителей, хранятся в запирающихся шкафах, в помещениях, доступ к которым может быть ограничен для определенного круга лиц. Обеспечивается контроль доступа к персональным данным.

9.3.3. Сохранность персональных данных, обрабатываемые при помощи вычислительной техники, обеспечивается средствами программного обеспечения, в т.ч. путем предоставления доступа к персональным данным только после ввода логина и пароля соответствующего лица, у которого есть доступ к персональным данным или иным способом, обеспечивающим контроль доступа к персональным данным.

9.3.4. Оператор ведет учет, хранения и обращения носителей, содержащих информацию с персональными данными.

9.3.5. На регулярной основе, но не реже одного раза в год, осуществляется проведение мероприятий по определению угроз безопасности персональных данных при их обработке и формирование моделей угроз.

9.3.6. На постоянной основе осуществляется контроль доступа в целях обнаружения фактов несанкционированного доступа к персональным данным.

9.3.7. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится Оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, осуществляющих деятельность по технической защите конфиденциальной информации. Регулярность проведения проверки устанавливается руководителем Оператора по мере необходимости, но в любом случае не реже одного раза в год.

9.3.8. Меры по контролю (анализу) защищенности персональных данных проводятся на регулярной основе и обеспечивают контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и

тестированию работоспособности системы защиты персональных данных.

9.3.9. Меры по выявлению инцидентов и реагированию на них включают обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов лицами, ответственными за защиту соответствующих персональных данных.

9.3.10. Оператор осуществляет организацию пропускного режима на территорию Общества, а также контроль доступа в помещения с техническими средствами обработки персональных данных.

9.3.11. Постоянный доступ в помещения, в которых осуществляется обработка персональных данных, имеют лица, непосредственно осуществляющие обработку персональных данных в соответствующей информационной системе. Лица, не осуществляющие обработку персональных данных, имеют допуск в указанные помещения только в присутствии лица, ответственного за защиту соответствующих ИСПД.

9.4. Правовые меры защиты персональных данных включают:

9.4.1. Включение в договоры с контрагентами положений, гарантирующих защиту персональных данных контрагентами Оператора, в случае, если в рамках таких договоров осуществляется обработка персональных данных.

9.4.2. Оператор разрабатывает и регулярно обновляет необходимые локальные нормативные акты, и издает приказы в области защиты персональных данных.

9.4.3. Оператор назначает, а также ведет систематический контроль и учет лиц, ответственных за защиту персональных данных, а также учет лиц, имеющих доступ к ИСПД.

9.5. В состав технических мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят следующие меры:

9.5.1. Оператор регулярно осуществляет проверку готовности и эффективности использования средств защиты информации, разграничение доступа пользователей к информационным ресурсам и программно-аппаратным средствам обработки информации, а также регистрацию и учет действий пользователей информационных систем персональных данных.

9.5.2. Оператором осуществляет использование антивирусных средств и средств восстановления системы защиты персональных данных, применение средств межсетевого обнаружения вторжений, анализа защищенности и средств криптографической защиты информации. Используемое программное обеспечение допускает восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

9.5.3. Меры по идентификации и аутентификации субъектов доступа и объектов доступа обеспечивают присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора.

9.5.4. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

9.5.5. Меры по ограничению программной среды обеспечивают установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения и/или исключают возможность установки и (или) запуска запрещенного программного обеспечения.

9.5.6. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) исключают возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

9.5.7. Меры по регистрации событий безопасности обеспечивают сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

9.5.8. Меры по антивирусной защите обеспечивают обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств

защиты информации, а также реагирование на обнаружение этих программ и информации.

9.5.9. Меры по обнаружению (предотвращению) вторжений обеспечивают обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

9.5.10. Меры по обеспечению целостности ИСПД обеспечивают обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

9.5.11. Меры по обеспечению доступности персональных данных обеспечивают авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

9.5.12. Меры по защите среды виртуализации исключают несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

9.5.13. Меры по защите технических средств исключают несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены.

9.5.14. Меры по защите информационной системы, ее средств, систем связи и передачи данных обеспечивают защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-

телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

9.5.15. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных обеспечивают управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

9.6. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

9.6.1. Определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных;

9.6.2. Адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

9.6.3. Уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

9.6.4. Дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

9.7. При невозможности реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на

нейтрализацию актуальных угроз безопасности персональных данных. В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

10.Правила осуществления контроля и аудита

10.1. Настоящий раздел устанавливает порядок осуществления внутреннего контроля и (или) аудита соответствия обработки персональных данных Закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

10.2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Оператор организует проведение регулярных проверок условий обработки персональных данных (не реже одного раза в год).

10.3. Проверки осуществляются лицом, ответственным за организацию обработки персональных данных, либо, если такое лицо посчитает необходимым, комиссией, образуемой руководителем Оператора. Состав комиссии определяется лицом, ответственным за организацию обработки персональных данных Оператора.

