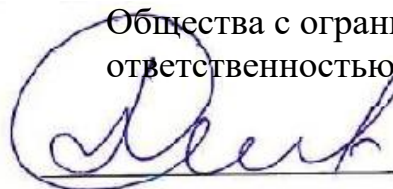


Приложение к приказу
№ 74 от 04.04.2016

УТВЕРЖДАЮ:

Генеральный директор
Общества с ограниченной
ответственностью «УК Креатив»

 А.А. Винокурова



ПОЛОЖЕНИЕ
о защите персональных данных клиентов, контрагентов и
работников
ООО «УК Креатив»

1. Общие положения

1.1. Настоящее Положение разработано в целях защиты персональных данных клиентов, работников и контрагентов ООО «УК Креатив» (далее – Общество).

1.2. Настоящее Положение устанавливает порядок получения, учета, обработки, хранения персональных данных клиентов, работников и контрагентов Общества.

1.3. Положение разработано в соответствии с Конституцией РФ, ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» и иных нормативно-правовых актов, регулирующих использование персональных данных.

1.4. В настоящем Положении используются следующие термины и определения:

Оператор – ООО «УК Креатив» (далее Общество), вступившее в договорные отношения с клиентом, работником или контрагентом или оказывающее услуги физическому лицу, юридическому лицу или индивидуальному предпринимателю.

Клиент – физическое лицо, официальный представитель – физическое лицо юридического лица и индивидуального предпринимателя, вступившее в договорные отношения по оказанию услуг с Обществом

Контрагент – физическое лицо, представитель – физическое лицо юридического лица и индивидуального предпринимателя, вступившие с Обществом в договорные отношения.

Работник – физическое лицо, работающее по трудовому договору с Обществом и получающее за это заработную плату.

Персональные данные Клиента – информация, необходимая Оператору в связи с договорными отношениями и касающаяся конкретного Клиента, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, паспортные данные, социальное положение, имущественное положение, образование, профессия, специальность, занимаемая должность, доходы, ИНН, сведения ВУС, СНИЛС, сведения о трудовом и общем стаже, адрес электронной почты, телефон, место работы или учебы членов семьи и родственников, состав декларируемых сведений о наличии материальных ценностей, содержание декларации, подаваемой в налоговую инспекцию, налоговый статус (резидент/нерезидент), иные сведения указанные заявителем.

Персональные данные Контрагента – информация, необходимая Оператору в связи с договорными отношениями и касающаяся конкретного Контрагента, в том числе фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, паспортные данные, социальное положение, имущественное положение, образование, профессия, специальность, занимаемая должность, доходы, ИНН, сведения ВУС, СНИЛС, сведения о трудовом и общем стаже, адрес электронной почты, телефон, место работы или учебы членов семьи и родственников, состав декларируемых сведений о наличии материальных ценностей, содержание декларации, подаваемой в налоговую инспекцию, налоговый статус (резидент/нерезидент), иные сведения указанные заявителем.

Персональные данные Работника – информация, необходимая Оператору в связи с договорными отношениями и касающаяся конкретного Работника, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, паспортные данные, социальное положение, имущественное положение, образование, профессия, специальность, занимаемая должность, доходы, ИНН, сведения ВУС, СНИЛС, сведения о трудовом и общем стаже, адрес электронной почты, телефон, место работы или учебы членов семьи и родственников, состав декларируемых сведений о наличии материальных ценностей, содержание декларации, подаваемой в налоговую инспекцию, налоговый статус (резидент/нерезидент), иные сведения указанные заявителем.

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

Субъект персональных данных – Клиент, Контрагент, Работник.

Защита персональных данных Клиента, Контрагента или Работника – деятельность Общества по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации.

Актуальные угрозы безопасности персональных данных - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе персональных данных, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Подразделение по работе с персоналом –сотрудник Общества, на которого возложены обязанности по работе с персоналом.

1.5. Действия настоящего Положения распространяется на всех Клиентов, Работников и Контрагентов Общества.

