# Положение
# «Обработка и защита персональных данных»

**Москва**
**2023**

**Оглавление**

## 1. Общие положения

Положение «Обработка и защита персональных данных» (далее – Положение) является внутренним нормативным документом Общества с ограниченной ответственностью «Форк ИТ» (сокращенное наименование ООО «Форк ИТ» далее – Компания), регламентирующим процесс режима защиты и обработки персональных данных по отношению к субъектам персональных данных, обрабатываемых в Компании.

Настоящее Положение разработано в соответствии с Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», иных федеральных законов и подзаконных нормативных актов.

Настоящее Положение является обязательным для исполнения всеми работниками Компании.

## 2. Термины, определения и принятые сокращения

В настоящем документе используются следующие термины и определения:

**Информация ограниченного доступа (ИОД)** — это информация, доступ к которой ограничен в соответствии с международными правовыми нормами (применимыми для РФ), законодательством РФ и внутренними нормативными документами Компании;

**Информационная система персональных данных (ИСПДн)** – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

**Конфиденциальность персональных данных** – обязательное для выполнения Компанией или иным лицом, получившим доступ к персональным данным, требование не допускать раскрытия ПДн третьим лицам, и их распространение без согласия Субъекта ПДн или наличия иного законного основания;

**Компания** – Общество с ограниченной ответственностью «Форк ИТ»;

**Неавтоматизированная обработка персональных данных** - обработка персональных данных, содержащихся в ИСПДн либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека;

**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, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

**Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

**Оператор** – Компания ООО «Форк ИТ», самостоятельно или совместно с другими лицами организующая и (или) осуществляющая обработку персональных данных, а также определяющая цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

**Ответственный за обработку персональных данных** – работник Компании, назначаемый приказом Генерального директора, осуществляющий обеспечение безопасности, защиты и соблюдения требований действующего законодательства при обработке персональных данных;

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

**Работники Компании -** штатные работники Компании с полной или частичной занятостью, независимо от их должности в Компании;

**Режим защиты и обработки персональных данных** – установленный порядок действий (правил) по защите и обработке персональных данных субъектов, обеспечивающий выполнение требований законодательства РФ, нормативных документов Компании;

**Система защиты персональных данных –** комплекс правовых, организационных, организационно-технических мероприятий, направленный на обеспечение защиты обрабатываемых персональных данных от несанкционированного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных несанкционированных действий;

**Система внутреннего контроля** – это совокупность сил, средств и мероприятий (процедур), принятых руководством Компании для обеспечения соблюдения режимов защиты и обработки персональных данных в Компании;

**Субъект персональных данных** (далее Субъект) – физическое лицо, определяемое или определенное персональными данными. Субъектами персональных данных могут являться граждане Российской Федерации, иностранные граждане и лица без гражданства;

**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.

## 3. Основные положения

3.1. Настоящее Положение разработано в соответствии с Федеральным законом РФ № 152-ФЗ от 27.07.2006 «О персональных данных», № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и защите информации», иных федеральных законов и подзаконных нормативных актов.

3.2. Главный специалист по безопасности является ответственным за обработку персональных данных в Компании.

3.2.1. Руководители структурных подразделений отвечают за реализацию и выполнение требований режима защиты и обработки персональных данных в своем структурном подразделении, а работники Компании за соблюдение данного режима.

3.3. Основными принципами обработки персональных данных в Компании являются:

- **законность и справедливость** (обработка персональных данных должна осуществляться на законной и справедливой основе);
- **разграничение по базам данных** (не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой);
- **соответствие заявленным целям** (обработке подлежат только персональные данные, которые отвечают целям их обработки; содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки; не допускается обработка персональных данных, излишних по отношению к заявленным целям обработки);
- **точность, достаточность и актуальность** (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. Неполные или неточные данные должны быть удалены или уточнены);
- **сохранность** (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);
- **своевременность уничтожения, обезличивания** (по достижении целей обработки или в случае утраты необходимости в достижении этих целей, персональные данные должны быть уничтожены или обезличены, если иное не предусмотрено федеральным законом);
- **конфиденциальность** (информация, относящаяся к персональным данным, ставшая известной Компании, является информацией ограниченного доступа и охраняется законом).

3.4. В Компании создана Система защиты персональных данных, основными принципами которой являются:

– **комплексность** (предполагает принятие в Компании комплекса мер, правового, организационного и технического характера направленных на обеспечение безопасности персональных данных, дополняющих и поддерживающих друг друга);

– **своевременность и превентивность** (меры обеспечения безопасности персональных данных, применяемые в рамках системы защиты, должны быть своевременными, а также носить предупреждающий характер);

– **надежность** (система защиты персональных данных должна обеспечивать достаточные гарантии Компании в том, что обрабатываемые персональных данных защищены в соответствии с требованиями законодательства).

