

ПОЛИТИКА ОБРАБОТКИ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРА ОБМЕНА ВИРТУАЛЬНЫХ АКТИВОВ ОсОО «Миллианс»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика обработки и защиты персональных данных (далее – Политика) определяет принципы, порядок и условия обработки персональных данных в Операторе обмена виртуальными активами (далее – Компания). Политика разработана и утверждена в соответствии с законодательством Кыргызской Республики и Уставом Компании. Политика направлена на соблюдение прав и свобод человека и гражданина при обработке его персональных данных, включая защиту права на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Действие настоящей Политики распространяется на все подразделения Компании, всех ее работников, клиентов, партнеров, контрагентов и иных лиц, чьи персональные данные обрабатываются Компанией. Политика является внутренним нормативным документом Компании, обязательным для исполнения всеми сотрудниками, допущенными к обработке персональных данных.

1.3. Целями обработки персональных данных в Компании являются:

- обеспечение защиты прав и свобод субъектов персональных данных при обработке их данных;
- предоставление услуг Компании клиентам и исполнение заключенных с ними договоров (в том числе операция обмена виртуальными активами и сопутствующие услуги);
- исполнение установленных законом обязанностей Компании (требований законодательства о противодействии отмыванию денег и финансированию терроризма, налогового и бухгалтерского учета, порядка рассмотрения обращений граждан и др.);
- продвижение товаров и услуг Компании на рынке посредством прямых контактов с потенциальными и существующими клиентами с помощью средств связи;
- ведение делопроизводства и архива в соответствии с требованиями законодательства;
- кадровое делопроизводство, содействие работникам Компании в трудоустройстве, обучении, продвижении по работе, оплата труда, управление персоналом и выполнение трудовых договоров;
- выполнение обязательств по договорам с контрагентами и партнерами, расчеты за оказанные услуги, выполненные работы и поставленные товары;
- обеспечение личной безопасности работников, клиентов и партнеров, охрана имущества и информационных ресурсов Компании;
- контроль качества и количества выполняемой работы, а также качества предоставляемых услуг;
- иные законные бизнес-цели Компании, соответствующие законодательству Кыргызской Республики.

1.4. Настоящая Политика не регулирует вопросы, связанные с организацией хранения, комплектования, учета и использования архивных документов, содержащих персональные данные, которые входят в Архивный фонд Кыргызской Республики или государственные архивы. Также действие Политики не распространяется на случаи обработки персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.5. При обработке персональных данных Компания придерживается следующих основных принципов:

1.5.1. Законность, справедливость и прозрачность обработки - обработка персональных данных осуществляется на законных основаниях, справедливым образом и прозрачно для субъекта персональных данных. Недопустима обработка персональных данных скрытыми способами.

1.5.2. Ограничение целями - обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Недопустимо обрабатывать персональные данные, несовместимые с изначально заявленными целями, либо расширять цели обработки без согласия субъекта, если иное не предусмотрено законодательством КР;

1.5.3. Минимизация данных - состав и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Обрабатываемые данные являются достаточными, актуальными и не избыточными по отношению к заявленным целям. При выявлении избыточности персональных данных Компания принимает меры по удалению или уточнению таких данных.

1.5.4. Точность и актуальность - компания обеспечивает точность персональных данных, их достаточность, а при необходимости и актуальность по отношению к целям обработки. При выявлении неточных или неполных данных они подлежат исправлению или уничтожению. Компания принимает необходимые меры для актуализации персональных данных, включая обращение к субъекту при необходимости.

1.5.5. Ограничение сроков хранения - персональные данные хранятся не дольше, чем этого требуют цели их обработки, если иной срок хранения не установлен законодательством или договором с участием субъекта. По достижении целей обработки или при утрате необходимости в их достижении обрабатываемые персональные данные подлежат уничтожению либо обезличиванию, если иное не предусмотрено законом.

1.5.6. Целостность и конфиденциальность - обработка персональных данных осуществляется способом, обеспечивающим их надлежащую безопасность. Компания принимает организационные и технические меры, предотвращающие несанкционированный или незаконный доступ к персональным данным, их случайное или умышленное уничтожение, искажение, блокирование, копирование, распространение, утечку, а также иные неправомерные действия.

1.5.7. Ответственность и подотчетность - компания (владелец персональных данных) несет ответственность за соблюдение принципов обработки персональных данных и готова подтвердить соответствие своей деятельности требованиям законодательства КР.

1.6. Настоящая Политика утверждается директором Компании и вводится в действие приказом по Компании. Все работники, допущенные к обработке персональных данных, обязаны ознакомиться с Политикой, новые работники знакомятся с Политикой при приеме на работу. Изменения и дополнения в Политику утверждаются уполномоченным руководителем и доводятся до сведения работников аналогичным порядком.

1.7. Все вопросы, касающиеся обработки и защиты персональных данных, которые не урегулированы настоящей Политикой, регулируются нормами законодательства Кыргызской Республики о персональных данных. В случае противоречия отдельных положений настоящей Политики нормам законодательства, применяются нормы законодательства.

2. ТЕРМИНЫ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные - любая информация относящаяся к прямо или косвенно определенному либо определяемому физическому лицу (субъекту персональных данных). Иными словами, это сведения, позволяющие идентифицировать конкретное лицо прямо либо опосредованно через совокупность данных. Персональные данные в цифровой форме представляют собой цифровые записи, содержащие информацию персонального характера.

2.2. Персональные данные, разрешенные субъектом для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен самим субъектом персональных данных. Такое предоставление осуществляется путем дачи субъектом отдельного согласия на обработку персональных данных, предназначенных для распространения, в порядке, предусмотренном законодательством Кыргызской Республики.

2.3. Состав (категории) обрабатываемых персональных данных. В зависимости от категории субъектов и целей обработки Компания может обрабатывать различные персональные данные, в том числе (при необходимости):

- фамилия, имя, отчество (при наличии);
- пол; возраст; дата и место рождения;
- гражданство; национальность; расовая или этническая принадлежность;
- сведения об образовании, квалификации, специальности;
- сведения о месте жительства и регистрации; фактический адрес проживания;
- семейное положение, наличие детей и иждивенцев, состав семьи, родственные связи;
- биографические данные (трудовая деятельность, воинский учет, стаж работы и службы, трудовой и учебный путь и др.);
- идентификационные данные: персональный идентификационный номер (ПИН) либо идентификационный номер налогоплательщика (ИНН); номер и серия паспорта или другого документа, удостоверяющего личность, дата выдачи и выдавший орган; сведения о прописке/регистрации;
- фотография (в том числе фото 3x4, изображения лица на документах и др.);
- контактная информация: номера телефонов, адрес электронной почты, почтовый адрес и иные способы связи;

- сведения о профессиональной деятельности: место работы, должность, структурное подразделение, должностные обязанности;
- сведения о трудовых отношениях: содержание трудового договора, приказы и распоряжения по личному составу, личное дело работника, трудовая книжка и сведения о трудовом стаже, результаты аттестаций, материалы служебных расследований и др.;
- финансово-экономические сведения: сведения о заработной плате, окладе, иных доходах, надбавках и премиях; банковские реквизиты (расчетный счет, номер банковской карты); данные о налогах и социальных отчислениях; сведения о применяемых социальных льготах и компенсациях;
- сведения о состоянии здоровья (медицинские справки о годности к работе, результаты медицинских осмотров, информация о временной нетрудоспособности, медицинские заключения);
- сведения о воинском учете (воинское звание, категория запаса, военный билет и др.);
- сведения о наличии или отсутствии судимости;
- личностные характеристики, в том числе деловые и иные качества субъекта (в том числе в виде оценочных суждений, рекомендаций);
- иные сведения, позволяющие идентифицировать субъекта персональных данных.