10.4. Срок осуществления внутреннего контроля не должен превышать 5 рабочих дней с даты начала проверки, если иной срок не потребуется для проведения надлежащего контроля.

10.5. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, составляется Акт проверки, который в течение направляется руководителю Оператора.

11.Правила проведения оценки потенциального вреда

11.1. Настоящий раздел устанавливает порядок проведения оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона, а также оценки соотношения указанного вреда и принимаемых оператором мер, направленных на защиту персональных данных.

11.2. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

11.3. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

11.3.1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;

11.3.2. Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;

11.3.3. Неправомерное изменение персональных данных является нарушением целостности персональных данных;

11.3.4. Нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации;

11.3.5. Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;

11.3.6. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объеме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных;

11.3.7. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;

11.3.8. Принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

11.4. Субъекту персональных данных может быть причинен вред в форме:

11.4.1. Убытков - расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

11.4.2. Морального вреда - физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

11.5. В оценке возможного вреда Оператор исходит из следующего способа учета последствий допущенного нарушения принципов обработки персональных данных:

11.5.1. Низкий уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;

11.5.2. Средний уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;

11.5.3. Высокий уровень возможного вреда - во всех остальных случаях.

11.6. Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых Оператором мер:

11.6.1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным за организацию обработки персональных данных.

11.6.2. Состав и перечень инструментов оценки потенциального вреда определяется лицом, ответственным за организацию обработки персональных данных на основании доступной практики и доступных статистических данных.

12.Правила ознакомления и обучения работников

12.1. Настоящий раздел политики устанавливает порядок ознакомления работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

12.2. Ознакомление работников с действующими локальными нормативными актами в области защиты персональных данных осуществляется в общем порядке ознакомления работников Оператора с локальными нормативными актами, действующими в организации.

12.3. Обучение работников осуществляется по мере необходимости актуализации знаний и навыков в области защиты персональных данных. Решение о необходимости проведения обучения принимается лицом, ответственным за организацию обработки персональных данных.

12.4. Оператор разрабатывает типовые положения и обязанности о защите персональных данных и включает такие положения в должностные инструкции работников, осуществляющих обработку персональных данных.

12.5. Оператор разрабатывает проект типового обязательства работника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей.

12.6. Оператор вправе издавать и утверждать иные инструкции по проведению контроля и инструктажу работников в области защиты персональных данных.

13. Ответственность за нарушение порядка обработки персональных данных

13.1. Работники Оператора, ответственные за обработку и защиту персональных данных, а также иные лица, получившие доступ к персональным данным, обязаны предпринимать все возможные меры по сохранению конфиденциальности персональных данных и предотвращению их разглашения.

13.2. В случае утраты лицом права доступа к соответствующей ИСПД по любой причине (прекращение договора, распорядительный акт оператора, требование субъекта персональных данных и т.д.), такое лицо обязано незамедлительно прекратить обработку персональных данных, а также возвратить непосредственному руководителю все ИСПД и средства доступа к ИСПД, находящиеся в распоряжении такого лица.

13.3. Лица, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

13.4. За нарушение порядка обращения с персональными данными ответственное лицо несет ответственность, предусмотренную законом, а также возмещает ущерб, причиненный неправомерным использованием информации, содержащей персональные данные.

14.Обращения субъектов персональных данных

14.1. Субъект персональных данных вправе направлять Оператору свои запросы и требования (далее – Обращение), в том числе относительно использования его персональных данных.

14.2. Обращение может быть направлено в письменной форме или в форме электронного документа. Документ должен быть направлен с адреса электронной почты, указанного субъектом при регистрации на Сайте или в договоре.

14.3. Субъект персональных данных вправе в любое время отозвать согласие на обработку его персональных данных.

14.4. Обращение должно содержать сведения о документе, удостоверяющем личность субъекта персональных данных или его представителя; сведения о договорных или иных законных отношениях с Оператором (в частности, логин и пароль на Сайте); Суть обращения; Подпись субъекта персональных данных или его законного представителя.

14.5. Оператор регистрирует поступление обращения и проверяет наличие всех обязательных реквизитов Обращения. При отсутствии в Обращении обязательных реквизитов Оператор вправе запросить дополнительные сведения, необходимые для идентификации субъекта персональных данных. По результатам рассмотрения надлежащего обращения, Оператор направляет ответ в форме, аналогичной поступившему обращению. Срок ответа на обращение не должен превышать 30 календарных дней, если иной срок прямо не предусмотрен действующим законодательством для отдельных видов обращений.

15.Заключительные положения

15.1. Настоящий локальный нормативный акт утверждается руководителем Оператора и вступает в силу с момента его утверждения.

15.2. Ознакомление работников с настоящим документом осуществляется в общем порядке, предусмотренном для ознакомления работников Оператора с локальными нормативными актами, действующими в организации, а также путем опубликования настоящего документа в открытом доступе для неограниченного круга лиц.

15.3. Правила рассмотрения запросов субъектов персональных данных или их представителей могут быть установлены в соответствующих положениях об ИСПД.