## 4. Режим защиты и обработки персональных данных

4.1. Режим защиты и обработки персональных данных включает в себя:

– порядок (правила) обработки персональных данных субъектов;

– порядок передачи информации, содержащей персональные данные;

– порядок выполнения правовых, организационных и технических (организационно-технических) мероприятий по защите персональных данных;

– порядок проведения мероприятий внутреннего контроля по соблюдению требований законодательства и внутренних нормативных документов Компании;

За реализацию режима защиты и обработки персональных данных в структурном подразделении отвечает руководитель подразделения Компании (должностное лицо, назначенное ответственным за защиту и обработку ПДн в подразделении).

Соблюдение режима защиты персональных данных обязательно для всех работников Компании.

4.2. Порядок (правила) обработки персональных данных субъектов.

Компания соблюдает принципы и условия обработки персональных данных, установленные законодательством Российской Федерации.

Обработка персональных данных субъектов осуществляется в целях обеспечения соблюдения законов и иных правовых актов РФ, в целях исполнения обязательств по договорам с субъектом, проведения расчетов в рамках заключенных договорах и отношений, возникших между компанией, как оператором и субъектом персональных данных.

Компания не получает и не обрабатывает специальные категории персональных данных, в том числе, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта.

4.2.1. В Компании обрабатываются субъекты персональных данных, подразделяющиеся на следующие категории:

- работники, имеющие договорные отношения с Компанией;

- родственники работников, имеющих договорные отношения с Компанией;

- соискатели на вакантные должности;

- работники контрагентов по гражданско-правовым договорам, заключенным с Компанией;

- посетители офисов Компании;

4.2.2. Согласие на обработку персональных данных предоставляют:

- работники Компании - посредством предоставления согласия в письменной форме при заключении договора, в процессе его исполнения;

- родственники работников Компании – посредством предоставления согласия в письменной форме в случаях, когда согласие требуется в соответствии с действующим законодательством;

- соискатель на вакантную должность - посредством действий по предоставлению/направлению резюме;

- работники контрагентов – предоставляют свое согласие на обработку персональных данных контрагенту, т.е. контрагент получает согласие от своего работника, уведомляет его о передачи персональных данных в ООО «Форк ИТ» для обеспечения взаимодействия по договору. При оформлении постоянного пропуска Компании согласие на обработку персональных данных работника контрагента получается Компанией при выдаче пропуска;

- посетители офисов – принятия условий обработки посредством предоставления документа для прохода на территорию Компании;

4.2.2. В соответствии с утвержденной Политикой обработки ПДн определен Перечень обрабатываемых персональных данных субъектов (Приложении № 1). Перечень представлен в виде сводной таблицы, сформированной по категориям субъектов.

4.2.3 Обработка субъектов осуществляется путем автоматизированной, не автоматизированной и смешанной обработки персональных данных.

4.2.4. Уничтожение персональных данных.

Персональные данные уничтожаются после достижения цели обработки, если в отношении персональных данных законодательством не установлены обязательные сроки хранения. Порядок уничтожения определен в Порядке «Обращения информации ограниченного доступа в Компании». Формы образцов актов уничтожения персональных данных субъекта представлены в настоящем Положении (Приложение №5).

4.2.5. Обезличивание персональных данных.

Обезличивание персональных данных субъектов, выбор способа, метода обезличивания должен соответствовать требованиям Приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 5 сентября 2013 г. N 996 «Об утверждении требований и методов по обезличиванию персональных данных».

4.3. Порядок передачи информации, содержащей персональные данные.

4.3.1. Передача информации, содержащей персональные данные осуществляется: по защищенным каналам внутренней сети ООО «Форк ИТ»»; посредством доставки почтовыми и курьерскими организациями, имеющими соответствующие лицензии; по защищенным каналам внутри группы компаний по сети интернет.

4.3.2. Передача персональных данных контрагенту для обработки по поручению Компании осуществляется только на основании заключаемого с этим лицом договора, определяющего:

- цели обработки;
- перечень действий с ПДн;
- требования (правовые, организационные и технические) к защите обрабатываемых ПДн, в том числе предусмотренные ст. 19 Федерального закона «О персональных данных) от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении ПДн;
- обязанности лица, осуществляющего обработку ПДн, соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;
- ответственность за невыполнение определенных в договоре требований к защите ПДн;
- других требований, утвержденных в Компании в виде внутренних нормативных документов.

4.4. Порядок выполнения правовых, организационных и технических (организационно-технических) мероприятий по защите персональных данных.

4.4.1. К **правовым мероприятиям** относится разработка нормативно-правовых актов Компании, в соответствии с требованиями законодательства РФ в области обработки и защиты персональных данных. Основными нормативно-правовыми актами в Компании является настоящее Положение, регламенты и процедуры, регламентирующие порядок обработки субъектов (работников, посетителей и т.д.).

Обеспечение данных мероприятий осуществляется Юридическим отделом и Службой безопасности.

