

Приложение № 1 к приказу
от 25.03.2025 № 72

ПОЛИТИКА
обработки персональных данных
в обществе с ограниченной ответственностью
«УГМК-Телеком»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика определяет принципы, цели, задачи, порядок, условия обработки и основные мероприятия по обеспечению безопасности персональных данных общества с ограниченной ответственностью «УГМК-Телеком» (ИНН: 6606022606; КПП: 668601001; ОГРН: 1069606006953; адрес юридического лица: 624090, Свердловская область, город Верхняя Пышма, Успенский проспект, д. 1, ком. 801), далее – Общество, Оператор.

1.2 Политика разработана в соответствии с действующим законодательством Российской Федерации в области защиты персональных данных, в том числе в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3 Политика является основой для разработки локальных нормативных актов Общества по обеспечению безопасности персональных данных.

1.4. Политика действует бессрочно после утверждения и до ее замены новой версией.

1.5. Настоящая Политика размещается на общедоступном ресурсе – на сайте Общества в сети Интернет по адресу: www.ugmk-telecom.ru.

1.6. Общество включено в реестр операторов, осуществляющих обработку персональных данных на основании приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 25.03.2010 № 185 (регистрационный номер 10-0094848).

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В Политике используются следующие термины и определения.

2.1.1. **Субъект персональных данных** – физическое лицо, к которому относятся соответствующие персональные данные;

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

2.1.3. **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;

2.1.4. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

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

средств;

2.1.6. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

2.1.7. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

2.1.8. Конфиденциальность персональных данных – обязанность Общества и его сотрудников не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

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

2.1.10. Оператор – ООО «УГМК-Телеком» (ИНН: 6606022606; КПП: 668601001; ОГРН: 1069606006953), адрес юридического лица: 624090, Свердловская область, город Верхняя Пышма, Успенский проспект, д. 1, ком. 801;

2.1.11. Абонент – физическое лицо, пользователь услугами связи, с которым заключен договор об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации;

2.1.12. Пользователь – любое физическое лицо, которое посещает сайт Общества в сети Интернет, пользуется его услугами и сервисами;

2.1.13. Сайт – совокупность графических и информационных материалов, а также программ для ЭВМ и баз данных, обеспечивающих их доступность в сети Интернет по сетевому адресу www.ugmk-telecom.ru;

2.1.14. Работник – физические лица, состоящие или ранее состоявшие в трудовых отношениях с Обществом;

2.1.15. Практиканты – физические лица (обучающиеся, студенты), проходящие ознакомительную, производственную или преддипломную практическую подготовку в Обществе;

2.1.16. Соискатели – физические лица, претендующие на замещение вакантных должностей в Обществе.

2.2. В Политике используются иные термины и определения в соответствии с их значениями, как они определены в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных».

2.3. Используемые сокращения:

Закон – Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

3. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ОБЯЗАННОСТИ ОБЩЕСТВА

3.1. Основные права субъекта персональных данных:

3.1.1 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных Законом;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- 9.1) информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 Закона;
- 10) иные сведения, предусмотренные законодательством РФ.

3.1.2 Субъект персональных данных имеет право требовать от Общества уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством меры по защите своих прав.

3.1.3 Субъект вправе обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Общества при обработке и защите его персональных данных.

3.1.4. Порядок организации приема и обработки обращений, запросов субъектов персональных данных определен в Приложении № 3 к Политике.

3.2. Обязанности Общества:

3.2.1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Закона.

3.2.2. Если в соответствии с федеральным законом предоставление персональных данных и (или) получение оператором согласия на обработку персональных данных являются обязательными, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

3.2.3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных ч. 4 ст. 18 Закона, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных информацию, предусмотренную ч. 3 ст. 18 Закона.

3.2.4. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Законом и принятыми в соответствии с ним нормативными правовыми актами:

3.2.5. Оператор обязуется принимать следующие меры:

1) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации;

2) предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы, суды и др.);

3) по требованию субъекта персональных данных прекратить обработку его персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;

4) опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике;

5) принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом и иными законодательными актами Российской Федерации;

6) обеспечить защиту персональных данных субъектов от неправомерного их использования или утраты за счет собственных средств в порядке, установленном федеральным законом;

7) давать ответы на запросы и обращения субъектов персональных данных, их представителей и уполномоченного органа по защите прав субъектов персональных данных.

3.2.6 Принимаемые Оператором меры по обеспечению безопасности

персональных данных описаны в Положении о защите персональных данных в ООО «УГМК-Телеком» (Приложение № 3 к Политике).

4. КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ, ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПРИНЦИПЫ И ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Цели обработки персональных данных и соответствующие им категории и перечень обрабатываемых персональных данных, категории субъектов персональных данных приведены в Приложении № 1 к настоящей Политике, являющемся ее неотъемлемой частью.

4.1.1. Особенности обработки персональных данных некоторых категорий субъектов персональных данных из числа вышеперечисленных могут быть установлены иными локальными нормативными актами Общества с учетом положений настоящей Политики.

