Дата публикации 12.04.2026г.

ПОЛИТИКА

В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

ООО «Мира Ретрит»

1. Общие положения

1.1. Настоящая Политика Общества с ограниченной ответственностью «Мира Ретрит» в отношении обработки персональных данных (далее - Политика) разработана во исполнение требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) в целях обеспечения 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. Настоящая Политика определяет основные принципы, цели, условия и способы обработки Персональных данных, права и обязанности общество с ограниченной ответственностью «Мира Ретрит» при обработке Персональных данных, права Субъектов Персональных данных, а также реализуемые в общество с ограниченной ответственностью «Мира Ретрит» меры по обеспечению безопасности Персональных данных при осуществлении установленных в Уставе видов деятельности.

1.2. Политика действует в отношении всех персональных данных, которые обрабатывает общество с ограниченной ответственностью «Мира Ретрит» (далее - Оператор, ООО «Мира Ретрит»).

1.3. Политика распространяется на отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящей Политики.

1.4. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных, в том числе для обеспечения неограниченного доступа к Политике, настоящая Политика публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на сайтах Оператора **https://miraretrit.ru, pilotsacademy.ru**

1.5. Положения настоящей Политики служат основой для разработки локальных актов, регламентирующих в ООО «Мира Ретрит» вопросы обработки Персональных данных.

1.6. Нормативные ссылки

- Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»).

- Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».

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

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

1.7. Действие настоящей Политики распространяется на все процессы Оператора, в рамках которых осуществляется обработка Персональных данных, как с использованием средств вычислительной техники, в том числе с использованием информационно-телекоммуникационных сетей, так и без использования таких средств, с учетом положений п. 1.2. настоящей Политики.

2. Термины и принятые сокращения

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (Субъекту Персональных данных), в том числе фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, должность, профессия, доходы, изображение, номер телефона и/или адрес электронной почты Субъекта Персональных данных, данные, автоматически передаваемые Оператору с помощью установленного на устройстве Субъекта Персональных данных программного обеспечения (при условии, что на основании этих данных можно идентифицировать Субъекта), в том числе IP-адрес, индивидуальный сетевой номер устройства, полученные Оператором в результате договорных или иных гражданско-правовых отношений с третьими лицами, а также при осуществлении Оператором хозяйственной деятельности (в том числе, Персональные данные Работника и/или Контрагента).

Субъект Персональных данных (Субъект) — физическое лицо, обладающее Персональными данными прямо или косвенно его определяющими.

Информационная система Персональных данных или ИСПДн — совокупность содержащихся в базах данных Персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Сервисы ООО «Мира Ретрит» — совокупность программных продуктов ООО «Мира Ретрит», объединяющих в своем составе Веб-сайт, Справочники организаций, базы данных, и т.д.;

Веб-сайты Оператора (Сайт) - совокупность графических и информационных материалов, а также программ для ЭВМ и баз данных, обеспечивающих их доступность в сети интернет по сетевому адресу https://miraretrit.ru, pilotsacademy.ru

PWA (Прогрессивное Веб-Приложение) «Путь к себе» — это технология, которая превращает веб-сайт в мобильное приложение, сохраняя его на главном экране устройства для быстрого доступа. PWA объединяют лучшие черты веб-сайтов и мобильных приложений, предлагая быструю работу, работу офлайн, пуш-уведомления и интуитивно понятный интерфейс.

Пользователь Веб-сайта/Веб-Приложения – дееспособное физическое лицо, использующее или намеревающееся использовать Веб-сайта/Веб-Приложение.

Оператор персональных данных (Оператор) – ООО «Мира Ретрит», самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с Персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с Персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение Персональных данных.

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

Распространение Персональных данных — действия, направленные на раскрытие Персональных данных неопределенному кругу лиц.

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

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 становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

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

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Иные данные — данные, не являющиеся Персональными данными и необходимые для функционирования Сервисов Оператора.