Юридический отдел - отвечает за разработку и внедрение в Компании правовых мер в области защиты и обработки персональных данных регламентирующих обработку персональных данных, обеспечивают правомерность и соответствие принимаемых руководством Компании решений и действий в области обработки персональных данных

законодательным актам РФ. Работники отдела являются экспертами в области законодательства РФ по защите персональных данных.

Служба безопасности - отвечает за регламентацию общих требований по защите и обработке персональных данных, общих правил, мероприятий, требований к защите ПДн в информационных и технологических системах Компании. Работники блока являются экспертами в области защиты и обработки персональных данных. Работники информационной безопасности являются экспертами в области технической защиты информации / информационных технологий.

Функциональные подразделения Компании, осуществляющие обработку ПДн, при разработке локальных нормативных актов обязаны руководствоваться настоящим Положением, внутренними нормативными документами Компании в области информационной безопасности, персональных данных. При разработке и согласовании внутренних документов привлекают экспертов Юридического отдела и Службы безопасности.

4.4.2. К **организационным мероприятиям,** которые проводятся в Компании, относятся:

- распределение ответственности между функциональными подразделениями Компании в области обработки и защиты персональных данных; назначение ответственных должностных лиц за защиту и обработку ПДн в подразделениях Компании;
- определение перечня персональных данных, обрабатываемых Компанией в процессе осуществления своей деятельности;
- определение, перечня информационных систем персональных данных;
- определение порядка доступа работников Компании в помещения, в которых ведется обработка персональных данных;
- реализация / выполнение требований пропускного и внутриобъектового режимов на объектах Компании;
- организация охраны объектов, мест обработки персональных данных;
- определение правил рассмотрения запросов субъектов персональных данных, их представителей;
- организация работы с персоналом Компании, по доведению (разъяснению) требований законодательства РФ, нормативных актов Компании, в области защиты ПДн;
- осуществление внутреннего контроля выполнения требований законодательства РФ, нормативных документов по Компании в области ПДн.

4.4.3. К **техническим (организационно-техническим) мероприятиям,** которые проводятся в Компании, относятся:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Компании;
- обеспечение безопасности персональных данных при их обработке в автоматизированных информационных системах персональных данных Компании.
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- порядок использования съемных носителей информации;
- предупреждение и своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

### 4.5. Требования к организации обработки персональных данных, местам обработки, местам хранения персональных данных

4.5.1. Требования к организации обработки персональных данных, осуществляемой без использования средств автоматизации:

1) Персональные данные при их обработке, должны обособляться от иной информации, в частности, путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков);

2) При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы;

3) Для каждого субъекта персональных данных определяются отдельные места хранения персональных данных (материальных носителей). Т.е. хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях организовывается раздельно;

4) Для каждого субъекта устанавливается отдельный перечень лиц, осуществляющих обработку персональных данных, либо имеющих доступ к данным субъекта;

5) Условия хранения персональных данных должны обеспечивать сохранность этих данных, а также исключать несанкционированный доступ.

4.5.2. Обработка персональных данных работникам Компании разрешается на рабочих местах, размещенных на объектах Компании.

**Руководитель** перед тем, как разрешить на объекте (помещении) обработку персональных данных, **обязан:**

- установить/определить рабочие места (пространство, зоны) для работников, осуществляющих обработку ПДн;
- определить места хранения персональных данных (материальных носителей), исключающие несанкционированный доступ к информации ограниченного доступа и довести их до подчиненных;
- определить места и порядок проведения встреч/приема третьих лиц (посетителей, клиентов, контрагентов);
- провести инструктаж с подчиненными работниками о порядке соблюдения режима защиты и обработки персональных данных в подразделении;

4.5.3. Требования к местам хранения. Требования к помещению (объекту), предназначенному для обработки персональных данных и организации работы в нем.

Помещение (объект), в котором осуществляется обработка персональных данных, должно пройти категорирование по защищенности, должно быть оснащено техническими средствами охраны.

Руководитель перед обработкой персональных данных в подразделении обязан убедиться в соответствии оснащения техническими средствами охраны помещения/объекта категории защищенности.

Места хранения материальных носителей, содержащие персональные данные, определяются руководителями, при необходимости согласовываются с работником безопасности. Документы (материальные носители), содержащие персональные данные хранятся в охраняемом (закрытом) помещении структурного подразделения, в ящиках/шкафах/сейфах под замком.

Ключи от помещения, в котором хранятся персональные данные субъектов ПДн, в течение рабочего дня находятся у руководителя (ответственного работника), который несет ответственность за сохранность вверенных ему персональных данных.

Проведение уборки, иных видов обслуживания помещения, где ведется обработка персональных данных, обязательно производится в присутствии и под контролем работников Компании.

Руководитель, в подразделении которого осуществляется обработка персональных данных, устанавливает /определяет:

- выделенные зоны (пространство, помещения) для работников, осуществляющих обработку ПДн;

- выделенные зоны (пространство, помещения), в котором осуществляется хранение документов, содержащих ПДн (т.е. где размещены шкафы, тумбы, сейфы для документов);

- выделенные зоны (пространство, помещения) для посетителей.