2.3.1. Из перечисленных категорий Компания собирает и использует только те сведения, которые необходимы для достижения конкретных законных целей обработки, указанных в разделе 1.3 настоящей Политики, а также для исполнения договорных и законных обязательств Компании. Обработке подлежат, как правило, данные, характеризующие субъекта как сторону договорных отношений с Компанией (клиента, сотрудника либо контрагента).

2.4. Сведения и документы, указанные в п. 2.3 настоящей Политики, являются конфиденциальными. Компания обеспечивает соблюдение режима конфиденциальности в отношении этих персональных данных. Режим конфиденциальности не применяется к обезличенным данным (данным, обезличенным таким образом, что идентификация субъекта более невозможна без использования дополнительной информации). В случае обезличивания персональных данных требования конфиденциальности иные ограничения на обработку снимаются.

2.5. Персональные данные могут содержаться в различных документах и информационных системах Компании, в том числе:

- заявления, анкеты, договоры и иные документы, предоставляемые субъектами персональных данных (клиентами, сотрудниками, кандидатами на работу, контрагентами) при вступлении в отношения с Компанией;
- комплекты документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении сотрудников;
- материалы по подбору персонала (резюме, анкеты, результаты тестирований, собеседований с кандидатами);
- приказы (распоряжения) по личному составу (о приеме, переводе, увольнении, поощрениях, взысканиях и др.);
- личные дела работников, трудовые книжки, трудовые договоры и соглашения к ним, должностные инструкции, сведения о трудовой деятельности;
- документы по воинскому учету работников;
- материалы аттестации работников, документы о повышении квалификации и переподготовке, результаты проверки знаний;
- материалы служебных расследований, докладные записки, акты проверок;
- журналы, реестры, базы данных и иные носители, формируемые в процессе деятельности Компании и содержащие персональные данные (базы данных клиентов, журналы регистрации посетителей, переписка с клиентами и партнерами, реестр договоров с контрагентами и т.п.);
- бухгалтерские и финансовые документы, содержащие данные о физических лицах (расчетно-платежные ведомости, платежные поручения, счета-фактуры с реквизитами физического лица и пр.);
- копии отчетов, направляемых в государственные органы (органы статистики, налоговые органы, органы социального страхования и др.), если в них включены персональные данные;
- иные документы и информационные системы, содержащие персональные данные в объеме, необходимом для деятельности Компании.

3. ПРАВА И ОБЯЗАННОСТИ КОМПАНИИ (ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ)

3.1. Компания, являясь оператором (владельцем) персональных данных, осуществляет обработку персональных данных субъектов в соответствии с требованиями законодательства. Компания имеет право:

- получать непосредственно от субъекта персональных данных достоверные сведения и/или документы, необходимые для достижения заявленных целей обработки и содержащие персональные данные;
- проверять и уточнять персональные данные, предоставленные субъектом (в том числе путем запроса у субъекта актуальных данных или документов, подтверждающих такие данные);
- прекращать обработку персональных данных (включая удаление или блокирование данных) в случае достижения цели обработки, отзыва согласия субъектом, выявления неправомерной обработки либо по другим основаниям, предусмотренным законодательством или настоящей Политикой.

3.2. Компания обязана:

- организовывать и осуществлять обработку персональных данных строго в соответствии с законодательством Кыргызской Республики и настоящей Политикой;
- соблюдать права субъектов персональных данных и обеспечивать их реализацию в установленном порядке;
- рассматривать обращения и запросы субъектов персональных данных, касающиеся обработки их данных, и давать ответы в срок, не превышающий 7 (семи) рабочих дней с момента поступления обращения, если законодательством не установлен иной срок;
- предоставлять субъекту персональных данных возможность бесплатного доступа к его персональным данным (в том числе ознакомления с ними, получения выписок или копий) за исключением случаев, предусмотренных законом;
- по обращению субъекта в разумный срок вносить изменения, уточнения в обрабатываемые персональные данные, обновлять их, блокировать или уничтожать, если данные являются неточными, устаревшими, неполными либо обработаны неправомерно или не соответствуют заявленным целям;
- в случае поступления от субъекта отзыва согласия на обработку тех или иных персональных данных прекратить соответствующую обработку, если дальнейшая обработка не допускается на иных законных основаниях;
- принимать правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, раскрытия, копирования, модификации, утечки, блокирования, уничтожения либо иных неправомерных действий (меры защиты подробно изложены в разделе 9 настоящей Политики);
- не раскрывать и не распространять персональные данные третьим лицам без законных оснований;
- выполнять законные предписания уполномоченного государственного органа по защите персональных данных, предоставлять ему необходимую информацию в случае проверок;
- вести учет операций, связанных с обработкой персональных данных (при сборе, изменении, передаче и т.п.), в случаях и порядке, установленных законодательством и внутренними процедурами Компании;
- назначить должностное лицо, ответственное за организацию обработки и защиты персональных данных либо привлечь на основании договора квалифицированного специалиста для выполнения функций ответственного за персональные данные;
- выполнять иные обязанности, предусмотренные законодательством Кыргызской Республики в сфере персональных данных.

3.3. Компания не вправе получать и обрабатывать персональные данные, относящиеся к специальным категориям (сведения о расовом или этническом происхождении, политических взглядах, религиозных или философских убеждениях, членстве в профсоюзах, здоровье и интимной жизни субъекта), за исключением случаев, когда:

- субъект дал явное согласие на обработку таких данных;
- либо обработка необходима в связи с выполнением договора с субъектом;
- либо обработка осуществляется на основании прямого указания закона и с соблюдением установленных мер защиты;
- либо применяется иное исключение, предусмотренное законодательством Кыргызской Республики

В общем случае Компания воздерживается от сбора и обработки специальных категорий данных, если это не обусловлено явной необходимостью и законными основаниями.

3.4. Компания не осуществляет сбор и обработку персональных данных о членстве субъекта в общественных объединениях, его партийной или профсоюзной деятельности, за исключением случаев, когда это требуется Компании в связи с исполнением закона или договора (сведения о членстве в профсоюзе для удержания членских взносов по заявлению работника) либо получено согласие субъекта.

3.5. При принятии Компанией решений, затрагивающих интересы субъекта персональных данных, не допускается основываться исключительно на результатах автоматизированной обработки персональных данных. Все решения, порождающие правовые последствия для субъекта или иным существенным образом влияющие на него, принимаются с участием уполномоченных сотрудников (человека), если иное не установлено законом. Автоматизированная обработка может использоваться для облегчения принятия решения, но окончательное решение подлежит оценке ответственным должностным лицом с целью исключения необоснованных выводов и возможной дискриминации субъекта.