Работник — физическое лицо, находящееся в трудовых отношениях с Оператором.

Соискатели — кандидаты на замещение вакантных должностей.

Контрагент — юридическое лицо, индивидуальный предприниматель, физическое лицо, заключившее или собирающееся заключить с Оператором какой-либо договор (соглашение) в своем интересе или от имени и в интересах представляемого им юридического лица / индивидуального предпринимателя / физического лица в соответствии с требованиями действующего законодательства.

Партнеры под брендом «Мира» — это физические и юридические лица, осуществляемые свою деятельность под брендом «Мира» на основании предоставленных им Правообладателем прав на использование изобразительного товарного знака и/или логотипа и/или разделяющие ценности бренда «Мира» (Приложение №2 к настоящей Политике).

Иные Партнеры — это физические и юридические лица, предоставляющие Оператору услуги (Приложение №2 к настоящей Политике).

3. Принципы и цели обработки персональных данных

3.1. При организации обработки Персональных данных Субъектов Персональных данных Оператор руководствуется принципами обработки персональных данных, предусмотренными ст. 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.2. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным в настоящей Политики. Обрабатываемые

персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.3. Для каждой цели обработки персональных данных определены цели обработки Персональных данных, категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных.

3.4. Ведение внутреннего реестра процессов обработки персональных данных, содержащий информацию о целях обработки персональных данных, категориях и перечне обрабатываемых персональных данных, категориях субъектов, персональные данные которых обрабатываются, способах, сроках их обработки и хранения, порядке уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований. Реестр регулярно актуализируется и обновляется владельцами процессов через лицо, ответственное за организацию обработки Персональных данных.
3.5. Информация в Реестре процессов используется для:
- разработки или актуализации внутренних локальных документов, связанных с обработкой и защитой персональных данных.;
- направления Уведомления или Информационного письма в Роскомнадзор;
- разработки внутренних нормативных документов Компании;
- проведения внутренних аудитов процессов обработки и защиты Персональных данных;
- в иных целях, связанных с обработкой и защитой персональных данных.

4. Порядок и условия обработки персональных данных

4.1. Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.

4.2. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

4.3. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

4.4. Согласие на обработку Персональных данных может быть отозвано Субъектом Персональных данных на основании его письменного запроса, направленного в том числе посредством электронной связи на адрес электронной почты, указанный в согласии на обработку персональных данных, а при отсутствии такового на адрес электронной почты o.hvorostyan@miraretrit.ru

4.5. Оператор осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.

4.6. К обработке персональных данных допускаются работники Оператора, в должностные обязанности которых входит обработка персональных данных.

4.7. Обработка персональных данных осуществляется путем:

- получения персональных данных в устной и письменной форме непосредственно с согласия субъекта персональных данных на обработку или распространение его персональных данных;
- получения персональных данных из общедоступных источников;
- внесения персональных данных в журналы, реестры и информационные системы Оператора;
- использования иных способов обработки персональных данных.

4.8. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

4.9. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд, Фонд социального страхования и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

4.10. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий.

4.11. Оператор осуществляет хранение персональных данных 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 или соглашением.

4.12. При сборе персональных данных, в том числе посредством информационно телекоммуникационной сети интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

4.13. Хранение Персональных данных.

4.13.1. Персональные данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.13.2. Персональные данные, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа.

4.13.3. Персональные данные субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках. Персональные данные Субъектов преимущественно хранятся на электронных носителях в электронном виде в персональных компьютерах, подключенных к локальной компьютерной сети Оператора. Доступ к электронным базам данных ограничен паролем.

4.13.4. Не допускается хранение и размещение документов, содержащих Персональные данные, в открытых электронных каталогах (файлообменниках).

4.13.5. Доступ к бумажным и электронным носителям Персональных данных получают только те Работники, которым это необходимо для выполнения их должностных обязанностей.