Средства вывода информации (принтер, факс и т.д.) должны находиться в зоне, исключающей нахождение посторонних лиц. При использовании средств вывода информации**, работник Компании обязан** контролировать передачу/вывод информации, в рамках исключения действий, направленных на раскрытие персональных данных неопределенному кругу лиц (обязательно обращается внимание на выбор корпоративного печатающего устройства). В Компании **запрещено** бесконтрольно производить печать документов, содержащих персональные данные субъекта, а также конфиденциальных документов.

4.5.4. Требования к местам обработки персональных данных. Требования к рабочему месту (рабочему пространству) работника.

Размещение рабочего места работника, осуществляющего обработку персональных данных, должно исключать возможность обозрения находящихся на его рабочем столе документов посторонними лицами. Информация на экране персонального компьютера работника не должна быть видна третьим лицам, не допущенным к обработке ПДн, при необходимости могут применяется другие виды защиты информации на экране компьютера (защитная пленка).

На рабочем месте работника должно быть минимальное количество документов (материалов) конфиденциального характера, т.е. должен находиться только тот документ и материалы к нему, с которыми в настоящее время работает работник.

4.5.5. Обязанности работника при работе в дистанционном режиме работы.

А) Работнику, использующему удаленный доступ к корпоративным ИТ-ресурсам запрещается:

- сохранять корпоративные пароли в письменном виде, что может стать причиной несанкционированного доступа к корпоративным информационным ресурсам;

- передавать/раскрывать парольную информацию кому бы то ни было;

- использовать любые типы внешних дисков или облачные интернет-сервисы для копирования/хранения информации ограниченного доступа и персональных данных;

- допускать к работе на мобильном устройстве посторонних лиц. Осуществлять доступ и обработку персональных данных и иных данных, отнесенных в Компании к информации ограниченного доступа, в присутствии посторонних лиц, в том числе членов семьи;

- сохранять на мобильное устройство снимки экрана, производить фото/видео съемку экрана удаленного рабочего места, с открытыми приложениями обработки персональных данных клиентов и работников Компании, передавать или ознакамливать с персональными данными третьих лиц (клиентов, работников третьих лиц, работников Компании), не имеющих доступа к таким данным;

- осуществлять локальное хранение (скачивание) ИОД и персональных данных из корпоративных информационных систем на мобильное устройство;

- оставлять удаленное мобильное устройство без блокировки доступа к нему (необходимо закрывать все активные соединения с корпоративной сетью после завершения работы с приложениями);

- использовать пароли доступа к информационным ресурсам и системам Компании для доступа к сторонним интернет-ресурсам.

**4.7. При работе с персональными данными, работнику запрещено:**

1) нарушать каким-либо образом конфиденциальность персональных данных субъекта (без основания передавать третьим лицам, распространять умышленно, или по неосторожности и т.п.);

2) покидать рабочее место с включенным персональным компьютером без применения аппаратных или программных средств блокирования доступа к персональному компьютеру, а также оставлять на рабочем месте документы, содержащие персональные данные;

3) допускать к своему рабочему месту (в том числе, при дистанционном формате работы) посторонних лиц (передавать коды/пароли доступа, либо документацию, содержащую персональные данные, другим лицам);

4) хранить в доступном месте значения кодов и паролей доступа, передавать свой пароль иным лицам;

5) использовать учетные записи в информационной системе, не принадлежащие Пользователю;

6) производить подбор кодов и паролей доступа других пользователей;

7) пользоваться неучтенными носителями, при обработке персональных данных;

8) использовать внешние накопители (в том числе, дискеты, DVD/CD диски, USB устройства, и т.п.) вне установленных в Компании процедур;

9) выносить электронные и бумажные носители с персональными данными за пределы объектов Компании не по служебным вопросам; Передавать ПДн, по каналам связи сети общего пользования и сети Интернет, включая системы обмена сообщениями;

10) препятствовать штатному исполнению служебных программ (сценариев регистрации в сети, антивирусного, диагностического, инвентаризационного и т.п. программного обеспечения); изменять конфигурацию, настройку и установленный порядок работы аппаратных и программных ИТ средств Компании (открывать, разбирать, ремонтировать технические средства, вносить изменения в конструкцию, подключать нештатные блоки устройства);

11) бесконтрольно производить печать документов, содержащих персональные данные субъекта, а также конфиденциальных документов.