2. ПРАВИЛА ПРЕДОСТАВЛЕНИЯ ДОСТУПА РАБОТНИКОВ К ПЕРСОНАЛЬНЫМ ДАННЫМ

2.1. Список лиц, допущенных к обработке персональных данных (далее Список) и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение правил обработки персональных данных, определяется и утверждается Генеральным директором Общества.

2.3. Подразделение по работе с персоналом, не реже одного раза в квартал, обязано проверять актуальность Списка. В случае выявления расхождений, Подразделение по работе с персоналом вносит изменения в Список.

2.4. Работники Общества выполняют действия по обработке персональных данных в соответствии с возложенными на Работников функциями.

2.5. Доступ к персональным данным предоставляется только лицам, замещающим должности из Списка.

2.6. Работники имеют доступ на ввод и коррекцию персональных данных в пределах, определенных должностными обязанностями.

2.7. Лица, получившие доступ к персональным данным, должны хранить в тайне известные им сведения конфиденциального характера и информировать об утечке персональных данных, о фактах нарушения порядка обращения с ними, о попытках несанкционированного доступа к персональным данным.

2.8. Лица, получившие доступ к персональным данным, должны использовать эти данные лишь в целях, для которых они сообщены, обязаны соблюдать режим конфиденциальности и дать Обязательство о неразглашении персональных данных.

2.9. Общество обеспечивает неограниченный доступ к сведениям о реализуемых требованиях к защите персональных данных.

3. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Персональные данные Клиента, Работника или Контрагента относятся к категории конфиденциальной информации.

3.2. В целях обеспечения прав и свобод человека и гражданина Оператор и его представители при обработке персональных данных Клиента, Работника или Контрагента обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных должна осуществляться на законной и справедливой основе, исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия выполнения договорных обязательств в соответствии с законодательством РФ;

3.2.2. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных за исключением случаев, предусмотренных законодательством Российской Федерации, когда обработка персональных данных допускается без согласия субъекта персональных данных, при условии регламентации вопросов обработки персональных данных соответствующим законодательством Российской Федерации;

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

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

3.2.5. Обработке подлежат только персональные данные, которые отвечают целям их обработки; 3.2.6. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

3.2.7. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

3.2.8. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

3.2.9. Оператор не имеет права получать и обрабатывать персональные данные Клиента, Работника или Контрагента о его расовой, национальной принадлежности,

политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев, предусмотренных законодательством РФ;

3.2.10. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда Клиента, Работника или Контрагента, затруднения реализации его прав и свобод;

3.2.11. При принятии решений, затрагивающих интересы Клиента, Работника или Контрагента, Оператор не имеет права основываться на персональных данных Клиента, Работника или Контрагента, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.

3.3. При идентификации Клиента, Работника или Контрагента Общества может потребоваться предъявления документов, удостоверяющих личность и подтверждающих полномочия представителя.

3.4. При заключении договора, как и в ходе выполнения договора может возникнуть необходимость в предоставлении Клиентом иных документов, содержащих информацию о нем.

3.5. После принятия решения о заключении договора или представления документов, подтверждающих полномочия представителя, а так же впоследствии, в процессе выполнения договора, содержащего персональные данные Клиента, Работника или Контрагента, так же будут относиться:

- договоры;
- приказы по основной деятельности;
- служебные записки;
- приказы о допуске представителей Контрагента;
- разовые или временные пропуска;
- другие документы, где включение персональных данных Клиента, Работника или Контрагента необходимо согласно действующему законодательству.

3.6. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

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

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

4. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Все Работники, имеющие доступ к персональным данным Клиентов, Работников или Контрагентов, обязаны подписать обязательство о неразглашении персональных данных.

4.2. Защита персональных данных Клиентов, Работников или Контрагентов от неправомерного их использования или утраты обеспечивается Оператором в порядке, установленном законодательством РФ.

4.3. Клиенты, Работники или Контрагенты до предоставления своих персональных данных должны иметь возможность ознакомиться с настоящим Положением.