4.13.6. Хранение Персональных данных в форме, позволяющей определить субъекта Персональных данных, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.13.7. Оператор обеспечивает необходимые организационные и технические меры для защиты Персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения Персональных данных, а также от иных неправомерных действий.

4.13.8. Возможна передача Персональных данных Субъектов по внутренней сети Оператора с использованием технических и программных средств защиты информации,

с доступом только для Работников, допущенных к работе с Персональными данными Субъектов и только в объеме, необходимом данным Работникам для выполнения своих должностных обязанностей.

4.13.9. Подразделения Оператора, осуществляющие кадровое делопроизводство, ведут личные дела Работников, в которых содержатся Персональные данные Работников и иные сведения, связанные с трудовой деятельностью Работников. Наряду с копиями документов и личными заявлениями к личному делу Работника приобщается анкета, заполненная Работником. Личные дела, трудовые договоры и трудовые книжки Работников хранятся в помещениях кадровых служб в несгораемых шкафах (сейфах). Ответственность за хранение указанных документов возлагается на руководителя кадрового подразделения.

4.13.10. Доступ к Персональным данным Субъектов имеют Работники Оператора, допущенные к работе с Персональными данными Субъектов. С данными категориями работников подписывается соглашение о неразглашении персональных данных.

4.13.11.Доступ к Персональным данным предоставляется Работнику Оператора в соответствии с приказом о назначении должностных лиц, которым необходим доступ к Персональным данным в целях выполнения их функциональных обязанностей, утвержденным Директором ООО «Мира Ретрит». В приложении к указанному приказу определен перечень должностей, непосредственно использующих Персональные данные в служебных целях, которые имеют право обрабатывать только те Персональные данные, которые необходимы им для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц.

4.13.12. При осуществлении доступа работника к информационным системам / базам данных ему должен быть предоставлен минимальный набор прав доступа в рамках закрепленной за пользователем роли. В информационных системах реализуется контроль доступа пользователя к Персональным данным.

4.13.13. Работники Оператора, получающие Персональные данные, обязаны: выполнять требования настоящей Политики; пресекать действия других лиц, которые могут привести к разглашению Персональных данных; использовать Персональные данные только в целях выполнения функциональных обязанностей; использовать в своей работе лишь те Персональные данные, которые действительно необходимы для полноценного выполнения функциональных обязанностей; документы, содержащие Персональные данные, во время работы располагать так, чтобы исключить возможность ознакомления с ними других лиц; об утрате или недостаче документов, содержащих Персональные данные, немедленно сообщать своему непосредственному руководителю; в случае увольнения сдать непосредственному руководителю все служебные документы, содержащие Персональные данные (бумажные, электронные носители), которые находились в его распоряжении в связи с выполнением функциональных обязанностей во время работы у Оператора.

4.13.14. Субъект Персональных данных, данные о котором обрабатываются у Оператора, имеет право на свободный доступ к своим Персональным данным, получение копий своих Персональных данных (за исключением случаев, предусмотренных федеральным законом) на основании его письменного запроса.

4.14. Уничтожение Персональных данных.

4.14.1. Персональные данные хранятся в течение срока, определенного в Приложении №1 к настоящей Политики, и подлежат уничтожению по достижении целей обработки, истечения срока или в случае утраты необходимости в их достижении.

4.14.2. Документы, содержащие Персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном настоящей Политикой и архивным законодательством Российской Федерации.

4.14.3. Уничтожение документов, содержащих Персональные данные, производится:

- в случае отзыва согласия Субъекта Персональных данных, если отсутствуют иные законные основания обработки Персональных данных;
- по достижении целей их обработки или при утрате необходимости в их достижении;
- по достижении окончания срока хранения Персональных данных;
- истек срок согласия на обработку Персональных данных;
- в случае выявления неправомерной обработки Персональных данных.

4.14.4. Уничтожение Персональных данных осуществляется согласно Приказа Роскомнадзора от 28.10.2022г. № 179 «Об утверждении требований к подтверждению уничтожения Персональных данных». Факт уничтожения Персональных данных подтверждается документально актом об уничтожении носителей.

