

УТВЕРЖДЕНО Приказом Генерального
директора АО «Астра УА»

Приказ № 27122023/1 от 27.12.2023 г.

Вступает в силу с 27.12.2023 г.

**ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И РЕАЛИЗАЦИИ
ТРЕБОВАНИЙ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

АО «Астра УА»

Москва 2023

1. Общие положения

1.1. Настоящий документ определяет политику АО «Астра УА» (далее – Компания) в отношении обработки персональных данных и реализации требований к защите персональных данных (далее – Политика).

Политика определяет принципы, условия и общий порядок обработки и защиты персональных данных Компанией и разработана с целью 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.

1.2. В настоящей Политике применяются следующие термины и определения:

Компания (оператор обработки персональных данных) – АО «Астра УА», осуществляющая обработку персональных данных, а также определяющая цели обработки персональных данных, состав персональных данных, подлежащих обработке, и действия, совершаемые с персональными данными.

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

Информационная система персональных данных (ИСПДн) – совокупность информационных технологий и технических средств, которые обеспечивают обработку персональных данных, а также баз данных и систем хранения данных, в которых обрабатываются персональные данные.

Безопасность персональных данных – состояние защищенности персональных данных, которое характеризуется способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке.

Информационная безопасность – состояние защищенности в условиях угроз в информационной сфере.

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Работник – лицо, состоящее с Компанией в трудовых отношениях на основании заключенного трудового договора.

Кандидат – физическое лицо, претендующее на вакантные должности Компании.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

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.

Файлы Cookie – текстовые файлы, пересылаемые браузером серверу при открытии страницы соответствующего сайта, используемые для аутентификации пользователя, хранения его персональных предпочтений и настроек, отслеживания состояния сессии доступа пользователя, ведения статистики о пользователях и т.п.

Угроза безопасности ПДн - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке ИСПДн.

Система защиты ПДн/СЗПДн - комплекс мероприятий технического, организационного и организационно-технического характера, направленных на обеспечение защиты ПДн.

Субъект персональных данных – физическое лицо, которому принадлежат персональные данные.

2. Правовые основания и принципы обработки Персональных данных

2.1. Обработка Персональных данных в Компании осуществляется в соответствии с федеральными законами и принятыми на их основе нормативными правовыми актами, в том числе:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ).
- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ с учетом изменений и дополнений.
- Налоговый кодекс Российской Федерации (ч. 1-2).
- Закон Российской Федерации от 07.02.1992 № 2300-1 «О защите прав потребителей».
- Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах».
- Федеральный закон от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг».
- Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 15.12.2001 N 167-ФЗ "Об обязательном пенсионном страховании в Российской Федерации";
- Федеральный закон от 06.12.2011 N 402-ФЗ "О бухгалтерском учете";
- Федеральный закон от 27.07.2010 N 224-ФЗ "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации";

- Постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Постановлением Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также иными действующими нормативными правовыми актами Российской Федерации, в сфере обработки и защиты персональных данных».

2.2. Правовыми основаниями обработки персональных данных являются федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью Компании, как профессионального участника рынка ценных бумаг, а также, как юридического лица, созданного в соответствии с законодательством Российской Федерации, уставные документы, договоры, заключаемые между Компанией и субъектом персональных данных, согласие на обработку Персональных данных.

2.3. Обработка Персональных данных в Компании осуществляется на основании следующих принципов:

- обеспечение законности и справедливости обработки Персональных данных, соблюдение их конфиденциальности и безопасности процессов их обработки;
- обеспечения надлежащей защиты персональных данных;
- ограничение обработки Персональных данных достижением конкретных, заранее определенных и законных целей;
- обработке подлежат только Персональные данные, которые отвечают целям их обработки;
- недопустимость объединения баз данных, содержащих Персональные данные, обработка которых осуществляется в несовместимых между собой целях;
- обеспечение точности, достаточности, а в необходимых случаях и актуальности Персональных данных по отношению к целям их обработки;
- хранение Персональных данных в форме, позволяющей определить Субъекта Персональных данных, не дольше, чем этого требуют цели обработки Персональных данных или установленный срок хранения;
- уничтожения или обезличивания персональных данных по достижении целей их обработки, если срок хранения персональных данных не установлен законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем, по которому является Субъект персональных данных;
- обеспечения конфиденциальности и безопасности обрабатываемых персональных данных.

3. Цели обработки Персональных данных в Компании

3.1. Компания осуществляет обработку Персональных данных в конкретных, заранее определенных и законных целях и на законных основаниях. Содержание и состав обрабатываемых персональных данных в Компании соответствует заявленным целям обработки.

3.2. Обработка Персональных данных осуществляется Компанией в целях оказания услуг, включая взаимодействие по вопросам предоставления услуг. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. Компания обрабатывает персональные данные как профессиональный участник рынка ценных бумаг (лицензия № 045-12747-001000 от 10 декабря 2009 г. выданной ФСФР России) в рамках деятельности по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами (лицензия № 21-000-1-01050 от 27 сентября 2021 г.), а также оказывает услуги в рамках деятельности в качестве Инвестиционного советника, осуществляемой Компанией на основании записи в Едином реестре инвестиционных советников.