## 5. Права субъекта, обязанности, ответственность Компании и должностных лиц

### 5.1. Права субъекта персональных данных

Субъект персональных данных имеет право:

1) на получение информации, касающейся обработки его персональных данных (часть 7 статьи 14 Федерального закона «О персональных данных» № 152-ФЗ), в том числе *содержащей*:

- подтверждение факта обработки персональных данных в Компании;
- правовые основания и цели обработки персональных данных;
- цели и применяемые в Компании способы обработки персональных данных;
- наименование и место нахождения Компании, сведения о лицах (за исключением работников Компании), которые имеют доступ к персональным данным;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту ПДН, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок реализации субъектом персональных данных своих прав, предусмотренных настоящим Федеральным законом;
- информацию об осуществленной или предполагаемой трансграничной передаче (статья 3 ФЗ № 152) данных;
- наименование /фамилию, имя, отчество/ и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные законодательством РФ.

2) требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

3) на обжалование действий или бездействия в Уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) или в судебном порядке;

4) на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 (№152-ФЗ).

**5.2. Обязанности Компании при сборе персональных данных:**

- безвозмездно предоставить субъекту ПДн или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных;

- внести необходимые изменения, уничтожить или блокировать персональные данные (по предоставлению заявления субъекта персональных данных, или его законного представителя), если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях, принятых мерах Компания обязана уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

В случае выявления неправомерной обработки персональных данных заблокировать персональные данные.

В случае выявления неправомерных действий с персональными данными в срок, не превышающий 3 (трех) рабочих дней с даты выявления, Компания обязана прекратить неправомерную обработку персональных данных и устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерности действий с персональными данными, Компания обязана уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных обязан уведомить субъекта персональных данных или его законного представителя.

В случае достижения целей обработки, Компания обязана прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 (тридцати) дней с момента достижения целей обработки.

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных (путем подачи заявления) **Компания обязана** прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 (тридцати) дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Компанией и субъектом персональных данных. Об уничтожении персональных данных **Компания обязан** уведомить субъекта персональных данных. В случае отсутствия возможности уничтожения в указанные выше сроки, Компания осуществляет блокирование персональных данных и обеспечивает уничтожение ПДн в срок не более, чем 6 (шести) месяцев.

❖ Оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации.

**5.3. Ответственность должностных лиц, работников Компании**

5.3.1. Компания, а также должностные лица, виновные в нарушении требований Федерального закона № 152, несут ответственность (административную, уголовную, иную) предусмотренную законодательством Российской Федерации

5.3.2. Руководители структурных подразделений Компании несут ответственность за организацию режима защиты и обработки ПДн в подчиненных подразделениях в соответствии с настоящим Положением.

Ответственные за обработку и защиту ПДн в Структурном подразделении назначаются распоряжением/указанием соответствующего Руководителя. Права и обязанности ответственных за обработку и защиту ПДн приведены в Таблице № 1.

Права и обязанности ответственных за обработку и защиту ПДн указаны в Таблице №1 к настоящему Положению.

**Таблица №1**

| **Должность** | **Обязанности (ответственность)** | **Права** |
|---|---|---|
| Руководитель структурного подразделения | 1. Организовывать и внедрять, выполнение политик, приказов, ВНД в области обработки и защиты ПДн в структурном подразделении;<br>2. Назначать должностных лиц, ответственных за обработку и защиту ПДн в Структурном подразделении;<br>2. Организовать в Структурном подразделении режим защиты и обработки ПДн, в соответствии с требованиями ВНД Компании;<br>3. Обеспечить в Структурном подразделении финансирование мероприятий, в области защиты и обработки ИОД и ПДн;<br>4. Разрабатывать внутренние нормативные документы, представлять отчеты о состоянии режимов защиты и обработки ПДн в подразделении;<br>5. Организовывать контроль исполнения приказов и распоряжений по обработке и защите ПДн. | 1. Делегировать свои полномочия другим должностным лицам, ответственным за организацию работы с ИОД в Структурном подразделении<br>2. Реализовывать свои права в рамках трудового договора / должностной инструкции.<br>3. Осуществлять контроль исполнения Приказов по Компании и настоящего Положения.<br>4. Накладывать взыскания на работников за неисполнение Приказа и Положения. |
| Ответственный за обработку и защиту ПДн в Структурном подразделении. | 1. Контролировать порядок обращения (приема, передачи, использования, хранения и т.п.) документов, содержащих ИОД, в соответствии с требованиями настоящего Положения и иных приказов по Компании;<br>2. Доводить политики, приказы, процедуры в области защиты и обработки ПДн, решения комиссий по защите ПДн до руководителя и работников;<br>3. Своевременно выполнять, реализовывать решения/мероприятия комиссий по защите ИОД и ПДн, ответственного за защиту и обработку | 1. Запрашивать и получать необходимые материалы для организации и проведения работ по обработке и защите ПДн;<br>2. Требовать от ответственных за организацию работы по защите ИОД по нижестоящим подразделениям выполнение мероприятий по порядку обращения и защиты ПДн (ИОД); |

| | | |
|---|---|---|
| | персональных данных в блоке.<br>4. Осуществлять контроль за выполнение работниками, Структурного подразделения требований по обработке и защите ПДн; принимать решения и давать указания обязательные для исполнения;<br>5. Незамедлительно докладывать своему руководителю о всех случаях нарушения правил обращения и защиты ИОД в Структурном подразделении. | |

## 6. Порядок рассмотрения обращений, запросов субъектов и их представителей

6.1. Сведения предоставляются субъекту персональных данных или его представителю при поступлении обращений (заявление, жалобе, запрос).