4.14.5. Уничтожение Персональных данных на бумажном носителе осуществляется путем дробления (измельчения). Для уничтожения бумажных документов допускается применение шредера.

4.14.6. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.15. Блокирование Персональных данных.

4.15.1. Блокирование Персональных данных конкретного Субъекта Персональных данных должно осуществляться во всех информационных системах Персональных данных Оператора, содержащих такие Персональные данные.

4.15.2. Блокирование Персональных данных в осуществляется:

- в случае выявления неправомерной обработки Персональных данных при обращении/направлении запроса Субъекта Персональных данных или его представителя либо уполномоченного органа по защите прав Субъектов Персональных данных с момента такого обращения или получения указанного запроса на период проверки;

- в случае отсутствия возможности уничтожения Персональных данных в установленные сроки до их уничтожения.

4.15.3. После устранения выявленной неправомерной обработки Персональных данных Оператора осуществляет снятие блокирования Персональных данных. Решение о блокировании и снятии блокирования Персональных данных принимается лицом, ответственным за организацию обработки Персональных данных Оператора.

5. Передача персональных данных

5.1. При передаче Персональных данных Субъекта Оператор обязан соблюдать следующие требования:

- не сообщать Персональные данные Субъекта третьей стороне без надлежащего согласия Субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта, а также в случаях, предусмотренных действующим законодательством;

- не сообщать Персональные данные Субъекта в коммерческих целях без его надлежащего согласия;

- передавать Персональные данные Субъекта представителям Субъекта в порядке, установленном действующим законодательством, и ограничивать эту информацию только

теми Персональными данными Субъекта, которые необходимы для выполнения указанными представителями их функций;

- предупредить лиц, получающих Персональные данные Субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

5.2. Лица, получающие Персональные данные Субъекта, обязаны соблюдать требования конфиденциальности.

5.3. Передача Персональных данных Субъектов третьим лицам осуществляется Оператором только с их надлежащего согласия, за исключением случаев, если:

- передача необходима для защиты жизни и здоровья Субъекта, либо других лиц и получение его согласия невозможно;

- по запросу органов дознания, следствия и суда в связи с проведением расследования или судебным разбирательством;

- в иных случаях, прямо предусмотренных федеральными законами.

5.4. Все меры конфиденциальности при сборе, обработке и хранении Персональных данных Субъекта распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

5.5. В случае если Оператор пользуется услугами третьих лиц на основании заключенных договоров (либо иных оснований), и в силу данных договоров они должны иметь доступ к Персональным данным, обрабатываемым Оператором, то соответствующие Персональные данные предоставляются Оператору только после подписания с данными лицами соглашения о неразглашении Персональных данных или включения в договоры пунктов о неразглашении Персональных данных, в том числе предусматривающих защиту Персональных данных.

5.6. Лицо, осуществляющее обработку персональных данных по поручению Оператора должно соответствовать требованиям, предусмотренным Федеральным закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». В поручении должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных по поручению Оператора, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Федеральным закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», обязанность по запросу Оператора в течение срока действия поручения, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Оператора требований, настоящего пункта, обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных», в том числе требование об уведомлении Оператора о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона «О персональных данных».

6. Обеспечение защиты персональных данных

6.1. Методы и способы защиты Персональных данных в информационных системах Оператора должны соответствовать требованиям, установленным: •Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

•Постановлением Правительства Р Ф от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах Персональных данных»;
• Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
• Иным требованиям законодательства о персональных данных.
6.2. При обработке Персональных данных должны приниматься необходимые правовые, организационные и технические меры 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.

Обмен Персональными данными при их обработке в информационных системах Персональных данных осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

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

Для осуществления мероприятий по защите Персональных данных при их обработке в информационных системах Персональных данных системы защиты могут включать в себя следующие подсистемы: управления доступом; регистрации и учета; обеспечения целостности; антивирусной защиты; обеспечения безопасности межсетевого взаимодействия; анализа защищенности; обнаружения вторжений.