3.3. Обработка Персональных данных осуществляется также в целях:

- осуществление функций, полномочий и обязанностей, возложенных на Компанию действующим законодательством Российской Федерации;
- заключение и исполнение договоров с контрагентами Компании в целях проведения операций/оказания услуг;
- регулирование трудовых отношений и организация учета работников Компании, для содействия указанным лицам в трудоустройстве, обучении и продвижении по службе, предоставлении различного вида льгот и социальных гарантий, поддержания корпоративной культуры, контроля количества и качества выполняемой работы, исполнении работниками Компании своих трудовых обязанностей в соответствии с Трудовым кодексом Российской Федерации;
- привлечение и отбор кандидатов на работу в Компании;
- предоставление отчетности государственным надзорным органам и ее раскрытие в соответствии с требованиями действующего законодательства Российской Федерации и нормативных актов Банка России;
- заключение и исполнение договоров гражданско-правового характера с физическими лицами;
- обработка заявок/заявлений, поступивших от потенциальных клиентов (субъектов ПДн) на оформление продуктов/услуг Компании;
- рассмотрение возможности совершения и совершение операций и сделок в соответствии с лицензиями, выданными Федеральной службой по финансовым рынкам и Банком России;
- верификация данных, указанных в заявке/заявлении на оформление продуктов/услуг;
- предоставление информации о Компании, ее продуктах и услугах, усовершенствование предлагаемых и/или разработки новых продуктов и услуг Компании, ведение статистики о пользователях сайта/мобильного приложения Компании, обеспечение функционирования и улучшения качества сайта Компании;
- проведение Компанией акций, опросов, маркетинговых и иных исследований;
- обработка корреспонденции и подготовка ответов на обращения субъектов ПДн;
- организация пропускного режима на территорию Компании;
- регистрация субъектов ПДн в единой биометрической системе;
- предоставление отчетности государственным надзорным органам и ее раскрытие в соответствии с требованиями действующего законодательства Российской Федерации и нормативных актов Банка России;
- обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам, ведения кадрового делопроизводства, исполнения требований трудового, налогового, пенсионного законодательства, в соответствии с кодексами, федеральными законами Российской Федерации, иными целями, предусмотренными соглашениями, полученными Компанией.

4. Принципы и условия обработки персональных данных

Обработка персональных данных Компанией осуществляется на основе следующих принципов и условий:

- 4.1. законность и справедливость обработки персональных данных;
- 4.2. ограничение обработки персональных данных при достижении заранее определенных и конкретных целей обработки. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- 4.3. соответствие содержания и объема обрабатываемых персональных данных, способов обработки персональных данных целям обработки;

4.4. недопустимость объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

4.5. точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

4.6. принятие необходимых мер либо обеспечение их принятия по удалению или уточнению неполных или неточных данных;

4.7. хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором;

4.8. уничтожение персональных данных либо обезличивание по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

4.9. соблюдение конфиденциальности защита персональных данных.

5. Перечень субъектов и права субъектов Персональных данных.

5.1. В Компании осуществляется обработка следующих категорий субъектов Персональных данных:

- клиенты;
- работники Компании;
- кандидаты на вакантные должности;
- исполнители по гражданско-правовым договорам;
- контрагенты по договорам;
- представители клиентов, контрагентов, работников, исполнителей;
- лица, обратившиеся в Компанию с обращением, жалобой или заявлением;
- иные физические лица, состоящие с Компанией в правоотношениях.

5.2. Субъект Персональных данных имеет право:

- на получение информации, касающейся обработки его персональных данных в соответствии со статьей 14 Федерального закона № 152-ФЗ;
- требовать уточнения его Персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
- принимать предусмотренные законом меры по защите своих прав;
- обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Компании при обработке его персональных данных;
- иные права, определенные главой 3 Федерального закона № 152-ФЗ.

Право субъекта персональных данных на доступ к своим персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма или иными нормативными актами;
- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

- При обращении в Компанию с запросом о предоставлении информации об обработке персональных данных, субъект обязан указать в запросе:
- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта персональных данных в отношениях с Компанией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Компанией;
- поставить личную подпись в запросе на предоставление информации.

6. Обработка персональных данных

6.1. Обработка персональных данных осуществляется Компанией:

- с использованием средств автоматизации;
- без использования таких средств;
- смешанным способом.

6.2. Сроки обработки персональных данных в Компании определяются в соответствии с нормативно-правовыми актами Российской Федерации, внутренними документами Компании, условиями договоров и иных соглашений, заключенных с субъектами персональных данных.

6.3. Обработка персональных данных включает следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

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

6.5. 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.

6.6. Обрабатываемые в Компании персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.7. Компания не предоставляет и не раскрывает сведения, содержащие персональные данные субъектов, третьей стороне без согласия субъекта Персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральными законами.

6.8. Компания может поручить обработку Персональных данных третьему лицу, если иное не предусмотрено законодательством Российской Федерации. В этом случае, обработка Персональных данных третьим лицом может осуществляться только с согласия субъекта Персональных данных (его законного представителя), если получение такого согласия необходимо в соответствии с требованиями Федерального закона № 152-ФЗ.