3.6. Компания обеспечивает защиту персональных данных субъекта от неправомерного их использования или утраты за счет собственных средств и сил, в порядке, установленном законодательством Кыргызской Республики и внутренними документами. Обязанность обеспечения безопасности персональных данных возлагается на руководителей подразделений, ответственных за соответствующие участки работы с персональными данными, и на специально назначенное ответственное лицо.

3.7. Иные права и обязанности Компании при обработке персональных данных определяются действующим законодательством Кыргызской Республики. В случае изменения законодательства соответствующие новые требования подлежат применению даже до внесения формальных изменений в настоящую Политику.

4. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Субъект персональных данных (физическое лицо, к которому относятся данные) обязан:

- предоставлять Компании только достоверные, точные и актуальные данные о себе, необходимые для достижения целей обработки; не вводить Компанию в заблуждение относительно своей личности или иных персональных сведений;
- предоставлять по запросу Компании документы, содержащие персональные данные, в объеме, необходимом для заявленной цели обработки (для заключения договора, для выполнения требований законодательства и т.д.);
- своевременно, по мере необходимости, сообщать Компании об изменении своих персональных данных. Субъект должен обновлять свои персональные данные, ранее предоставленные Компании, в разумные сроки после произошедших изменений (не позднее 5-7 рабочих дней), чтобы обеспечить их актуальность и достоверность.

4.2. Субъект персональных данных имеет право:

4.2.1. На полную информацию о своих персональных данных и об их обработке Компанией. Субъект вправе запросить у Компании сведения о том, обрабатываются ли его персональные данные, и если да, то какие именно данные, откуда они получены, в каких целях и на каких правовых основаниях обрабатываются, кому передаются, как долго хранятся, и какие права имеет субъект в отношении такой обработки. Предоставление информации субъекту осуществляется в порядке, предусмотренном законом (в том числе по письменному запросу субъекта). Компания при ответе предоставляет запрашиваемые сведения либо мотивированный отказ в случаях, предусмотренных законодательством.

4.2.2. Субъект имеет право свободного и бесплатного доступа к своим персональным данным, обрабатываемым Компанией, за исключением случаев, предусмотренных законом. Предоставление доступа к данным третьим лицам осуществляется в порядке, установленном законодательством и внутренними правилами Компании, при наличии надлежащим образом оформленной доверенности или иного правового основания.

4.2.3. Субъект вправе требовать от Компании исправления неточных персональных данных, а также дополнения неполных данных о себе. Кроме того, в случаях, предусмотренных законом, субъект может требовать временной приостановки обработки (блокирования) либо уничтожения своих персональных данных, если данные являются неполными, устаревшими, недостоверными, были получены незаконным путем или не являются необходимыми для заявленной цели обработки. Компания обязана рассмотреть такое требование и выполнить его, если оно обосновано и не противоречит требованиям законодательства.

4.2.4. Если обработка персональных данных осуществляется на основании согласия субъекта, последний вправе в любое время отозвать свое согласие (в отношении одной, нескольких или всех целей обработки, на которые было

дано согласие). Отзыв согласия не имеет обратной силы и не влияет на законность обработки, осуществленной до отзыва. Также субъект персональных данных вправе в любой момент потребовать прекратить распространение (передачу, предоставление, открытие доступа) своих персональных данных, ранее разрешенных им для распространения. Такой отзыв или требование оформляется в письменной форме, с указанием фамилии, имени, отчества (при наличии) субъекта, его контактной информации (телефон, email или почтовый адрес) и перечня персональных данных, распространение которых следует прекратить. Компания обязуется выполнить обоснованный отзыв/требование субъекта в предусмотренных законом случаях и объеме.

4.2.5. Субъект персональных данных имеет право возразить против обработки своих персональных данных определенными способами или в определенных целях, если такая обработка осуществляется на основаниях, отличных от согласия (например, в целях реализации законных интересов Компании).

4.2.6. В случае нарушения своих прав при обработке персональных данных субъект вправе обращаться с жалобами и заявлениями в уполномоченный государственный орган по защите персональных данных, либо в судебные органы, а также иными способами защищать свои права и законные интересы, предусмотренные законодательством.

4.2.7. На осуществление иных прав, предусмотренных законодательством Кыргызской Республики. К таким правам, в частности, относятся: право требовать уведомления о передаче персональных данных третьим лицам, право требовать извещения о произведенных исправлениях или уничтожении данных, право на ознакомление с механизмом автоматизированной обработки своих данных, право на защиту от решения, имеющего для субъекта правовые последствия, принятого исключительно на основе автоматизированной обработки, и другие права, предусмотренные профильным законом и Цифровым кодексом КР.

4.3. Права субъекта персональных данных могут быть ограничены в случаях, предусмотренных законодательством. В частности, предусмотрено, что право субъекта на доступ к своим данным может быть ограничено, если доступ субъекта к информации нарушает права и законные интересы третьих лиц либо препятствует правосудию, а также в иных случаях, определенных законом. В случае отказа Компании в предоставлении информации по запросу субъекта такой отказ дается в письменной форме с указанием оснований отказа со ссылкой на конкретную норму закона.

4.4. Субъект персональных данных несет ответственность за предоставление недостоверных сведений о себе, а также за несвоевременное обновление своих данных. Компания не несет ответственности за негативные последствия, возникшие в результате предоставления субъектом недостоверных или устаревших персональных данных, либо не уведомления Компании об изменениях в данных.

5. ЦЕЛИ, ОСНОВАНИЯ И СПОСОБЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Обработка персональных данных в Компании осуществляется с соблюдением установленных правовых оснований. Основания обработки персональных данных – наличие хотя бы одного из следующих условий:

- субъект персональных данных дал согласие на обработку своих персональных данных для одной или нескольких конкретных целей;
- обработка необходима для заключения или исполнения договора, стороной которого является субъект персональных данных (либо выгодоприобретателем, поручителем по договору), либо для рассмотрения запроса субъекта перед заключением договора;
- обработка необходима для выполнения Компанией обязанностей, возложенных на нее законом или иными нормативными правовыми актами (обязанностей по предоставлению отчетности, ответам на запросы уполномоченных органов, ведению официальной статистики и др.);
- обработка необходима для защиты жизненно важных интересов субъекта персональных данных либо другого физического лица;
- обработка необходима для осуществления Компанией публично значимых задач либо законных интересов Компании или третьих лиц, при условии что при этом не нарушаются права и свободы субъекта персональных данных.
- При наличии указанных оснований отдельное согласие субъекта на обработку его данных может не требоваться, за исключением случаев, прямо предусмотренных законом. Во всех остальных случаях (при отсутствии иных оснований) Компания запрашивает у субъекта добровольное, конкретное, информированное и сознательное согласие на обработку его персональных данных для конкретных целей. Согласие субъекта может быть дано в письменной форме (на бумаге) либо в форме электронного документа, подписанного электронной подписью в соответствии с законодательством.