6.3. Основными мерами защиты Персональных данных, используемыми Оператором, являются:

- разработано и утверждено Положение об обработке персональных данных Оператора.

- разработка политики в отношении обработки персональных данных;

- назначение лица, ответственного за обработку Персональных данных, которое осуществляет организацию обработки Персональных данных, внутренний контроль за соблюдением Оператора и его работниками требований к защите Персональных данных;

- оценен вред, который может быть причинен Субъекту персональных данных в случае нарушения законодательства РФ в области персональных данных, оценено соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения законодательства РФ в области персональных данных;

- проводится ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ в области персональных данных, в том числе с 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;

- определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

- установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

- антивирусное программное обеспечение.

- соблюдение условий, обеспечивающих сохранность Персональных данных и исключающих несанкционированный к ним доступ;

- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

- восстановление Персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

- проводится оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных;

- учетом машинных носителей персональных данных;
- осуществляется установление 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;
- осуществляется контроль принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

6.4. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем применения электронной подписи, используются антивирусные средства защиты информации, межсетевое экранирование, присвоение персональных паролей для каждого рабочего места (конкретного работника), наличие средств восстановления системы защиты персональных данных. Установлены сейфы для хранения личных дел работников и персональных данных физических лиц, запирающиеся металлические шкафы, установлена пожарная сигнализация, видеонаблюдение.

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

6.6. Обеспечение сохранности носителей персональных данных.

6.7. Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

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

6.9. Обеспечено раздельное хранение материальных носителей персональных данных, обработка которых осуществляется в различных целях. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

6.10. Ответственность за организацию защиты Персональных данных в информационных системах Персональных данных возлагается на Информационно-технический отдел.

7. Основные права субъекта Персональных данных и обязанности Оператора

7.1. Основные права субъекта Персональных данных.

7.1.1. Субъект имеет право на свободный доступ к его персональным данным и следующим сведениям:

- подтверждение факта обработки Персональных данных Оператором;

- правовые основания и цели обработки Персональных данных;

- цели и применяемые Оператором способы обработки Персональных данных;

- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к Персональным данным или которым могут быть раскрыты Персональные данные на основании договора с Оператором или на основании федерального закона;

- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом Персональных данных прав, предусмотренных настоящим Федеральным законом;

- наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку Персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

7.1.2. Обращение к Оператору и направление ему запросов;

7.1.3. Обжалование действий или бездействия Оператора.

7.2. Обязанности Оператора.

Оператор обязан:

- за свой счет обеспечить защиту Персональных данных Субъекта от неправомерного их использования или утраты в порядке, установленном законодательством РФ;

- при сборе Персональных данных предоставить информацию об обработке Персональных данных;

- в случаях если Персональных данных были получены не от субъекта Персональных данных, уведомить субъекта;

- при отказе в предоставлении Персональных данных субъекту разъясняются последствия такого отказа;

- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки Персональных данных, к сведениям о реализуемых требованиях к защите Персональных данных;

- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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;

- давать ответы на запросы и обращения субъектов Персональных данных, их представителей и уполномоченного органа по защите прав субъектов Персональных данных.

7.3. Система защиты Персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности Персональных данных и информационных технологий, используемых в информационных системах в соответствии с Постановлением Правительства Р Ф от 01 ноября 2012 г. № 1119