4.2. Для каждой цели обработки персональных данных в Обществе определены:

- 1) соответствующие категории и перечень обрабатываемых персональных данных;
- 2) категории субъектов персональных данных, персональные данные которых обрабатываются Обществом;

4.3. Общество не осуществляет обработку специальных категорий персональных данных, касающихся расовой и национальной принадлежности, политических взглядов, религиозных и философских убеждений, интимной жизни, судимости физических лиц, если иное не установлено законодательством Российской Федерации.

4.4. Обработка персональных данных в Обществе осуществляется на основании следующих принципов:

- 1) законности и справедливости целей и способов обработки персональных данных;
- 2) соответствия целей обработки персональных данных законным целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Общества;
- 3) соответствия объема и содержания обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- 4) точности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- 5) недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональных данных;
- 6) хранения персональных данных в форме, позволяющей

определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, или устанавливающий срок хранения персональных данных, федеральный закон, договор, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных;

7) уничтожения или обезличивание персональных данных по достижении целей их обработки, в случае утраты необходимости в достижении целей обработки или по окончании срока хранения персональных данных, установленного федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

8) обеспечения конфиденциальности и безопасности обрабатываемых персональных данных.

4.5. Правовыми основаниями обработки персональных данных являются:

Конституция Российской Федерации;

Гражданский кодекс Российской Федерации;

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

Федеральный закон от 10.12.1995 № 196-ФЗ «О безопасности дорожного движения»;

Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 08.02.1998 № 14-ФЗ «Об обществах с ограниченной ответственностью»;

Федеральный закон от 06.12.2011 г. № 402-ФЗ «О бухгалтерском учете»;

Федеральный закон от 29.12.2009 г. № 273-ФЗ «Об образовании в Российской Федерации»;

Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»;

Постановление Правительства РФ от 27.11.2006 г. № 719 «Об утверждении Положения о воинском учете»;

Приказ Минобрнауки России от 18.04.2013 № 291 «Об утверждении Положения о практике обучающихся, осваивающих основные профессиональные образовательные программы среднего профессионального образования»;

Приказ Минобрнауки России от 27.11.2015 № 1383 «Об утверждении Положения о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования»;

иные нормативные правовые акты, регулирующие отношения, связанные с деятельностью Общества;

устав Общества;

локальные акты Общества в области защиты и обработки персональных

данных;

гражданско-правовые договоры, заключаемые Обществом;

согласие субъектов персональных данных на обработку их персональных данных.

5. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Общество осуществляет обработку персональных данных, перечень которых применительно к конкретным целям и категориям субъектов персональных данных, приведен в таблице, являющейся Приложением № 1 к настоящей Политике.

5.2. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку персональных данных, а также без такового в случаях, предусмотренных законодательством о персональных данных, в том числе если обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных.

5.3. Общество осуществляет обработку персональных данных путем сбора, записи, систематизации, накопления, хранения, уточнения (обновление, изменение) после внесения изменений субъектом персональных данных, извлечения, использования, передачи (распространение, предоставление, доступ), блокирования, удаления, уничтожения персональных данных.

5.4. Способы обработки персональных данных:

5.4.1. при помощи средств вычислительной техники (автоматизированная обработка);

Автоматизированная обработка персональных данных производится с помощью средств вычислительной техники, как установленных локально, так и объединенных в сеть, а также с помощью информационных систем. Доступ к такой сети предоставляется уполномоченным работникам только для исполнения ими своих функций и должностных обязанностей.

При обработке персональных данных с использованием информационных систем Общество обеспечивает их защиту в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными действующим законодательством РФ.

5.4.2. без использования средств вычислительной техники (неавтоматизированная обработка).

Неавтоматизированная обработка персональных данных осуществляется таким образом, чтобы персональные данные обособлялись от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм

(бланков) и иным способом.

5.4.3. обработка как с использованием средств вычислительной техники, так и без них (смешанная обработка).

5.5. К обработке персональных данных допускаются работники Общества, в должностные обязанности которых входит обработка соответствующих категорий персональных данных. Перечень указанных работников утверждается приказом Общества, при этом указанные в приказе лица должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения непосредственных должностных обязанностей.

5.6. Лица, осуществляющие обработку персональных данных со стороны Общества, ознакомлены с положениями законодательства Российской Федерации о персональных данных, локальными актами Общества по вопросам обработки персональных данных.

5.7. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Общество обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в действующем законодательстве.

5.8. Обществом не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, за исключением случаев, когда такое раскрытие и распространение без согласия субъекта персональных данных требуется/допускается действующим законодательством.

5.9. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования, Единый государственный внебюджетный Социальный фонд России (СФР) и другие уполномоченные органы исполнительной власти и организации осуществляется Обществом в соответствии с требованиями законодательства.

5.10. В случае подтверждения факта неточности персональных данных или неправомерности их обработки, персональные данные подлежат актуализации, а обработка должна быть прекращена.

5.11. Трансграничная передача данных Обществом не осуществляется.