6.9. Компания осуществляет передачу Персональных данных государственным органам и уполномоченным лицам в рамках их полномочий и компетенции в соответствии с законодательством Российской Федерации.

6.10. Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение Персональных данных, осуществляются с использованием баз данных, расположенных на территории Российской Федерации.

6.11. Хранение Персональных данных в форме, позволяющей идентифицировать субъекта, осуществляется не дольше, чем того требует достижение целей их обработки, если иное не установлено законодательством Российской Федерации или договором.

6.12. В случае выявления необходимости внесения изменений в Персональные данные, с целью обеспечения их точности, достоверности и актуальности, в том числе по отношению к целям обработки Персональных данных, такие изменения вносятся уполномоченным работником Компании на основании предоставленных надлежащим образом оформленных оригиналов документов или их заверенных копий.

6.13. Сроки обработки Персональных данных определяются в соответствии требованиями действующего законодательства Российской Федерации, нормативными правовыми актами, внутренними документами Компании, условиями договоров.

6.14. Компания прекращает обработку персональных данных (блокирует) в следующих случаях:

- выявлен факт их неправомерной обработки;
- достигнута цель их обработки; в этом случае, если иное не предусмотрено нормами действующего законодательства РФ, Компания прекращает обработку ПДн и обеспечивает прекращение обработки ПДн третьими лицами, обрабатывающими ПДн по договору с Компанией;
- истек срок действия согласия на обработку ПДн;
- субъект персональных данных отозвал согласие на обработку ПДн.

6.15. Компания вправе продолжить обрабатывать персональные данные без согласия субъекта персональных данных при наличии оснований, указанных в ч. 2 ст. 9 Федерального закона «О персональных данных».

6.16. Компания осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требует каждая цель обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором.

7. Безопасность Персональных данных

7.1. В Компании принят комплекс правовых, организационных и технических мер по обеспечению безопасности Персональных данных, направленных на предотвращение несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними, в том числе со стороны третьих лиц, в соответствии с требованиями Федерального закона № 152-ФЗ и его подзаконными актами.

7.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Компании определены и применяются с учетом установленных уровней защищенности персональных данных при их обработке в информационных системах персональных данных Компании в соответствии с требованиями, установленными Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

7.3. Средства защиты в рамках системы защиты персональных данных при их обработке в информационных системах персональных данных Компании определены и внедрены в соответствии с требованиями законодательства Российской Федерации в области персональных данных.

К мерам, направленным на обеспечение Компанией обязанностей, предусмотренных Федеральным законом № 152-ФЗ и к мерам обеспечения безопасности Персональных данных относятся, в том числе, но не ограничиваясь:

- Компания проводит оценку вреда, который может быть причинен субъектам персональных данных и определяет угрозы безопасности персональных данных. В соответствии с выявленными актуальными угрозами Компания определяет уровень защищенности ИСПДн, применяет необходимые и достаточные организационные и технические меры, включающие в себя использование средств защиты информации, обнаружение фактов несанкционированного доступа, предотвращения внедрения в ИСПДн вредоносного программного обеспечения, восстановление персональных данных, установление правил доступа к персональным данным, а также контроль и оценку эффективности применяемых мер;
- в Компании назначено лицо, ответственное за организацию обработки и обеспечение безопасности Персональных данных;
- в Компании осуществляется учет обрабатываемых в Компании Персональных данных, информационных систем Компании, в которых обрабатываются Персональные данные, должностей работников Компании, доступ которых к Персональным данным необходим для выполнения их трудовых обязанностей;
- устанавливаются правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, на основе принципа минимально необходимых полномочий для выполнения функциональных обязанностей и поставленных перед сотрудником задач в объеме, необходимом для их исполнения, а также обеспечение регистрации и учета действий, совершаемых с персональными данными в информационной системе персональных данных;
- обеспечивается возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществляется резервирование технических средств, дублирования массивов и носителей, содержащих ПДн;
- при обработке Персональных данных, осуществляемой без использования средств автоматизации, выполняются требования, установленные Постановлением Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- иные меры, предусмотренные действующим законодательством Российской Федерации, Федеральным законом № 152-ФЗ и нормативными правовыми актами в сфере защиты персональных данных.

7.4. Руководство Компании осознает необходимость и заинтересовано в обеспечении должного как с точки зрения требований нормативных документов РФ, так и обоснованного с точки зрения оценки рисков для бизнеса уровня безопасности персональных данных, обрабатываемых в рамках выполнения основной деятельности Компании.

8. Заключительные положения

8.1. Настоящая Политика является локальным актом Компании и относится к общедоступной информации. Действующая редакция Политики подлежит размещению на официальном сайте Компании.

8.2. Ответственность за контроль соблюдения настоящей Политики возлагается на лицо, ответственное за организацию обработки и обеспечение безопасности Персональных данных в Компании.

8.3. Любые изменения и/или дополнения в настоящую Политику вступают в силу с даты утверждения новой версии документа.