5.2. Обработка персональных данных понимается как любое действие (операция) или совокупность действий, совершаемых с персональными данными, независимо от используемых средств и методов (автоматизированных или нет). К таким действиям относятся, в частности: сбор, запись, организация, структурирование, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, просмотр, использование, аналитическое обрабатывание, распространение (передача, предоставление, доступ), обмен, обезличивание, блокирование, сокращение, удаление, уничтожение персональных данных, а также любые другие операции с персональными данными. Обработка персональных данных в Компании может осуществляться как с использованием средств автоматизации (в информационных системах, базах данных), так и без использования таковых (неавтоматизированным способом, например, на бумажных носителях). Вне зависимости от способа обработки, Компания соблюдает все применимые принципы, требования и ограничения, установленные законодательством и настоящей Политикой.

5.3. Категории субъектов персональных данных. Компания обрабатывает персональные данные следующих основных категорий субъектов:

- Клиенты (пользователи услуг Компании) – физические лица, пользующиеся услугами оператора обмена виртуальными активами, либо обратившиеся за получением таких услуг, а также их представители;
- Работники Компании - сотрудники, состоящие с Компанией в трудовых отношениях; а также соискатели (кандидаты на трудоустройство), бывшие сотрудники; стажеры и лица, привлеченные на практику;
- Контрагенты - физические лица (либо представители контрагентов-юридических лиц) - поставщики, подрядчики, агенты, иные лица, с которыми Компания вступает в гражданско-правовые отношения, и которые предоставляют свои персональные данные для целей заключения и исполнения договоров;
- Посетители офиса и мероприятия Компании - лица, посещающие помещения Компании либо участвующие в мероприятиях, организуемых Компанией, и предоставляющие свои данные при регистрации либо допуске (предъявляющие документ удостоверения личности на входе, заполняющие регистрационную форму и т.д.);
- Иные субъекты, персональные данные которых поступают в Компанию от третьих лиц или из открытых источников в рамках осуществления деятельности Компании на законных основаниях (например, персональные данные представителей государственных органов, партнеров, контактных лиц контрагентов, заявителей в порядке официальной переписки и пр.).

5.4. Компания обеспечивает соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки. Обрабатываемые данные ограничиваются тем, что необходимо для достижения конкретной цели. При изменении целей на несовместимые с первоначальными Компания запрашивает новое согласие субъекта или иную законную основу. В случае выявления избыточных персональных данных, которые не требуются для заявленных целей, такие данные либо не подлежат сбору, либо удаляются (уничтожаются) либо переводятся в обезличенную форму.

6. УСЛОВИЯ И СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных в Компании, как правило, осуществляется с согласия субъекта персональных данных. До получения персональных данных от субъекта Компания доводит до него необходимые сведения, предусмотренные законодательством (в том числе цели и предполагаемые источники и способы обработки, характер собираемых данных, последствия отказа предоставить данные и др.). Исключения, когда обработка персональных данных допускается без согласия субъекта, определены законодательством Кыргызской Республики – такие случаи включают, например, выполнение обязательств по закону, необходимость для исполнения договора с субъектом, защиту жизни или здоровья субъекта либо иных лиц, общественно значимые цели, и другие основания, указанные в п. 5.1 настоящей Политики и законе.

6.2. Согласие субъекта на обработку персональных данных запрашивается Компанией в форме, предусмотренной законом. Согласие считается действительным, если оно дано субъектом добровольно, на конкретные цели, будучи информированным о предполагаемой обработке и принятым осознанно. Согласие должно быть выражено четко и недвусмысленно. В случаях, требуемых законом, согласие оформляется в письменном виде (в том числе электронном документе, подписанном ЭЦП). Запрос на получение согласия формулируется Компанией таким образом, чтобы он был понятен и выделен из иных положений (если содержится в составе другого документа). Субъект персональных данных имеет право отозвать данное ранее согласие в любой момент (см. п. 4.2.4), при этом процедура отзыва согласия не должна быть сложнее, чем процедура его предоставления.

6.3. Обработка персональных данных, разрешенных субъектом для распространения (общедоступных персональных данных). Если субъект персональных данных принял решение предоставить определенные свои

данные для общего доступа неограниченному кругу лиц (например, для публикации на веб-сайте, в общедоступном справочнике, профиле и т.п.), он должен дать отдельное явное согласие на обработку таких персональных данных, разрешенных для распространения. Компания организует получение такого письменного согласия отдельно от иных согласий субъекта. После получения согласия на распространение Компания в течение 3 (трех) рабочих дней публикует информацию об условиях обработки этих персональных данных (включая перечень данных, цели и ограничения на их обработку неограниченным кругом лиц). Если субъект установил запреты или условия для неограниченного круга лиц на обработку своих данных (при даче согласия), Компания обязана соблюдать указанные ограничения. Согласие на распространение данных действует до момента поступления от субъекта требования о прекращении их распространения (см. п. 4.2.4 выше); после получения такого требования Компания прекращает дальнейшее распространение данных в течение срока, установленного законом.

6.4. Обработка биометрических персональных данных (содержащих информацию о физиологических и биологических особенностях человека, на основе которых можно установить его личность, например, отпечатки пальцев, изображение лица для системы распознавания, данные дактилоскопии или иные параметры) допускается только при наличии письменного согласия субъекта персональных данных, за исключением случаев, прямо предусмотренных законодательством Кыргызской Республики. Компания осуществляет биометрическую идентификацию личности (цифровую аутентификацию) только в случаях, когда это необходимо для целей обработки (например, для обеспечения информационной безопасности, для выполнения законодательных требований по идентификации клиентов) и на основании согласия или иного законного основания.

6.5. Обработка персональных данных в Компании может осуществляться как с помощью средств автоматизации, так и без них (неавтоматизированным способом). В случае автоматизированной обработки персональные данные хранятся и обрабатываются в информационных системах (базах данных) Компании, имеющих необходимый уровень защиты. При неавтоматизированной (ручной) обработке персональные данные содержатся в документах на бумажных носителях, систематизированных определенным образом (в картотеках, досье, реестрах и пр.). Независимо от способа обработки, Компания соблюдает принципы, ограничения и требования, установленные законодательством Кыргызской Республики для защиты прав субъектов (включая принципы, изложенные в п. 1.5 настоящей Политики).

6.6. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки. Срок хранения персональных данных может быть установлен законодательством или договором с участием субъекта – в таких случаях данные хранятся в соответствии с указанными требованиями. Если обязательный срок хранения не установлен, персональные данные хранятся не дольше, чем необходимо для целей их получения и дальнейшей обработки. По достижении целей обработки либо при утрате необходимости в их достижении данные подлежат уничтожению либо обезличиванию (если только их сохранение не требуется законом, например, для архивных целей, статистики, либо в интересах самого субъекта). Обрабатываемые персональные данные также подлежат уничтожению в случае поступления от субъекта законного требования об их удалении (см. раздел 10).

6.7. Персональные данные субъектов хранятся Компанией как на бумажных носителях, так и в электронном виде. Документы, содержащие персональные данные на бумаге, хранятся в специальных местах (в архивных комнатах, шкафах, сейфах), обеспечивающих защиту от несанкционированного доступа, порчи или утраты документов. Электронные базы данных, содержащие персональные данные, размещаются на защищенных серверах или в облачных хранилищах, сертифицированных для работы с персональными данными, с использованием современных средств защиты информации (средства резервного копирования, системы контроля доступа, антивирусная защита, шифрование и др.).