5.12. Обработка специальных категорий персональных данных осуществляется Обществом в случаях, предусмотренных законодательством Российской Федерации, с согласия субъекта персональных данных на обработку своих персональных данных в письменной форме.

5.13. Согласие субъекта персональных данных на обработку

персональных данных может быть выражено в форме совершения действий по принятию условий договора-оферты, проставления соответствующих отметок, заполнения полей в анкетах, формах, бланках.

Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью.

5.14. Общество вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ. Такая обработка персональных данных осуществляется на основании договора, заключенного между Обществом и третьим лицом, в котором должны быть определены:

1. перечень персональных данных и действий (операций) с персональными данными, которые будут совершаться третьим лицом, осуществляющим обработку персональных данных;
2. цели обработки персональных данных;
3. обязанности третьего лица соблюдать конфиденциальность персональных данных и обеспечивать их безопасность при обработке, а также требования к защите обрабатываемых персональных данных и иные сведения, предусмотренные ч. 3 ст. 6 Закона.

5.15. Оператор обрабатывает персональные данные Абонента (Пользователя) только в случае их заполнения и/или отправки Пользователем самостоятельно через специальные формы, расположенные на сайте www.ugmk-telecom.ru или направленные Оператору посредством электронной почты или иным способом. Заполняя соответствующие формы на сайте, Пользователь выражает свое согласие с данной Политикой.

5.16. Оператор обрабатывает обезличенные данные о Пользователе в случае, если это разрешено в настройках браузера Пользователя (включено сохранение файлов cookie).

5.17. На Сайте Оператора происходит сбор и обработка обезличенных данных об Абонентах и Пользователях (в том числе файлов cookie) с помощью сервиса интернет статистики «Яндекс Метрика».

5.18. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта персональных данных.

6. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Сроки обработки персональных данных определяются в соответствии со сроком действия заключенного с субъектом персональных

данных (работодателем субъекта персональных данных) договора, сроком исковой давности.

6.2. Обработка персональных данных начинается с момента их поступления в Общество и прекращается:

6.2.1. Достижение целей обработки персональных данных или максимальных сроков хранения – в течение 30 дней.

6.2.2. Утрата необходимости в достижении целей обработки персональных данных – в течение 30 дней.

6.2.3. Предоставление субъектом персональных данных или его законным представителем подтверждения того, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки – в течение 3 рабочих дней.

6.2.4. Невозможность обеспечения правомерности обработки персональных данных – в течение 10 рабочих дней.

6.2.5. Отзыв субъектом персональных данных согласия на обработку персональных данных, если сохранение персональных данных более не требуется для целей обработки персональных данных – в течение 30 дней.

6.2.6. Требование субъекта персональных данных о прекращении обработки персональных данных – в течение 10 рабочих дней.

6.2.7. Истечение сроков исковой давности для правоотношений, в рамках которых осуществляется либо осуществлялась обработка персональных данных – в течение 30 дней.

6.3. Уничтожение персональных данных производится в случаях и в сроки, указанные выше, если иное не установлено действующим законодательством.

7. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1 Лица, виновные в нарушении положений законодательства РФ в области персональных данных при обработке персональных данных несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами Российской Федерации.

7.2 Моральный вред, причиненный субъекту вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, установленных Законом, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом убытков.

**Цели, категории и субъекты обработки персональных данных в
ООО «УГМК-Телеком»**

<i>Цель обработки персональных данных</i>	<i>Категория субъектов персональных данных</i>	<i>Перечень персональных данных</i>
Ведение кадрового и бухгалтерского учета	Работники; Родственники работников; Уволенные работники	фамилия, имя, отчество (при наличии); год рождения; месяц рождения; дата рождения, паспортные данные (в т.ч. данные документа, удостоверяющего личность за пределами Российской Федерации) или данные иного документа, удостоверяющего личность; гражданство; ИНН; страховой номер индивидуального лицевого счета; семейное положение; сведения о наличии детей, социальное положение; пол; адрес места жительства; адрес регистрации; номер телефона; данные документа, содержащиеся в свидетельстве о рождении; данные документа, содержащиеся в свидетельстве о заключении/расторжении брака; реквизиты банковской карты; номер расчетного счета; номер лицевого счета; профессия; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); отношение к воинской обязанности, сведения о воинском учете; сведения об образовании; сведения об изменении фамилии, имени, отчества (причина изменения, дата); сведения о владении иностранными языками (наименование, степень владения) и уровень владения компьютером; социальный статус (сведения об инвалидности, сведения о социальных льготах, сведения об удержании алиментов и т.д.); сведения об ученой степени, квалификации, профессиональной переподготовке и повышении квалификации, сведения о предыдущем месте работы (должность, обязанности, причина увольнения с предыдущего места работы, дисциплинарные взыскания); данные о государственной (муниципальной) службе за последние два года; основания прекращения трудовых отношений с бывшим работником, дата увольнения; финансовая информация о субъекте персональных данных: сведения о доходах, имуществе и финансовых обязательствах, сведения о размере вычетов, суммах удержаний из заработной платы; сведения об исполнительных производствах; сведения об участии лица в гражданском, административном, уголовном судопроизводстве; сведения о поощрениях и наградах, почетных званиях; табельный номер; адрес электронной почты; сведения о составе семьи (ФИО близких родственников, степень родства, год, месяц,