«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
7.4. Обработка, уточнение, уничтожение или блокирование Персональных данных Субъектов при осуществлении их обработки без использования средств автоматизации осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». Для обеспечения безопасности Персональных данных Субъектов при неавтоматизированной обработке Оператором предпринимаются следующие меры:
- определяются места хранения Персональных данных Субъектов, которые оснащаются следующими средствами защиты:
- в кабинете соответствующего департамента находятся специально оборудованные шкафы, защищенные от несанкционированного доступа;
- помещения Оператора находятся под круглосуточной охраной сотрудников ЧОП;
- все действия по обработке Персональных данных Субъектов осуществляются только Работниками Оператора, надлежащим образом допущенными к работе с Персональными данными Субъектов, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.
7.5. Для обеспечения безопасности Персональных данных Субъектов Оператором при автоматизированной обработке предпринимаются следующие меры:
- Все действия при автоматизированной обработке Персональных данных Субъектов осуществляются только Работниками Оператора, занимающим должности, указанные в списке должностей, утвержденном соответствующим приказом, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.
- Персональные компьютеры, в которых содержатся Персональные данные Субъектов, защищены паролями доступа. Пароли устанавливаются сотрудником Информационно-технического отдела Оператора и сообщаются индивидуально Работнику, допущенному к работе с Персональными данными и осуществляющему обработку Персональных данных Субъектов на данном персональном компьютере.
- Обработка Персональных данных при автоматизированной обработке Персональных данных осуществляется с соблюдением порядка, предусмотренного Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
7.6. Оператор осуществляет регулярный мониторинг изменений законодательства о персональных данных и в случае необходимости осуществляет информирование работников о соответствующих изменениях.

8. Требования к согласию на обработку персональных данных

8.1. Согласие на обработку персональных данных должно отвечать требованиям:
- должно быть конкретным, информированным, сознательным, предметным и однозначным;
- может быть дано Субъектом или его представителем в любой позволяющей подтвердить факт его получения форме, если законодательством РФ не установлена обязанность получать согласие в письменной форме;
- должно быть дано свободно, своей волей и в своем интересе.
8.2. Оператор персональных данных, обязан получать согласие Субъекта в письменной форме в следующих случаях:
- включение персональных данных Субъекта в общедоступные источники персональных данных;
- обработка биометрических персональных данных;
- обработка специальных категорий персональных данных;
- трансграничная передача персональных данных на территорию государства,

не обеспечивающего адекватную защиту прав Субъектов персональных данных;
- принятие решения на основании исключительно автоматизированной обработки персональных данных, порождающего юридические последствия в отношении Субъекта или иным образом затрагивающего его права и законные интересы;
8.3. Содержание согласие Субъекта в письменной форме должно отвечать требованиям ч. 4 ст. 9 федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных»:
8.4. Согласие Субъекта в письменной форме оформляется на бумажном носителе с собственноручной подписью Субъекта или его представителя. Равнозначным, содержащему собственноручную подпись Субъекта, согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с требованиями федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
8.5.В случаях, не требующих в соответствии с действующим законодательством оформлять Оператору согласие в письменной форме, может быть получено согласие в любой форме с применением сервисов Оператора, принадлежащих или используемых Оператором, позволяющей подтвердить факт его получения. К таким случаям относятся получение согласий в письменной форме и в форме электронного документа, а также в случаях совершения Субъектом явного действия, например, но не ограничиваясь:
- отправка Оператору после процедуры ознакомления с текстом согласия на обработку персональных данных ответного SMS-сообщения с Кодом подтверждения полученного Субъектом на мобильный номер телефона;
- нажатие Субъектом на кнопку «Подтверждаю», «Согласен», «Принимаю», «Продолжить» и т. п. после процедуры ознакомления с текстом согласия на обработку персональных данных;
- заполнение Чек-бокса рядом с текстом согласия на обработку персональных данных в графическом интерфейсе бизнес-сервиса;
- ответное электронное письмо на электронный почтовый ящик оператора, исходящее от Субъекта с информацией о согласии на обработку персональных данных.
8.7. Обеспечение доказательств наличия правовых оснований на обработку персональных данных.
8.7.1. В соответствии с требованиями федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных» по запросу уполномоченного органа или Субъекта Оператор обязан предоставить доказательство получения согласия Субъекта на обработку его персональных данных или доказательство наличия иных оснований обработки персональных данных.
8.7.2. Подтверждением факта получения согласия на бумажном носителе является бланк согласия с собственноручной подписью Субъекта или его представителя и указанием даты его подписи.
8.7.3. Хранение Согласий, оформленных на бумажном носителе, в зависимости от вида осуществляется в ответственных подразделениях оператора.
8.7.4. При получении согласия от представителя Субъекта Оператору необходимо осуществлять хранение документов, подтверждающих полномочия представителя, в течение срока, установленного для хранения согласий. Хранение документов, подтверждающих полномочия представителя, осуществляется совместно с согласиями.
8.7.5. Место хранения согласий, а также лица ответственные за организацию хранения, определяется внутренним локальным нормативным документом Оператора.
8.7.6. В целях обеспечения подтверждения получения Оператором согласий в электронном виде, в информационных системах Оператора должны быть реализованы функции учета полученных согласий и хранение подтверждений (с возможностью их выгрузки для последующей печати). В связи с этим, Оператор и Субъект персональных данных признают выгрузки Лог-файлов, выписки из электронных журналов, электронной базы данных, извлекаемых и хранящихся на сервере Оператора, в том числе в формате Excel, формате CSV), а также указанных выгрузок из Лог-файлов на бумажном носителе, заверенные