Обращение от субъекта персональных данных должно содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных (его представителя), сведения о дате выдачи указанного документа и выдавшем его органе;

- сведения, подтверждающие участие субъекта персональных данных в отношениях с Компанией (номер и дата договора), либо сведения, иным образом подтверждающие факт обработки персональных данных Компанией;

- подпись субъекта персональных данных или его представителя.

6.2. Обращение от субъекта персональных данных или его представителя может быть направлено Компании в форме электронного документа и подписано электронной подписью в соответствии с законодательством Российской Федерации.

6.3. При поступлении обращения от субъекта персональных данных или его представителя, уполномоченный работник Компании должен зарегистрировать его в журнале учета корреспонденции в день поступления, передать лицу ответственному за обработку персональных данных в целях определения структурного подразделения для ответа на обращение.

6.4. Компания в течение 30 (тридцати) дней со дня получения заявления обязана сообщить ему информацию о наличии персональных данных, предоставить возможность ознакомления с ними.

6.5. Сведения, указанные в 6.1. должны быть предоставлены субъекту персональных данных или его представителю в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.6. В случае отказа в предоставлении субъекту или его представителю информации о наличии персональных данных о соответствующем субъекте, а также самих персональных данных, мотивированный ответ должен быть дан в письменной форме в срок, не превышающий 30 (тридцати) дней со дня получения запроса.

6.7. Субъекту персональных данных или его представителю безвозмездно представляется возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, при необходимости внесение в них необходимых уточнений. Компания обязана уничтожить или блокировать персональные данные, если субъект персональных данных считает их неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели

обработки. О внесенных уточнениях и предпринятых мерах необходимо уведомить субъекта персональных данных или его представителя, а также третьих лиц, которым персональные данные этого субъекта персональных данных были переданы.

6.8. В случае, если сведения, указанные в пункте 6.1., а также обрабатываемые персональные данные были предоставлены для ознакомления субъекта персональных данных по его запросу, субъект персональных данных вправе обратиться повторно, или направить повторный запрос в целях получения сведений, указанных в пункте 6.1., и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального заявления, если более короткий срок не установлен федеральным законом, принятыми в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.9. Субъект персональных данных вправе обратиться повторно, или направить повторный запрос в целях получения сведений, указанных в пункте 6.1, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 6.8 настоящего Раздела, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 6.1, должен содержать обоснование направления повторного запроса.

6.10. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 6.8. и 6.9. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

6.11. Формы образцов запросов и уведомлений субъекта обработки персональных данны отражены в анстоящем Положении (Приложение № 4).

## 7. Заключительные положения

Настоящее Положение утверждается Генеральным директором, и вступает в силу с момента опубликования.

Вопросы толкования положений настоящего Порядка следует адресовать в Юридический отдел или Службу Безопасности.

С момента вступления в силу настоящего Положения, предыдущее Положение считать недействительным.