		дата рождения); реквизиты разрешения на работу, патента, вида на жительство, разрешения на временное проживание (включая копии разрешения на работу, патента, вида на жительство, разрешения на временное проживание); сведения об аттестации; сведения о трудовом договоре; сведения, содержащиеся в трудовой книжке и иных кадровых документах. Специальные категории персональных данных: сведения о состоянии здоровья; данные изображения лица, полученные с помощью фото-видео устройств, позволяющие установить личность субъекта персональных данных.
Обеспечение соблюдения трудового законодательства РФ	Работники; Родственники работников; Учащиеся; Студенты; Уволенные работники	фамилия, имя, отчество; паспортные (в т.ч. данные документа, удостоверяющего личность за пределами Российской Федерации) или данные иного документа, удостоверяющего личность год рождения; месяц рождения; дата рождения; место рождения; семейное положение; сведения о наличии детей; социальное положение; доходы; пол; адрес места жительства; адрес регистрации; номер телефона; СНИЛС; ИНН; гражданство; данные документа, содержащиеся в свидетельстве о рождении; данные, содержащиеся в свидетельстве заключении/расторжении брака; реквизиты банковской карты; номер расчетного счета; номер лицевого счета; профессия; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); отношение к воинской обязанности, сведения о воинском учете; сведения об образовании; сведения об изменении фамилии, имени, отчества (причина изменения, дата); сведения о владении иностранными языками (наименование, степень владения) и уровень владения компьютером; социальный статус (сведения об инвалидности, сведения о социальных льготах, сведения об удержании алиментов и т.д.); сведения об ученой степени, квалификации, профессиональной переподготовке и повышении квалификации, сведения о предыдущем месте работы (должность, обязанности, причина увольнения с предыдущего места работы, дисциплинарные взыскания); данные о государственной (муниципальной) службе за последние два года; основания прекращения трудовых отношений с бывшим работником, дата увольнения; финансовая информация о субъекте персональных данных: сведения о доходах, имуществе и финансовых обязательствах, сведения о размере вычетов, суммах удержаний из заработной платы; сведения о поощрениях, наградах, почетных званиях; сведения об аттестации; сведения о командировках, отпусках; сведения о членстве в профсоюзной организации; сведения о владении автомобилем; данные водительского удостоверения; сведения о деловых и личных качествах, носящих оценочный характер.

		Специальные категории ПД: сведения о состоянии здоровья.
Обеспечение соблюдения налогового законодательства РФ	Работники; Уволенные работники; Контрагенты; Выгодоприобретатели по договорам; Законные представители	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; доходы; пол; адрес регистрации; СНИЛС; ИНН; гражданство; номер расчетного счета; номер лицевого счета; профессия; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); отношение к воинской обязанности, сведения о воинском учете; финансовая информация о субъекте персональных данных: сведения о доходах, имуществе и финансовых обязательствах; сведения о размере вычетов, суммах удержаний из заработной платы; сведения о поощрениях, наградах.
Обеспечение соблюдения пенсионного законодательства РФ	Работники; Контрагенты; Выгодоприобретатели по договорам, уволенные работники	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; семейное положение; пол; адрес места жительства; адрес регистрации; номер телефона; СНИЛС; ИНН; гражданство; данные документа, удостоверяющего личность; реквизиты банковской карты; номер расчетного счета; номер лицевого счета; доходы, сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации).
Добровольное медицинское страхование	Работники	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; пол; адрес регистрации; СНИЛС; ИНН; гражданство; данные документа, удостоверяющего личность; должность; место работы; телефон; адрес электронной почты.
Подготовка, заключение и исполнение гражданско-правового договора	Контрагенты; Представители контрагентов; Выгодоприобретатели по договорам	фамилия, имя, отчество (при наличии); год рождения; месяц рождения; дата рождения, паспортные данные (в т.ч. данные документа, удостоверяющего личность за пределами Российской Федерации) или данные иного документа, удостоверяющего личность; пол; гражданство; адрес регистрации; СНИЛС; ИНН; адрес фактического места жительства; семейное положение, сведения о членах семьи; адрес электронной почты; номер телефона; реквизиты банковской карты; номер расчетного счета; номер лицевого счета; профессия; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); сведения об образовании; сведения об изменении фамилии, имени, отчества (причина изменения, дата); сведения о владении иностранными языками (наименование, степень владения) и уровень владения компьютером; социальный статус (сведения об инвалидности, сведения о социальных льготах, сведения об удержании алиментов и т.д.); сведения об ученой степени, квалификации, профессиональной переподготовке и повышении квалификации, сведения о предыдущем месте работы (должность, обязанности, причина увольнения с предыдущего места работы, дисциплинарные взыскания); данные о государственной (муниципальной)