4.4. Защите подлежит:

- информация о персональных данных субъекта;
- документы, содержащие персональные данные субъекта;
- персональные данные, содержащиеся на электронных носителях.

4.5. Оператор назначает ответственного за организацию обработки персональных данных.

4.6. Оператор издает документы, определяющие политику оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

4.7. Оператор принимает необходимые правовые, организационные и технические меры или обеспечивает 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 в соответствии со статьей 19 Федерального закона от 27.07.2006 года №152-ФЗ «О персональных данных», в том числе:

1) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учет машинных носителей персональных данных;

6) обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) 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;

9) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

4.8. Оператор осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону от 27.07.2006 года №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

4.9. Оператор осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

4.10. Ознакомливает своих работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных

данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

4.11. Ответственные лица соответствующих подразделений, хранящих персональные данные на бумажных носителях и машинных носителях информации, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному Постановлением правительства РФ 15 сентября 2008 г. N 687.

4.12. Ответственные лица структурных подразделений, обрабатывающие персональные данные в информационных системах персональных данных и машинных носителях информации, обеспечивают защиту в соответствии с законодательством РФ.

5. ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Сведения о Клиентах, Работниках и Контрагентах хранятся на бумажных носителях в помещении Общества. Для хранения носителей используются специально оборудованные шкафы и сейфы.

5.2. Обязанности по хранению документов, где содержатся персональные данные Клиентов, Работников или Контрагентов, возлагаются на конкретного работника Общества и закрепляются в его должностной инструкции.

5.3. Ключи от шкафов и сейфов, в которых хранятся носители, находится у ответственного работника Общества, которому они передаются по Акту. При отсутствии данного работника используются дубликаты ключей, находящиеся у непосредственного начальника ответственного работника.

5.4. Персональные данные Клиентов, Работников или Контрагентов могут так же храниться в электронном виде, доступ к которым ограничен и регламентируется Оператором.

5.5. Доступ к персональным данным Клиентов, Работников или Контрагентов без специального разрешения имеют работники, занимающие в Обществе следующие должности: Генеральный директор, заместитель генерального директора, главный бухгалтер, бухгалтер, специалист по взысканию дебиторской задолженности, паспортист.

5.6. Внутренний доступ (доступ внутри организации) к персональным данным Клиентов, Работников или Контрагентов имеют работники, внесенные в список лиц, допущенных к обработке персональных данных.

5.7. Хранение персональных данных Клиента, Работника или Контрагента должно осуществляться в форме, позволяющей определить Клиента, Работника или Контрагента, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является Клиент, Работник или Контрагент. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Сроки хранения документов, содержащих персональные данные Клиента, Работника или Контрагента, определяются в соответствие со сроком действия договора с Клиентом, Работником или Контрагентом, сроком исковой давности, а также иными требованиями законодательства РФ.

5.8. Период хранения и обработки персональных данных определяется в соответствии с Законом «О персональных данных». Обработка персональных данных начинается с момента поступления персональных данных в информационные системы персональных данных и прекращается:

- в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, Общество устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений, Общество в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Общество уведомляет субъекта персональных данных или его законного представителя, а в случае, если

обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Общество уведомляет также указанный орган;

- в случае достижения цели обработки персональных данных Общество незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, и уведомляет об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Общество уведомляет также указанный орган;

- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Общество прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных Общество уведомляет субъекта персональных данных.

- в случае прекращения деятельности Общества.

6. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. При передаче персональных данных Клиента, Работника или Контрагента Оператор соблюдает следующие требования:

6.1.1. Не сообщает персональные данные Клиента, Работника или Контрагента третьей стороне без письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, при поступлении официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях», при поступлении официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Федерального социального страхования, судебных органов, а также в случаях, предусмотренных иными федеральными законами. Оператор в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же лицо, обратившееся с запросом, не уполномочено на получение персональных данных Клиента, Работника или Контрагента, либо отсутствует письменное согласие Клиента, Работника или Контрагента на предоставление его персональных сведений, либо, по мнению Оператора, присутствует угроза жизни или здоровью Клиента, Работника или Контрагента, Работодатель обязан отказать в предоставлении персональных данных лицу. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

6.1.2. Не сообщает персональные данные Клиента, Работника или Контрагента в коммерческих целях без его письменного согласия.