**Приложение № 1**
к Положению «Обработка и защита персональных данных»

**Перечень персональных данных, обрабатываемых в Компании**

| № п. п. | Вид деятельности | Категория субъектов ПДн | Перечень обрабатываемых категорий ПДн | Цель обработки | Срок хранения | Правовые основания для обработки |
|---|---|---|---|---|---|---|
| 1. | Кадровое администрирование | Работник, имеющий договорные отношения с Компанией | фамилия, имя, отчество работника; паспортные и биографические данные работника; пол работника гражданство работника; должность работника; места регистрации и фактического проживания работника; номера домашнего телефона работника и личные номера телефонов членов его семьи; адрес электронной почты работника (при наличии), семейное положение и состав семьи работника, в том числе данные о Свидетельстве о вступлении в брак, данные о Свидетельстве о рождении ребенка; место учебы или работы с<br>работника, прошлая трудовая деятельность работника, стаж работы; социальное положение работника; образование работника, в том числе наименование учебного заведения, номер и дата выдачи документа об образовании; сведения об имущественном положении работника и членов его семьи; фотография работника; данные страхового свидетельства государственного пенсионного страхования; данные полиса ОМС; ИНН работника; сведения о воинском учете, в том числе данные военного билета; информация о владении иностранными языками; информация о владении компьютером, общие сведения о профессиональной пригодности работника по состоянию здоровья, необходимые для выполнения трудового договора и требований законодательства; сведения о заработной плате и иных выплатах и удержаниях, получаемых и производимых в процессе трудовой деятельности у | кадровое обеспечения деятельности Компании; выполнения обязанностей по трудовым договорам | Архивное хранение в течение 75 лет | Трудовой договор, Трудовой кодекс, Согласие, Форма Т-2. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | Оператора, данные об автотранспортном средстве работника, номера счетов; данные водительского удостоверения (для работников - водителей);государственный регистрационный номер личного автомобиля (в случае оформления пропуска на въезд на объекты ООО «Форк ИТ»); реквизиты документа, подтверждающего инвалидность (в установленных законом случаях); информация о текущей занятости, включая рабочие контактные данные (рабочий номер телефона, номер телефона рабочей сотовой связи, адрес электронной почты, номер факса и т.д.); описание должности и должностных обязанностей; дата найма и прекращения трудовых отношений; информация о дисциплинарных взысканиях; информация о предоставленных льготах; информация о несчастных случаях и выплаченных страховых возмещениях; сведения о об отработанном времени и трудовом графике, а также отпусках; данные о полученных доступах к IT системам Компании, включая логины и пароли; сведения о повышении квалификации (свидетельства и сертификаты); оценка и информация о производительности и эффективности труда Работника:**:** биометрические данные в виде фотографии для системы контроля управления доступом в помещения Компании; данные о пройденном обязательном медицинском освидетельствовании; листок нетрудоспособности (факты обращения за медицинской помощью), в том числе факты наступления страхового случая по договору, заключаемому Компанией; информация о незаконным или нежелательным поведением в связи с проведением служебных проверок или в связи с расследованием неправомерного поведения в случае нарушения положений действующего применимого законодательства; а также иные данные Работника, связанные с выполнением должностных обязанностей. | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2. | Кадровое администрирование | Родственник работника, имеющего договорные отношения с Компанией | фамилия, имя, отчество родственника работника Компании; паспортные и биографические данные; адрес регистрации, телефонные номера; сведения об имущественном положении (в случае предоставления); | Реализация требований трудового законодательства. Участие в программах Компании. | Архивное хранение в течение 75 лет в личном деле работника Компании | Трудовой кодекс, Согласие, форма Т-2. |
| 3. | Кадровое администрирование | Соискатель на вакантную должность | фамилия, имя, отчество соискателя вакантной должности в ООО «Форк ИТ» (далее соискатель); паспортные и биографические данные соискателя; гражданство соискателя; места регистрации и фактического проживания соискателя; номера домашнего телефона соискателя и личные телефонов членов его семьи; семейное положение и состав семьи соискателя; место учебы или работы соискателя, прошлая трудовая деятельность соискателя, стаж работы; социальное положение соискателя; образование соискателя, в том числе наименование учебного заведения, номер и дата выдачи документа об образовании; информация о владении иностранными языками; информация о владении компьютером; | Кадровое обеспечение Компании | 30 дней с момента принятия решения о закрытии вакансии, если иной срок не указан в согласии, но не более 3 лет. | Согласие |
| 4. | Договорная работа | Работники контрагентов по гражданско-правовым договорам, заключенным с Компанией | фамилия, имя, отчество, дата рождения, должность, адрес работника контрагента, реквизиты документа, удостоверяющего личность, абонентские номера, фотография (для работников контрагентов оформляющих многоразовый пропуск для доступа на территорию Компании. | Взаимодействие в рамках заключенного гражданско-правового договора, выполнение требований законодательных актов, нормативных документов | 5 лет с момента прекращения действия договора с контрагентом | Договор |

* Персональные данные субъектов относятся к категории информации ограниченного доступа. Конфиденциальность, сохранность и защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий обеспечивается путем принятия необходимых правовых, организационных и технических мер для защиты от неправомерного или случайного доступа к ним.

Работа с Персональными данными субъектов должна осуществляться только в целях, по перечням и в сроки, которые необходимы для выполнения задач Оператора или пользователя персональных данных.

**Приложение № 2**
к Положению «Обработка и защита персональных данных»

**Таблица действий в ответ на запросы субъекта, его представителя**

| № п.п | Запрос | Действия | Срок | Ответ |
|---|---|---|---|---|
| 1 | Наличие ПДн | Подтверждение обработки ПДн | 30 дней (согласно пункту 1 статьи 20, 152-ФЗ) | Подтверждение обработки ПДн |
| | | Отказ подтверждения обработки ПДн | 30 дней (согласно пункту 2 статьи 20, 152-ФЗ) | Уведомление об отказе подтверждения обработки ПДн |
| 2 | Ознакомление с ПДн | Предоставление информации по ПДн | 30 дней (согласно пункту 1 статьи 20, 152-ФЗ) | 1. Подтверждение обработки ПДн, а также правовые основания и цели такой обработки;<br>2. Способы обработки ПДн;<br>3. Сведения о лицах, которые имеют доступ к ПДн;<br>4. Перечень обрабатываемых ПДн и источник их получения;<br>5. Сроки обработки ПДн, в том числе сроки их хранения;<br>6. Информация об осуществленных или о предполагаемой трансграничной передаче. |
| | | Отказ предоставления информации по ПДн | 30 дней (согласно пункту 2 статьи 20, 152-ФЗ) | Уведомление об отказе предоставления информации по ПДн |
| 3 | Уточнение ПДн | Изменение ПДн | 7 рабочих дней со дня предоставления уточняющих сведений (согласно пункту 3 статьи 20, 152-ФЗ) | Уведомление о внесенных изменениях |
| | | Отказ изменения ПДн | 30 дней | Уведомление об отказе предоставления информации по ПДн |
| 4 | Уничтожение ПДн | Уничтожение ПДн | 7 рабочих дней со дня предоставления сведений о незаконном получении | Уведомление об уничтожении |