		службе за последние два года; основания прекращения трудовых отношений с бывшим работником, дата увольнения; финансовая информация о субъекте персональных данных: сведения о доходах, имуществе и финансовых обязательствах; сведения об участии в уголовных и административных судопроизводствах; реквизиты разрешения на работу, патента, вида на жительство, разрешения на временное проживание (включая копии разрешения на работу, патента, вида на жительство, разрешения на временное проживание). Специальные категории ПД: сведения о состоянии здоровья; данные изображения лица, полученные с помощью фото-видео устройств, позволяющие установить личность субъекта персональных данных.
Обеспечение соблюдения законодательства РФ об исполнительном производстве	Работники; Контрагенты; Представители контрагентов	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; доходы; адрес регистрации; СНИЛС; ИНН; номер расчетного счета; профессия; должность.
Исполнение судебного акта	Работники; Контрагенты; Представители контрагентов; Клиенты	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; доходы; пол; адрес регистрации; СНИЛС; ИНН; данные документа, удостоверяющего личность; номер расчетного счета; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); имущество/имущественное положение, социальный статус .
Продвижение товаров, работ, услуг на рынке	Контрагенты; Представители контрагентов; Клиенты; Посетители сайта	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; пол; адрес электронной почты; адрес места жительства; адрес регистрации; данные документа, удостоверяющего личность; реквизиты банковской карты; номер расчетного счета; сведения о участии в партнерских и бонусных программах; сведения об используемых продуктах и услугах ООО "УГМК-Телеком"
Обеспечение пропускного режима на территорию оператора	Работники; Соискатели; Контрагенты; Представители контрагентов; Клиенты; Учащиеся; Студенты; Иные категории субъектов персональных данных, персональные данные	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; пол; номер телефона; данные документа, удостоверяющего личность; табельный номер сотрудника, государственный регистрационный номер транспортного средства.

	которых обрабатываются; посетители	
Подбор персонала (соискателей) на вакантные должности оператора	Соискатели	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; паспортные данные (в т.ч. данные документа, удостоверяющего личность за пределами Российской Федерации) или данные иного документа, удостоверяющего личность; семейное положение; пол; адрес электронной почты; адрес места жительства; адрес регистрации; номер телефона; СНИЛС; ИНН; гражданство; профессия; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); отношение к воинской обязанности, сведения о воинском учете; сведения об образовании; сведения об изменении фамилии, имени, отчества (причина изменения, дата); сведения о владении иностранными языками (наименование, степень владения) и уровень владения компьютером; сведения об ученой степени, квалификации, профессиональной переподготовке и повышении квалификации, сведения о предыдущем месте работы (должность, обязанности, причина увольнения с предыдущего места работы, дисциплинарные взыскания); основания прекращения трудовых отношений с бывшим работником, дата увольнения; сведения о наличии кредитных обязательств, о наличии текущей непогашенной задолженности, о наличии собственного бизнеса, о наличии статуса государственного или муниципального служащего; сведения о составе семьи (ФИО близких родственников, степень родства, год, месяц, дата рождения); сведения о доходах, имуществе; реквизиты разрешения на работу, патента, вида на жительство, разрешения на временное проживание (включая копии разрешения на работу, патента, вида на жительство, разрешения на временное проживание; сведения о владении автомобилем; сведения о поощрениях (наградах, почетных званиях); об участии лица в гражданском, административном, уголовном судопроизводстве; сведения о деловых и личных качествах, носящие оценочный характер; профили в социальных сетях Специальные категории персональных данных сведения о состоянии здоровья; данные изображения лица, полученные с помощью фото-видео устройств, позволяющие установить личность субъекта.
Обеспечение прохождения ознакомительной,	Учащиеся; Студенты	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; пол; адрес электронной почты; адрес места жительства; адрес регистрации; номер телефона; СНИЛС; адрес электронной почты гражданство; данные документа, удостоверяющего

производственной или преддипломной практики на основании договора с учебным заведением		личность; а также: сведения об учебном заведении и программе обучения (наименование учебного заведения, в котором студент проходит обучение, наименование образовательной программы, форма обучения, номер курса и т.д.). Специальные категории персональных данных: сведения о состоянии здоровья
Оказание услуг по организации выдачи карт тахографа	Контрагенты; Представители контрагентов; Клиенты	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; пол; адрес электронной почты; адрес регистрации; номер телефона; СНИЛС; ИНН; гражданство; данные документа, удостоверяющего личность; данные водительского удостоверения; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); а также: Данные о ранее выданной карты тахографа
Функционирование сайта ООО «УГМК-Телеком», анализ пользовательской активности и сбора статистики посещения сайта ООО «УГМК-Телеком», включая cookies	Клиенты; Посетители сайта	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; адрес электронной почты; адрес регистрации; номер телефона; данные документа, удостоверяющего личность; сведения, собираемые посредством метрических программ;
Обеспечение соблюдения законодательства РФ об обороне	Работники	фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; семейное положение; пол; адрес места жительства; адрес регистрации; номер телефона; СНИЛС; ИНН; гражданство; данные документа, удостоверяющего личность; данные водительского удостоверения; данные документа, удостоверяющего личность за пределами Российской Федерации; профессия; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); отношение к воинской обязанности, сведения о воинском учете; сведения об образовании; Специальные категории персональных данных: сведения о состоянии здоровья;

ПОРЯДОК ОРГАНИЗАЦИИ ПРИЕМА И ОБРАБОТКИ ОБРАЩЕНИЙ, ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО «УГМК-ТЕЛЕКОМ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет порядок организации приема и обработки обращений, запросов субъектов персональных данных в ООО «УГМК-Телеком» (далее – Общество, Оператор).