6.8. Сроки хранения (удержания) конкретных видов документов и персональных данных определяются номенклатурой дел Компании, внутренними приказами и иными организационно-распорядительными документами. По истечении установленного срока хранения документы (носители), содержащие персональные данные, подлежат своевременному уничтожению установленным порядком (см. раздел 10). Если документы с персональными данными представляют архивную ценность, вопрос об их дальнейшем хранении решается в соответствии с законодательством об архивном деле.

7. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ ОсОО «Миллианс»

7.1. При передаче (предоставлении) персональных данных субъектов третьим лицам Компания соблюдает следующие правила и требования:

7.1.1 Компания не раскрывает и не передает персональные данные субъекта персональных данных третьей стороне без письменного согласия субъекта, за исключением случаев, когда такая передача необходима в целях предотвращения угрозы жизни или здоровью самого субъекта либо иных лиц, а также случаев, предусмотренных законодательством Кыргызской Республики (например, передачи по законному требованию суда, следственных органов, при исполнении обязанности по закону и т.п.). В частности, персональные данные не сообщаются посторонним организациям или лицам в коммерческих целях без предварительного согласия субъекта.

7.1.2 Если персональные данные субъекта сообщаются третьему лицу, Компания предупреждает получателя о том, что данные могут использоваться исключительно в тех целях, для которых они были предоставлены. Компания требует от получателя подтверждения, что указанное правило им соблюдено (например, включает соответствующее условие в договор с получателем или берет расписку о соблюдении конфиденциальности). Все лица, получающие персональные данные субъекта, обязаны соблюдать их конфиденциальность и обеспечивать безопасность данных. Данное положение не распространяется на случаи, когда персональные данные передаются на основании закона уполномоченным органам в установленном порядке – в таких случаях порядок использования данных определяется самим законом.

7.1.3 В пределах Компании персональные данные сотрудников и клиентов передаются (раскрываются) в соответствии со специальными внутренними нормативными документами и приказами, определяющими перечень лиц, имеющих доступ к той или иной категории данных. С этими документами соответствующие сотрудники ознакамливаются под подпись. Доступ сотрудников Компании к персональным данным коллег или клиентов разрешается только в пределах должностных обязанностей и полномочий таких сотрудников и при условии соблюдения конфиденциальности.

7.1.4 Доступ к персональным данным субъектов предоставляется в Компании только специально уполномоченным работникам, которым такие данные необходимы для выполнения своих трудовых (служебных) обязанностей. Каждое структурное подразделение Компании определяет круг должностей (работников), которым требуется доступ к тем или иным персональным данным (например, кадровая информация доступна работникам отдела кадров, расчетные данные – бухгалтерии, данные клиентов – сотрудникам подразделения по работе с клиентами и службе безопасности, и т.д.). Эти сотрудники допускаются к персональным данным на основании приказа (распоряжения) руководства Компании и обязаны соблюдать режим конфиденциальности.

7.1.5 Компания не запрашивает и не передает информацию о состоянии здоровья субъекта персональных данных третьим лицам, за исключением тех сведений, которые относятся к вопросу о возможности выполнения субъектом своих трудовых обязанностей или условий договора с Компанией, либо в иных случаях, разрешенных законом (например, передача сведений о травме на производстве в уполномоченные органы). Медицинские данные сотрудников предоставляются внутри Компании только медицинскому персоналу (если таковой имеется) либо строго ограниченному кругу лиц в отделе кадров сугубо для целей выполнения требований трудового законодательства (например, сведения о нетрудоспособности для расчета пособий).

7.1.6 Персональные данные работника могут передаваться представителям работников (например, уполномоченным лицам профсоюза) в случаях и порядке, установленном трудовым законодательством Кыргызской Республики. При этом объем предоставляемых данных ограничивается только теми сведениями, которые необходимы указанным представителям для выполнения их функций по защите прав работников. Аналогично, данные клиента или иного субъекта могут быть предоставлены его представителю (законному представителю, доверенному лицу) при предъявлении надлежащих полномочий и только в объеме, необходимом для реализации поручения.

7.2. Трансграничная передача персональных данных

7.2.1 Передача персональных данных в электронном виде или на материальных носителях на территорию зарубежных государств (трансграничная передача) осуществляется Компанией в строгом соответствии с требованиями законодательства Кыргызской Республики. До осуществления трансграничной передачи персональных данных Компания обязана убедиться, что в государстве, на территорию которого передаются данные, обеспечивается адекватная защита прав субъектов персональных данных.

7.2.2 Трансграничная передача персональных данных на территорию государств, включенных в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется на тех же условиях и в тех же целях, что и обработка данных на территории Кыргызской Республики. Передача данных в такие страны не требует получения специального разрешения и не может быть запрещена, если соблюдаются общие требования закона и цели обработки соответствуют заявленным.

7.2.3 Трансграничная передача персональных данных в страны, не обеспечивающие адекватной защиты прав субъектов (не включенные в указанный перечень уполномоченного органа) допускается только при наличии одного из следующих условий:

- субъект персональных данных дал явное согласие на такую трансграничную передачу;
- трансграничная передача предусмотрена международным договором Кыргызской Республики;
- передача необходима для защиты основ конституционного строя Кыргызской Республики, обеспечения обороны страны, безопасности государства либо иных общественно значимых интересов в случаях, предусмотренных законом;
- передача необходима для исполнения договора между Компанией и субъектом персональных данных (либо для заключения договора по запросу субъекта), а также в случаях, когда субъект является стороной договора, заключенного в его интересах между Компанией и третьим лицом;
- передача необходима для защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц, когда получение согласия субъекта невозможно;
- передача осуществляется во исполнение договора между Компанией и иностранным субъектом (например, иностранным обработчиком или партнером), при условии что таким договором обеспечивается надлежащая защита прав субъектов персональных данных. Необходимые условия такого договора определяются уполномоченным органом по защите персональных данных.

7.2.4 В каждом случае трансграничной передачи Компания соблюдает требования законодательства страны назначения в части обработки передаваемых данных, если это прямо установлено международным договором или законом. При передаче данных иностранному получателю Компания ставит условие о соблюдении конфиденциальности и принятии мер защиты данных со стороны получателя.

7.3. Компания ведет учет переданных за пределы Кыргызской Республики персональных данных и стран-получателей в порядке, предусмотренном внутренними процедурами и нормативными актами уполномоченного органа. В случае инцидента, повлекшего утечку персональных данных при трансграничной передаче, Компания незамедлительно информирует уполномоченный орган и действует согласно его предписаниям и планам реагирования.

8. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ ВНУТРИ КОМПАНИИ И ПО ВНЕШНИМ ЗАПРОСАМ

8.1. Внутри Компании доступ к персональным данным субъектов персональных данных (как сотрудников, так и клиентов, контрагентов) имеют только те работники, которым такой доступ необходим для выполнения их трудовых функций:

8.1.1 Директор Компании - доступ к любым персональным данным, обрабатываемым в Компании, в силу занимаемой должности и ответственности за организацию обработки данных.