6.1.3. Предупреждает лиц, получающих персональные данные Клиента, Работника или Контрагента, 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. Лица, получающие персональные данные Клиент, Работника или Контрагента, обязаны соблюдать требования конфиденциальности.

6.1.4. Осуществляет передачу персональных данных Клиента, Работника или Контрагента в пределах своей организации в соответствии с настоящим Положением.

6.1.5. Разрешает доступ к персональным данным Клиентов, Работников или Контрагентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные Клиента, Работника или Контрагента, которые необходимы для выполнения конкретных функций. Лица, получающие персональные данные Клиента, Работника или Контрагента, обязаны соблюдать требования конфиденциальности.

6.1.6. Не запрашивает информацию о состоянии здоровья Клиента, Работника или Контрагента, за исключением тех сведений, которые относятся к вопросу о возможности выполнения Клиентом, Работника или Контрагентов своих представительских функций;

6.1.7. Передает персональные данные Клиента, Работника или Контрагента его представителям в порядке, установленном законодательством РФ, и ограничивает эту

информацию только теми персональными данными Клиента, Работника или Контрагента, которые необходимы для выполнения указанными представителями их функций.

6.2. В случае если Оператору оказываются услуги юридическими или физическими лицами на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным Клиентов, Работников или Контрагентов, то соответствующие данные предоставляются Оператором только после подписания с ними соглашения о конфиденциальности (неразглашении конфиденциальной информации).

6.3. Все сведения о передаче персональных данных Клиентов, Работников или Контрагентов регистрируются в Журнале учета передачи персональных данных в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана.

7. ОБЯЗАННОСТИ КЛИЕНТА, РАБОТНИКА, КОНТРАГЕНТА И ОПЕРАТОРА

7.1. В целях обеспечения достоверности персональных данных, Клиент, Работник или Контрагент обязан:

7.1.1. При заключении договора предоставить Оператору полные и достоверные данные о себе;

7.1.2. В случае изменения сведений, составляющих персональные данные Клиента, Работника или Контрагента, незамедлительно, но не позднее пяти рабочих дней, предоставить данную информацию Оператору.

7.2. Оператор обязан:

7.2.1. Обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты в порядке, установленном законодательством РФ;

7.2.2. Предоставить возможность Клиенту, Работнику, Контрагенту или их представителям ознакомиться с настоящим Положением и его правами в области защиты персональных данных;

7.2.3. Обеспечить хранение первичной учетной документации. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.

7.2.4. Вести учет передачи персональных данных Клиента, Работника или Контрагента третьим лицам путем ведения соответствующего журнала, отражающего сведения о поступившем запросе (кто является отправителем запроса, дата его поступления Оператору, дату ответа на запрос, какая именно информация была передана либо отметка об отказе в ее предоставлении).

7.2.5. В случае реорганизации или ликвидации Оператора учет и сохранность документов, порядок передачи их на государственное хранение осуществлять в соответствии с правилами, предусмотренными учредительными документами и действующим законодательством Российской Федерации.

7.2.6. Вести журнал учета обращений субъектов персональных данных в части Федерального Закона №152-ФЗ.

7.2.7. Осуществлять передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации.

7.2.8. По требованию субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных.

7.3. Анализ угроз. Обеспечение безопасности персональных данных, а также разработка и внедрение средств защиты персональных данных основывается на анализе угроз безопасности персональных данных. Общество, при возникновении необходимости разрабатывает и поддерживает Частную модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - Частная модель угроз). Частная модель угроз отражает актуальное состояние защищенности информационных систем персональных данных и актуальные угрозы безопасности

персональных данных. Разработка Частной модели угроз осуществляется на основании анализа существующих угроз безопасности и возможности их реализации в обследуемой информационных системах персональных данных.