1.2. Субъект персональных данных – это физическое лицо, прямо или косвенно определяемое с помощью информации, относящейся к этому лицу.

1.3. Под субъектами персональных данных для целей настоящего порядка понимаются:

- 1) Работники Общества;
- 2) Учащиеся и студенты, находящиеся на ознакомительной, производственной и преддипломной практиках;
- 3) Контрагенты, представители контрагентов;
- 4) Клиенты (лица, заключившие с Обществом договоры оказания услуг связи; договор организации выдачи карт тахографа) Общества;
- 5) Посетители помещений, принадлежащих Обществу (в случае установления пропускного режима);
- 6) Посетители сайтов Общества;
- 7) Выгодоприобретатели по договорам Общества;
- 8) Родственники работников;
- 9) Уволенные работники.

1.4. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения,

если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

9.1) информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

10) иные сведения, предусмотренные законодательством РФ.

1.5. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с законодательством РФ.

1.6. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. НАПРАВЛЕНИЕ ОБРАЩЕНИЙ, ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВО.

2.1. Обращение, запрос субъекта персональных данных к Оператору в целях реализации его прав, установленных Законом о персональных данных, осуществляется путем направления обращения в письменном виде следующими способами:

– в виде сканированного документа на адрес электронной почты info@ugmk-telecom.ru;

– путем направления электронного документа, подписанного электронной подписью субъекта персональных данных, на адрес электронной почты info@ugmk-telecom.ru;

– путем направления документа на бумажном носителе почтовым отправлением по адресу: 624090, Россия, Свердловская область, г. Верхняя Пышма, пр-т Успенский, 1, к. 801.

2.2. Обращение, запрос должны содержать следующие данные:

- 1) номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
- 2) сведения, подтверждающие факт обработки Оператором персональных данных субъекта персональных данных;
- 3) подпись субъекта персональных данных.

2.2.1. В обращении, запросе рекомендуется также указывать способ получения ответа от Оператора. В случае если способ получения ответа не указан, то ответ на обращение субъекта персональных данных направляется аналогичным способом тому, как были направлены обращение, запрос субъекта персональных данных.

2.2.2. В случае если обращение, запрос не содержат сведений, указанных в п. 2.2, в связи с чем Оператор не имеет возможности предоставить субъекту персональных данных информацию в установленный Законом срок, то Оператор направляет субъекту персональных данных уведомление о необходимости уточнения требований запроса субъекта персональных данных и о продлении срока ответа на обращение, запрос субъекта персональных данных в пределах сроков, установленных п. 3.3 Порядка.

2.3. Субъект персональных данных вправе обратиться к Оператору повторно не ранее чем через 30 (Тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен законодательством.

2.4. Субъект персональных данных вправе обратиться повторно к Оператору до истечения срока, указанного в п. 2.3 Порядка, в случае если сведения, предусмотренные п. 1.4 Порядка, не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п.2.2 Порядка, должен содержать обоснование направления повторного запроса.

2.4.1. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным п. 2.4 Порядка.

3. РАССМОТРЕНИЕ ОБРАЩЕНИЙ, ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЩЕСТВОМ.

3.1. В случае получения запроса от субъекта персональных данных или его представителя о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, Оператор в срок, не превышающий 10 (Десять) рабочих дней с даты такого обращения или получения заявления предоставляет субъекту персональных данных информацию и возможность ознакомления с этими персональными данными.

3.2. В случае обращения субъекта персональных данных или его представителя Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных.

3.3. Указанные в п. 3.1, 3.2 Порядка сроки могут быть продлены Оператором. В случае невозможности предоставления информации в установленный срок Оператор направляет в адрес субъекта персональных данных мотивированное уведомление с указанием причин и срока продления. Срок может быть продлен не более чем на 5 (Пять) рабочих дней.

3.4. В случаях, предусмотренных законодательством РФ, Оператор вправе отказать в предоставлении запрашиваемой субъектом персональных данных информации, о чем уведомляет субъекта персональных данных или его представителя, с указанием обоснования такого отказа, в срок, не превышающий десяти рабочих дней с даты обращения или получения заявления.

3.5. Оператор обязан предоставить субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

3.6. В случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Оператор обязан внести в них необходимые изменения в срок, не превышающий 7 (Семь) рабочих дней со дня предоставления сведений.

3.7. В случае представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки Оператор в срок, не превышающий семи рабочих дней со дня представления таких сведений обязан уничтожить персональные данные и уведомить субъекта персональных данных об уничтожении его персональных данных.