8.1.2 Руководитель отдела кадров (службы управления персоналом) – доступ к персональным данным работников, кандидатов, стажеров в объеме, необходимом для выполнения функций по подбору, ведению кадрового делопроизводства, учета персонала, социальных выплат и иных трудовых вопросов.

8.1.3 Руководители структурных подразделений – доступ к персональным данным работников соответствующего подразделения (отдела, отдела), а также к релевантным данным клиентов или контрагентов в рамках проектов данного подразделения, в объеме, согласованном с руководством Компании. Например, руководитель отдела по работе с клиентами имеет доступ к данным клиентов данного отдела; руководитель технического отдела – к данным, необходимым для технической поддержки пользователей, и т.д.

8.1.4 В случае перевода работника из одного подразделения в другое его новый руководитель может получить доступ к персональным данным этого работника (личному делу, данным о заработной плате и пр.) только после оформления соответствующего доступа с согласия директора Компании.

8.1.5 Работники бухгалтерии и финансовой службы – доступ к персональным данным, необходимым для начисления заработной платы, выполнения расчетов с работниками и контрагентами, уплаты налогов и взносов, подготовки финансовой отчетности (например, к данным сотрудников о окладах, ИНН, к реквизитам контрагентов-физических лиц для оплаты услуг и др.).

8.1.6 Работники подразделений, обслуживающих клиентов – доступ к персональным данным клиентов и потенциальных клиентов, необходимым для проведения идентификации, проверки, обслуживания запросов клиентов, мониторинга операций, обеспечения безопасности и выполнения иных обязанностей, возложенных на

эти подразделения. Объем предоставляемых таким сотрудникам данных определяется внутренними инструкциями с учетом принципа минимально необходимых привилегий.

8.1.7 Сам субъект персональных данных (носитель данных) – доступ к своим собственным персональным данным (например, работник имеет право ознакомиться со своим личным делом, клиент – с данными своего аккаунта и историей операций и т.д.).

8.1.7 Каждый работник, имеющий доступ к персональным данным, действует в пределах предоставленных ему полномочий и только в интересах достижения целей обработки. Перед получением доступа работник подписывает обязательство о неразглашении персональных данных и проходит ознакомление с настоящей Политикой и другими инструкциями по безопасности данных.

8.2. Внешние запросы и предоставление данных без согласия субъекта. В ряде случаев законодательство разрешает предоставлять персональные данные третьим лицам без получения согласия субъекта. Компания тщательно проверяет любые внешние запросы и предоставляет данные только при наличии законных оснований. К случаям, когда согласие субъекта не требуется, относятся:

8.2.1 передача персональных данных уполномоченным органам в целях защиты жизни и здоровья субъекта либо иных лиц, когда субъект не в состоянии самостоятельно дать согласие. Например, в экстренной ситуации (несчастный случай, резкое ухудшение здоровья на рабочем месте) Компания может предоставить медицинским работникам или правоохранительным органам информацию о человеке для спасения его жизни;

8.2.2 направление сведений о работниках и иных физических лицах во внебюджетные фонды (Фонд пенсионного и социального страхования Кыргызской Республики) в объеме, предусмотренном действующим законодательством (например, для начисления пенсий, пособий, взносов социального страхования и т.п.);

8.2.3 предоставление необходимых персональных данных в налоговые органы – в пределах, установленных налоговым законодательством (например, сведения о доходах физических лиц, о выплаченных вознаграждениях, для целей налогообложения и отчетности);

8.2.4 предоставление информации по мотивированному запросу органов прокуратуры – если такой запрос оформлен в соответствии с требованиями закона и связан с проверкой или надзорными мероприятиями прокуратуры;

8.2.5 предоставление информации по мотивированному требованию правоохранительных органов или органов национальной безопасности (например, полиции, следственных органов, государственных служб национальной безопасности) – в рамках их компетенции (оперативно-розыскные мероприятия, следствие, контртеррористическая деятельность и др.) и в порядке, установленном соответствующими процессуальными нормами;

8.2.6 предоставление необходимых сведений по запросу государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности – в пределах их полномочий (например, предоставление документов по трудовым вопросам при проверке);

8.2.7 раскрытие персональных данных по постановлению суда либо по запросу суда в связи с рассмотрением гражданского, административного или уголовного дела – в объеме, предписанном запросом суда;

8.2.8 уведомление компетентных органов и организаций о тяжелом несчастном случае (в том числе со смертельным исходом), связанном с деятельностью Компании или произошедшем на территории Компании, – передача минимально необходимой информации о пострадавшем лице (Ф.И.О., должность, характер травмы или причина смерти и т.д.) в органы, которые должны быть уведомлены согласно законодательству (например, правоохранительные органы, госинспекция труда, Фонд социального страхования);

8.2.9 предоставление персональных данных в иных случаях, связанных с исполнением работником должностных обязанностей и вытекающих из трудовых отношений. Например, передача сведений о сотруднике в командующее предприятие при служебной командировке, либо предоставление данных о сотруднике-заемщике по запросу банка при выдаче ему кредита (если такое предоставление предусмотрено законом). Во всех перечисленных случаях Компания строго соблюдает пределы и объем данных, которые разрешено сообщать без согласия субъекта. Передача данных фиксируется (при необходимости составляется акт или делается отметка в журнале выдачи данных).

8.3. Запросы от других организаций. Если персональные данные субъекта (в том числе уволенного сотрудника) запрашиваются другой организацией (например, для подтверждения стажа работы, предоставления характеристики, проверки рекомендаций при приеме на работу и др.), Компания предоставляет такие данные только при получении официального письменного запроса от организации. Запрос должен быть оформлен на бланке этой организации с указанием цели запроса и перечня запрашиваемых сведений. Также желательно

наличие копии согласия субъекта (или его личного заявления) о предоставлении информации в данную организацию. В ответе на запрос Компания указывает только те данные, которые запрошены и необходимы для заявленной цели, избегая излишней информации. Ответ предоставляется в письменной форме на официальном бланке Компании и подписывается уполномоченным лицом.

8.4. Предоставление данных родственникам и членам семьи. Персональные данные субъекта (как сотрудника, так и клиента) могут быть предоставлены его близким родственникам или членам семьи только при наличии письменного разрешения самого субъекта персональных данных либо при наличии законных оснований (например, законному представителю недееспособного лица). В ситуациях, не терпящих отлагательства (например, доставка пострадавшего сотрудника в больницу), минимально необходимые сведения могут быть переданы близким родственникам без формального согласия, но с последующим уведомлением субъекта (когда это станет возможным) или его законных представителей.

8.5. Все внешние запросы, поступающие в Компанию (как по официальным каналам, так и от частных лиц), регистрируются и рассматриваются ответственными сотрудниками с точки зрения законности предоставления персональных данных. Компания вправе запросить у инициатора запроса уточняющие документы (например, предоставить нотариально заверенную доверенность представителя, решение суда, ссылку на норму закона, обязывающую предоставить данные и т.п.). При малейших сомнениях в законности или добросовестности запроса – Компания отказывает в предоставлении данных, мотивируя отказ соответствующими положениями закона.

9. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ (ЗАЩИТА ПД)

9.1. Компания принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, утечки, а также от иных неправомерных действий. В целях обеспечения безопасности персональных данных внутри Компании реализована система защиты, включающая:

9.1.1 Разграничение прав доступа. Назначен ответственный за защиту персональных данных. Определены категории работников, которым предоставляется доступ к персональным данным, а также уровень доступа (какие действия можно совершать с данными). Доступ на уровне информационных систем защищается механизмами аутентификации (имя пользователя, паролей, двухфакторной аутентификации и/или цифровой подписи). Каждый пользователь информационной системы имеет уникальные учетные данные; права доступа распределяются по ролям в соответствии с должностными обязанностями.

9.1.2 Обучение и обязательства сотрудников. Все работники, допущенные к работе с персональными данными, проходят инструктаж по правилам обращения с такими данными и подписывают соглашение о неразглашении (NDA). Внутренними регламентами Компании установлены правила обращения с персональными данными (как в бумажном виде, так и в электронных системах). Проводятся периодические тренинги и информирование персонала о актуальных угрозах безопасности данных и способах их предотвращения.

9.1.3 Физическая защита носителей. Документы и другие носители, содержащие персональные данные, хранятся в условиях, исключающих доступ к ним посторонних лиц. Бумажные документы хранятся в закрывающихся шкафах, сейфах, помещениях с ограниченным доступом. Доступ в архивы и помещения, где обрабатываются персональные данные, разрешен только уполномоченным лицам. При уходе ответственных сотрудников с рабочего места документы убираются в защищенные места хранения (реализуется политика «чистого стола»).

9.1.4 Защита информационных систем. Персональные данные в электронном виде хранятся в защищенных информационных системах. Серверы и компьютеры, на которых хранятся данные, оснащены актуальными средствами защиты: антивирусное программное обеспечение, межсетевые экраны системы обнаружения вторжений, средства шифрования каналов связи и шифрования хранящихся данных. Для доступа к компьютерам и системам используются пароли, которые периодически изменяются согласно политике Компании. Внедрена многоуровневая система резервного копирования, чтобы предотвратить утрату данных.

9.1.5 Цифровая аутентификация и подпись. Для обеспечения контроля доступа и целостности данных используются современные методы цифровой идентификации и аутентификации пользователей. В необходимых случаях Компания применяет цифровую подпись для подтверждения подлинности электронных документов и неизменности данных. Цифровая подпись позволяет удостовериться, что электронный документ (например, соглашение, запрос субъекта или согласие на обработку) не изменялся и исходит именно от того лица, которое его подписало. Это снижает риски несанкционированных изменений и фальсификации данных в цифровой среде.

9.1.6 Регистрация операций и мониторинг. В информационных системах Компании ведется журнал (лог) операций с персональными данными: фиксируются действия пользователей (просмотр, изменение, удаление,

передача данных), время и ответственные лица. Эти логи регулярно просматриваются ответственным за безопасность для выявления подозрительных действий. Система безопасности настроена на уведомление администраторов при обнаружении аномальной активности или попыток несанкционированного доступа.

9.1.7 Контроль передачи данных. Передача персональных данных по открытым каналам связи (телефон, факс, электронная почта без шифрования) запрещается, если на это нет прямого разрешения субъекта и уверенности в защищенности канала. По электронной почте персональные данные пересылаются только в зашифрованном виде или через защищенные корпоративные системы обмена сообщениями. Запрещается выносить за пределы офиса документы, содержащие конфиденциальные персональные данные, без разрешения руководства. При необходимости передачи данных внешним получателям заключаются соглашения о защите данных или используются обезличенные/обобщенные сведения.

9.1.8 Антишпионские меры и обновления. На рабочих станциях отключены несогласованные средства копирования информации (например, запрет несанкционированного использования внешних USB-накопителей). Программное обеспечение, используемое для обработки персональных данных, регулярно обновляется для устранения выявленных уязвимостей. Проводятся аудиты безопасности и тестирование на проникновение (pen-test) при внедрении новых систем, чтобы изначально учесть требования безопасности (принцип «защита данных по умолчанию и на этапе проектирования»).

9.1.9 Взаимодействие с госорганами по инцидентам. Компания обеспечивает взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Кыргызской Республики. В частности, при выявлении компьютерного инцидента, повлекшего неправомерную передачу (утечку) персональных данных либо иное нарушение их безопасности, Компания оперативно информирует компетентный государственный орган (например, службу реагирования на компьютерные инциденты) и действует согласно инструкциям по ликвидации последствий. Проводится служебное расследование причин инцидента; пострадавшим субъектам персональных данных направляется уведомление в случаях, предусмотренных законодательством или внутренними политиками.

9.2. Все сотрудники Компании, допущенные к обработке персональных данных, несут персональную ответственность за соблюдение требований конфиденциальности и обеспечения безопасности данных. За нарушение установленных правил к работникам могут применяться дисциплинарные взыскания, вплоть до увольнения, а также иные меры ответственности согласно разделу 11 настоящей Политики.

9.3. Компания регулярно актуализирует меры защиты персональных данных с учетом изменений законодательства, появления новых технологий защиты и актуальных угроз. Политики и процедуры безопасности пересматриваются не реже одного раза в год, а также после значимых инцидентов или изменений в информационных системах.

10. ПОРЯДОК АКТУАЛИЗАЦИИ, УДАЛЕНИЯ И УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Компания обеспечивает актуализацию (обновление, корректировку) обрабатываемых персональных данных по мере необходимости. Если субъект обращается с заявлением о том, что его персональные данные являются неполными или неточными, Компания в кратчайший срок проверяет и вносит необходимые исправления. На период проверки по запросу субъекта спорные данные могут быть временно заблокированы (приостановлена их обработка).

10.2. В случае подтверждения факта недостоверности персональных данных или неправомерности их обработки Компания осуществляет блокирование таких персональных данных или, если исправление невозможно, их уничтожение. Блокирование данных означает временное прекращение любых операций с ними (за исключением хранения) до устранения причин неправомерной обработки. Если выявлено, что персональные данные были получены или обрабатываются незаконно (например, без необходимого согласия или иного законного основания), Компания прекращает обработку таких данных и устраняет нарушение – удаляет либо уничтожает незаконно полученные сведения.

10.3. Удаление и уничтожение персональных данных. Условиями прекращения обработки и основаниями для удаления/уничтожения персональных данных являются: достижение целей, ради которых данные обрабатывались; истечение установленных сроков хранения; отзыв субъектом согласия (если данные обрабатывались только на основании согласия и отсутствуют иные законные основания обработки); вынесение уполномоченным органом или судом решения о необходимости удаления (уничтожения) данных; а также иные основания, предусмотренные законодательством. При наступлении любого из этих условий Компания

немедленно (без необоснованной задержки) прекращает активную обработку соответствующих персональных данных и приступает к процедуре их удаления или уничтожения.