уполномоченным работником Оператора в качестве надлежащего доказательства факта обмена Сообщениями.

9. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

9.1. Лица, виновные в нарушении требований законодательства о персональных данных, несут ответственность, предусмотренную действующим законодательством Российской Федерации.

10. Утверждение и пересмотр

10.1. Настоящая Политика вступает в силу с момента ее утверждения Директором Оператора и действует бессрочно.

10.2. Директор проводит пересмотр положений настоящей Политики и их актуализацию по мере необходимости, но не реже одного раза в три года, а также:

- при изменении требований законодательства РФ к порядку обработки и обеспечению безопасности Персональных данных;

- по результатам проверок органа по защите прав Субъектов Персональных данных, выявившим несоответствия требованиям законодательства РФ по обеспечению безопасности Персональных данных;

- в случае выявления существенных нарушений по результатам внутренних проверок системы защиты Персональных данных;

- при изменении процессов и технологий обработки Персональных данных Оператора.

10.3. При внесении изменений указывается дата последнего обновления редакции. Новая редакция утверждается приказом Директора ООО «Мира Ретрит».

11. Кто имеет доступ к Вашей Персональной информации и кому она может быть передана

11.1. Оператор может передавать Вашу Персональную информацию своим сотрудникам. Оператор также может передавать Вашу Персональную информацию своим Партнерам - согласно Приложению №2 к настоящей Политики.

11.2 Оператор также может передавать Персональную информацию третьим лицам, не предусмотренным п. 11.1., для достижения целей, указанных в разделе 3 настоящей Политики.

К таким третьим лицам могут относиться:

- лица, участвующие в организации приема Ваших платежей и проведении платежных операций с использованием Сайтов и Сервисов (платежные системы, поставщики платежных инструментов, банки и иные финансовые организации и т.д.);

- лица, предоставляющие информацию для выявления угроз безопасности для Сайтов и Сервисов, пользователей, Оператора и/или третьих лиц, в том числе при проверке Вашей благонадежности при заключении договоров с использованием Сайтов и Сервисов;

- регулирующие органы, правоохранительные органы, исполнительные органы власти, другие официальные или государственные органы или суды, в отношении которых Оператор обязан предоставлять информацию в соответствии с применимым законодательством по соответствующему запросу;

- третьи лица, в случае если Вы выразили согласие на передачу Вашей Персональной информации либо передача Персональной информации требуется для предоставления Вам соответствующего Сервиса или выполнения определенного соглашения или договора, заключенного с Вами;

- любому третьему лицу в целях обеспечения правовой защиты Оператора или третьих лиц при нарушении Вами настоящей Политики настоящей Политики или условий, регулирующих использование отдельных Сервисов, либо в ситуации, когда существует угроза такого нарушения.