3.8. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом,

действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки.

3.9. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.10. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.11. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора.

3.12. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4. ОТЗЫВ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ СОГЛАСИЯ НА ОБРАБОТКУ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

4.2. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, предусмотренных ч. 2 ст. 9 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных».

4.3. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО «УГМК-ТЕЛЕКОМ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящее положение о защите персональных данных в ООО «УГМК-Телеком» (далее по тексту – Положение) является неотъемлемой частью Политики обработки персональных в ООО «УГМК-Телеком».

1.2. Цель Положения – защита персональных данных, обрабатываемых Обществом, от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

2. СВЕДЕНИЯ О РЕАЛИЗУЕМЫХ ТРЕБОВАНИЯХ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Общество при обработке персональных данных принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2.2 Реализация требований к защите персональных данных в Обществе осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлениями Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2.3 Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

2.4 Выбор средств защиты информации для системы защиты персональных данных осуществляется Обществом в соответствии с законодательством Российской Федерации.

2.5 Основными мерами защиты персональных данных, используемыми

Обществом, являются:

- назначение лица, ответственного за обработку персональных данных, обучение и инструктаж, внутренний контроль, за соблюдением Обществом и его работниками требований к защите персональных данных;
- определение актуальных угроз безопасности персональных данных при их обработке в информационной системе персональных данных, и разработка мер и мероприятий по защите персональных данных;
- разработка локальных нормативных актов в отношении обработки персональных данных;
- установление индивидуальных паролей доступа работников в информационные системы в соответствии с их трудовыми обязанностями;
- использование сертифицированного антивирусного программного обеспечения с регулярно обновляемыми базами;
- использование сертифицированных программных средств защиты информации от несанкционированного доступа;
- соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ.

2.6. Обеспечение безопасности персональных данных достигается, в частности:

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

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

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

3.1) применением для уничтожения персональных данных, прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, в составе которых реализована функция уничтожения информации;

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

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

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

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

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

3. ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Персональные данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде. Хранение материальных носителей персональных данных осуществляется с соблюдением условий, обеспечивающих их сохранность и исключающих несанкционированный доступ к ним.

3.2 Персональные данные, зафиксированные на бумажных носителях, хранятся в запираемых шкафах и помещениях.

3.3. Персональные данные субъектов, обрабатываемые в информационных системах в разных целях, хранятся в обособленно (в разных папках, вкладках).

3.4 Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен 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 законом.

3.5 При осуществлении хранения персональных данных Общество обязано использовать базы данных, находящиеся на территории Российской Федерации.

4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ И ИХ ПЕРЕДАЧА

4.1. Внутренний доступ.

Право доступа к персональным данным в Обществе имеют:

- генеральный директор Компании;
- работники Управления по работе с персоналом;
- работники Блока экономики и финансов;
- работники Блока по безопасности;

- работники Юридического управления
- работники Отдела управления делами;
- работники Блока телекоммуникаций;
- работники Блока безопасности дорожного движения;
- заместители генерального директора и руководители структурных подразделений по направлению деятельности;
- иные уполномоченные сотрудники структурных подразделений, расположенных вне местонахождения (юридического и/или фактического адреса) Компании, перечень которых определен отдельным локально-нормативным актом;
- сам работник, соискатель, практикант в отношении своих персональных данных.

При этом лица, перечисленные в данном пункте, должны имеют право доступа только к тем персональным данным, которые необходимы для выполнения конкретной функции.

4.2. Внешний доступ.

Общество вправе осуществлять передачу персональных данных субъектов третьим лицам только с их предварительного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника (соискателя, практиканта), а также в других случаях, предусмотренных действующим законодательством Российской Федерации.

Передача персональных данных третьим лицам в коммерческих целях требует предварительного письменного согласия субъекта персональных данных.

Перед передачей персональных данных Общество предупреждает лиц, получающих персональные данные о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные обязаны соблюдать режим секретности (конфиденциальности).

Не требуется согласие субъекта персональных данных на передачу его персональных данных:

- третьим лицам в целях предупреждения угрозы жизни и здоровью субъекта персональных данных;
- в Социальный фонд Российской Федерации в объеме, предусмотренном действующим законодательством Российской Федерации;
- в налоговые органы;
- в военные комиссариаты;
- по мотивированному запросу органов прокуратуры;
- по мотивированному запросу (требованию) правоохранительных органов и органов безопасности;

- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;
- по запросу суда;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом;
- в случаях, связанных с исполнением работником должностных обязанностей, выполнением практикантом программы практической подготовки;
- в кредитную организацию, обслуживающую платежные (зарплатные) карты работников;
- в иные государственные (муниципальные) органы, организации и учреждения в случаях и в порядке, определённом законодательством РФ.

5. ГАРАНТИИ КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Все работники организации, осуществляющие обработку ПД, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Положением, требованиями законодательства РФ.

5.2. Работник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

5.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.

6. УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

6.2. Существует 3 типа угроз безопасности персональных данных:

- Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

- Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

-Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

6.3. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится Оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

6.4. По результатам оценки возможного вреда Оператор издает приказ об определении уровня защищенности персональных данных.

6.4.1. Первый уровень защищенности персональных данных присваивается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

6.4.2. Второй уровень защищенности персональных данных присваивается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

6.4.3. Третий уровень защищенности персональных данных присваивается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

6.4.4. Четвертый уровень защищенности персональных данных присваивается при наличии хотя бы одного из следующих условий:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

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

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в

области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

6.5. Исходя из уровня защищенности персональных данных Оператор определяет необходимые меры защиты персональных данных.

Уровень защищенности	Меры
Первый	а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения; б) обеспечение сохранности носителей персональных данных; в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей; г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз; д) назначение должностного лица, ответственного за обеспечение безопасности персональных данных в информационных системах; е) обеспечение доступа к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей; ж) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе; з) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Второй	а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения; б) обеспечение сохранности носителей персональных данных; в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей; г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз; д) назначение должностного лица, ответственного за обеспечение безопасности персональных данных в информационных системах; е) обеспечение доступа к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.
Третий	а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения; б) обеспечение сохранности носителей персональных данных; в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей; г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области

	обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз; д) назначение должностного лица, ответственного за обеспечение безопасности персональных данных в информационных системах.
Четвертый	а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения; б) обеспечение сохранности носителей персональных данных; в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей; г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

7. УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В случае если обработка персональных данных осуществляется оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

7.2. В случае если обработка персональных данных осуществляется оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее - выгрузка из журнала).

7.3. Акт об уничтожении персональных данных должен содержать:

- а) наименование и адрес Оператора;
- б) наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица), адрес лица (лиц), осуществляющего (осуществляющих) обработку персональных данных субъекта (субъектов)

персональных данных по поручению оператора (если обработка была поручена такому (таким) лицу (лицам);

в) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

г) фамилию, имя, отчество (при наличии), должность лиц (лица), уничтоживших персональные данные субъекта персональных данных, а также их (его) подпись;

д) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

е) наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

ж) наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

з) способ уничтожения персональных данных;

и) причину уничтожения персональных данных;

к) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

7.4. Акт об уничтожении персональных данных в электронной форме, подписанный электронной подписью, признается электронным документом, равнозначным акту об уничтожении персональных данных на бумажном носителе, подписанному собственноручной подписью лиц, указанных в подпункте "г" пункта 7.3 Положения.

7.5. Выгрузка из журнала должна содержать:

а) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

б) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

в) наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;

г) причину уничтожения персональных данных;

д) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

7.6. В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные пунктом 7.5 Положения, недостающие сведения вносятся в акт об уничтожении персональных данных.

7.7. В случае если обработка персональных данных осуществляется оператором одновременно с использованием средств автоматизации и без использования средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных, соответствующий требованиям, установленным пунктами 7.3 и 7.4 Положения, и выгрузка из журнала, соответствующая требованиям, установленным пунктом 7.5 Положения.

7.8. Акт об уничтожении персональных данных и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

7.9. Уничтожение персональных данных осуществляется комиссией, созданной на основании приказа Оператора.

7.10. Уничтожение ПДн, зафиксированных на материальных носителях, производится следующими способами:

- уничтожение материальных носителей путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления;
- уничтожение части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку таких персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание);
- стирание ПДн с материального носителя производится по технологии, предусмотренной для данного типа носителя, с применением средств гарантированного уничтожения информации.

Бумажные и прочие сгораемые материальные носители уничтожаются путем измельчения на мелкие части, исключающего возможность последующего восстановления информации (шредирование), или термической обработки (сжигание).

7.11 Уничтожение персональных данных из информационных систем ПДн производится встроенными средствами информационной системы администраторами таких систем.

7.12. Форма акта об уничтожении персональных данных является Приложением № 1 к Положению.

ФОРМА

АКТ
ОБ УНИЧТОЖЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Место составления акта: _____

Дата составления акта: _____

Комиссия в составе:

- председатель комиссии:

_____ (ФИО, должность);

- члены комиссии:

_____ (ФИО, должность);

_____ (ФИО, должность);

в соответствии со ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» составила **акт об уничтожении персональных данных**, обрабатываемых **ООО «УГМК-Телеком»**, ИНН: 6606022606; КПП: 668601001; ОГРН: 1069606006953; адрес юридического лица: 624090, Свердловская область, город Верхняя Пышма, Успенский проспект, д. 1, ком. 801

Ф.И.О. субъектов, чьи ПДн были уничтожены	Перечень категорий уничтоженных ПДн	Наименование ИСПДн, из которой были уничтожены ПДн	Способ уничтожения ПДн	Причина уничтожения ПДн	Дата уничтожения ПДн

ИСПДн – информационная система персональных данных

ПДн – персональные данные

Акт подлежит хранению в течение 3 лет: до _____.

Председатель комиссии:

_____ (ФИО, должность);

Члены комиссии:

_____ (ФИО, должность);

_____ (ФИО, должность);