7.4. Порядок уничтожения персональных данных Ответственным за уничтожение персональных данных является уполномоченное лицо, назначаемое приказом директора. Уполномоченное лицо является председателем комиссии Общества по уничтожению персональных данных. Назначение комиссии по уничтожению персональных данных производится приказом директора. При наступлении любого из событий, повлекших, согласно законодательства РФ, необходимость уничтожения персональных данных, Уполномоченное лицо обязано:

- уведомить членов комиссии о работах по уничтожению персональных данных;
- определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);
- установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные, подлежащие уничтожению (и/или материальные носители персональных данных);
- определить технологию (приём, способ) уничтожения персональных данных (и/или материальных носителей персональных данных);
- определить технические (материальные, программные и иные) средства, посредством которых будет произведено уничтожение персональных данных;
- руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных);
- оформить соответствующий Акт об уничтожении персональных данных (и/или материальных носителей персональных данных) и представить Акт об уничтожении персональных данных (и/или материальных носителей персональных данных) на утверждение директору;
- в случае необходимости уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

8. ПРАВА КЛИЕНТОВ, РАБОТНИКОВ ИЛИ КОНТРАГЕНТОВ В ЦЕЛЯХ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. В целях обеспечения защиты персональных данных, хранящихся у Оператора, Клиенты, Работники или Контрагенты имеют право на:

8.1.1. Полную информацию о составе персональных данных и их обработке, в частности Клиент, Работник или Контрагент имеет право знать, кто и в каких целях использует или использовал информацию о его персональных данных.

8.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Клиента, Работника или Контрагента, за исключением случаев, предусмотренных законодательством РФ.

8.1.3. Определение своих представителей для защиты своих персональных данных.

8.1.4. Требование об исключении или исправлении неверных или неполных устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Оператора персональных данных. При отказе Оператора исключить или исправить персональные данные Клиента, Работника или Контрагента он имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия.

8.1.5. Требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные Клиента, Работника или Контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях.

8.1.6. Обжалование в суд любых неправомерных действий или бездействия Оператора при обработке и защите его персональных данных.

9. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ПОЛУЧЕНИЕ, ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными

законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном законодательством РФ.

10. УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, АКТУАЛЬНЫЕ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1 Угрозами безопасности персональных данных, актуальными при их обработке в информационных системах персональных данных, являются, в том числе: угроза несанкционированного доступа к персональным данным лицами, обладающими полномочиями в информационной системе персональных данных, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных; угроза воздействия вредоносного кода, внешнего по отношению к информационной системе персональных данных; угроза использования методов социального инжиниринга к лицам, обладающим полномочиями в информационной системе персональных данных; угроза несанкционированного доступа к отчуждаемым носителям персональных данных; угроза утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных; угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в организации защиты персональных данных; угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в программном обеспечении информационной системы персональных данных; угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных; угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных; угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации. Определение типа угроз безопасности персональных данных, актуальных для информационной системы персональных данных, производится оператором информационной системы персональных данных в соответствии с пунктом 7 постановления Правительства Российской Федерации от 1 ноября 2012 года N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1 Настоящее Положение вступает в силу с момента его утверждения приказом директора ООО «УК Креатив»

11.2 Настоящее Положение доводится до сведения всех Работников ООО «УК Креатив» персонально под роспись.

11.3 Настоящее Положение размещается в свободном доступе на сайте управляющей организации по адресу: <https://kreativmo.ru/>

Приложения:

1. Список лиц, имеющих доступ к персональным данным работников.

**Список должностей, имеющих доступ
к персональным данным работника**

№	Должность
1	генеральный директор
2.	главный бухгалтер
3.	юрист
4.	Специалист по взысканию дебиторской задолженности
5.	Паспортист