10.3.1 Удаление персональных данных – это исключение (стирание) данных из информационных систем Компании таким образом, что восстановление содержания персональных данных без специальных знаний и средств становится невозможным. Удаленные электронные данные подлежат также исключению из резервных копий (при ближайшей ротации бэкапов, если непосредственное удаление технически затруднительно). Персональные данные на бумажных носителях считаются удаленными после того, как соответствующие страницы (записи) изъяты из документов либо сами документы изъяты из дела для последующего уничтожения.

10.3.2 Уничтожение персональных данных – физическое уничтожение носителей, на которых содержатся персональные данные, либо приведение персональных данных в форму, не поддающуюся восстановлению. Документы на бумажном носителе уничтожаются посредством shreddera (механического измельчения) либо сжигания в присутствии комиссии. Электронные носители (жесткие диски, флеш-накопители, оптические диски), содержащие конфиденциальные персональные данные, уничтожаются путем разрушения или стираются с применением специальных программ без возможности восстановления.

10.4. Процедура уничтожения персональных данных в Компании регламентируется отдельным внутренним документом – Положением о порядке уничтожения персональных данных (либо соответствующим разделом в настоящей Политике). Уничтожение персональных данных производится комиссией, назначенной приказом руководителя, либо уполномоченным должностным лицом с составлением акта об уничтожении.

10.5. Акт об уничтожении персональных данных является документом, подтверждающим факт и дату уничтожения, составом комиссии и способом уничтожения. В акте перечисляются категории (виды) уничтоженных персональных данных или документов. Копия акта об уничтожении персональных данных может быть предоставлена субъекту персональных данных по его письменному запросу.

10.6. По общему правилу, после истечения срока хранения и (или) достижения целей сбора персональных данных, указанные данные подлежат уничтожению в течение 2 (двух) недель (14 календарных дней), если иное не установлено внутренними регламентами или не требуется в интересах субъекта. Если по истечении срока хранения персональных данных, установленного для конкретного вида документов, эти документы не были уничтожены (например, из-за того что они необходимы для расследования, судебного разбирательства, аудиторской проверки), ответственное лицо обязано обосновать продление хранения и обеспечить уничтожение данных сразу после отпадения причин задержки.

10.7. Обезличивание (анонимизация) персональных данных может использоваться Компанией как альтернатива уничтожению, если последующее хранение обезличенных данных необходимо для статистических, научных или иных законных целей. Обезличивание осуществляется таким способом, чтобы определить по обезличенным данным конкретного субъекта было невозможно даже с привлечением дополнительной информации.

11. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Субъект персональных данных несет ответственность за предоставление Компании недостоверных сведений или подложных документов при заключении договора или в процессе отношений с Компанией. Представление ложных или фальсифицированных персональных данных может служить основанием для отказа в заключении договора, либо для его расторжения (прекращения) в одностороннем порядке со стороны Компании, а также для отказа в предоставлении услуг. В трудовых отношениях предоставление подложных документов при поступлении на работу является грубым нарушением, способным повлечь прекращение трудового договора по инициативе работодателя.

11.2. Лица, виновные в нарушении требований законодательства Кыргызской Республики и норм настоящей Политики при обработке персональных данных, несут ответственность в установленном порядке. В зависимости от характера нарушения и его последствий, виновные могут быть привлечены:

11.2.1 к дисциплинарной ответственности - замечание, выговор, строгий выговор, увольнение и др. меры согласно Трудовому кодексу КР;

11.2.2 к материальной ответственности – обязанность возместить ущерб, причиненный Компании вследствие нарушения (например, штрафные санкции, взыскание стоимости утраченного имущества, компенсация репутационного вреда, выплата возмещений субъектам за причиненный ущерб и т.п.), в пределах, установленных трудовым законодательством;

11.2.3 к гражданско-правовой ответственности – возмещение имущественного вреда, причиненного субъекту персональных данных или другим лицам, в порядке гражданского судопроизводства;

11.2.4 к административной ответственности – уплата административного штрафа, назначенного уполномоченным органом или судом, за совершение административного правонарушения в области защиты персональных данных (например, нарушение правил обработки, утечка данных и пр.), согласно Кодексу КР о нарушениях;

11.2.5 к уголовной ответственности – в случаях, когда нарушение законодательства о персональных данных содержит признаки состава преступления (например, незаконный сбор или распространение сведений о частной жизни, повлекшие существенный вред гражданину), виновные лица могут понести наказание по приговору суда (штраф, исправительные работы, лишение свободы и др.) согласно Уголовному кодексу КР.

11.3. Если в результате неправомерной обработки персональных данных Компанией субъекту причинены убытки или моральный вред, субъект вправе требовать полного возмещения причиненных убытков, а морального вреда – в размере, определенном соглашением сторон или судом. Компания несет ответственность перед субъектом в пределах, установленных гражданским законодательством Кыргызской Республики.

11.4. В случае утечки персональных данных (неправомерного доступа посторонних лиц к персональным данным) по вине сотрудников Компании либо вследствие недостаточности мер защиты, Компания проводит внутреннее расследование, информирует уполномоченный госорган (если это требуется по закону) и принимает меры для устранения последствий. За допущенную утечку ответственные лица привлекаются к дисциплинарной ответственности, а при наличии ущерба для субъектов – могут быть применены меры материальной ответственности или другие санкции.

12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ ОсОО «Миллианс»

12.1. Вопросы, не урегулированные настоящей Политикой или другими внутренними документами Компании, регулируются непосредственно нормами законодательства Кыргызской Республики о персональных данных. Условием применения нормативного акта в Компании является его официальное опубликование и вступление в силу в установленном порядке.

12.2. Если какое-либо положение (норма) настоящей Политики будет признано недействительным, это не влечет за собой недействительность остальных положений Политики. В таком случае вместо недействительной нормы применяется норма законодательства либо вводится новая норма, максимально приближенная по смыслу и цели к исходной и допущенная законодательством. Недействительная норма подлежит изменению при ближайшей актуализации Политики.

12.3. Настоящая Политика доводится до сведения всех сотрудников Компании под подпись. При необходимости (с учетом характера деятельности) ключевые положения Политики могут быть доведены до сведения контрагентов, партнеров и клиентов (например, путем размещения Политики или ее выдержек на официальном сайте Компании, включения в соглашения с клиентами условий об обработке данных). Все изменения и/или дополнения к настоящей Политике также подлежат доведению до сведения сотрудников в порядке, предусмотренном п. 1.6. Работники, непосредственно осуществляющие обработку персональных данных, должны не только ознакомиться, но и руководствоваться положениями настоящей Политики в своей повседневной работе.

12.4. Компания оставляет за собой право вносить изменения в настоящую Политику в любой момент, в связи с изменением законодательства или внутренних процедур. При внесении изменений в текст Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее утверждения и размещения в открытом доступе (например, на внутреннем портале Компании или официальном сайте) для ознакомления, при условии обязательного предварительного объявления сотрудникам и иным затронутым лицам о планируемых изменениях не менее чем за 14 (четырнадцать) рабочих дней до даты введения новой редакции.

12.5. Контроль исполнения настоящей Политики осуществляет ответственное лицо, назначенное приказом по Компании, а также руководство Компании. Политика пересматривается на регулярной основе на предмет соответствия актуальным требованиям законодательства и деятельности Компании.