| | | | | |
|---|---|---|---|---|
| | | | ПДн или отсутствии необходимости ПДн для заявленной цели обработки (согласно пункту 3 статьи 20, 152-ФЗ) | |
| | | Отказ уничтожения ПДн | 30 дней | Уведомление об отказе уничтожения ПДН |
| 5 | Отзыв согласия на обработку ПДн | Прекращение обработки и уничтожение ПДн | 3 рабочих дня (согласно пункту 5 статьи 21, 152-ФЗ) | Уведомление о прекращении обработки и уничтожения ПДн |
| | | Отказ прекращения обработки и уничтожения ПДн | 30 дней | Уведомление об отказе прекращения обработки и уничтожения ПДн |
| 6 | Недостоверность ПДн субъекта | Блокировка ПДн | С момента обращения Субъекта ПДн о недостоверности или с момента получения запроса на период проверки (согласно пункту 1 статьи 21, 152-ФЗ) | Уведомление о внесенных изменениях |
| | | Изменение ПДн | 7 рабочих дней со дня предоставления уточненных сведений (согласно пункту 2 статьи 21, 152-ФЗ) | |
| | | Снятие блокировки ПДн | | |
| | | Отказ изменения ПДн | 30 дней | Уведомление об отказе изменения ПДН |
| 7 | Неправомерность действий с ПДн субъекта | Прекращение неправомерной обработки ПДн | 3 рабочих дня (согласно пункту 5 статьи 21, 152-ФЗ) | Уведомление об устранении нарушений |
| | | Уничтожение ПДн в случае невозможности обеспечения правомерности обработки | 10 рабочих дней (согласно пункту 3 статьи 21, 152-ФЗ) | Уведомление об уничтожении ПДн |
| 8 | Достижение целей обработки ПДн субъекта | Прекращение обработки ПДн Уничтожение ПДн | 30 рабочих дней (согласно пункту 4 статьи 21, 152-ФЗ) | Уведомление об уничтожении ПДн |

**Приложение № 3**
к Положению «Обработка и защита
персональных данных»

**Формы образцов запросов и уведомлений субъекта обработки персональных данных**

### 1) Запрос к субъекту на уточнение персональных данных.

**Запрос**

Уважаемый(ая) _____
(ФИО),
в связи с _____ у ООО «Форк ИТ» возникла необходимость получения следующей информации, составляющей Ваши персональные данные
_____
(перечислить информацию)
_____
_____
Просим Вас предоставить указанные сведения в течение 7 рабочих дней с момента получения настоящего запроса.

По результатам обработки указанной информации нами планируется принятие следующих решений, которые будут доведены до Вашего сведения _____.

_____ _____ _____
(должность) (подпись) (ФИО)
"___" _____ 20__ г.

### 2) Уведомление субъекта о блокировании

Уважаемый(ая) _____
(Ф.И.О.), в связи с _____ сообщаем Вам, что Ваши персональные данные:
_____
заблокированы.

_____ _____ _____
(должность) (подпись) (ФИО)

"___" _____ 20__ г.

### 3) Уведомление субъекта об уточнении

Уважаемый(ая) _____ (Ф.И.О.), в связи с _____ сообщаем Вам, что Ваши персональные данные уточнены в соответствии со сведениями: _____ _____.

_____ _____ _____
(должность) (подпись) (ФИО)

"___" _____ 20__ г.

### 4) Уведомление субъекта об уничтожении

Уважаемый(ая) _____ (Ф.И.О.), в связи с _____ сообщаем Вам, что Ваши персональные данные _____ уничтожены.
(указать персональные данные)

_____ _____ _____
(должность) (подпись) (ФИО)

"___" _____ 20__ г.

### 5) Уведомление субъекта об устранении допущенных нарушений

Уважаемый(ая) _____ (Ф.И.О.), в связи с _____ сообщаем Вам, что все допущенные нарушения при обработке Ваших персональных данных устранены.

_____ _____ _____
(должность) (подпись) (ФИО)

"___" _____ 20__ г.

### 6) Уведомление об отсутствии обрабатываемых персональных данных

Уважаемый(ая) _____ (Ф.И.О.), в связи с поступившим от Вас заявлением сообщаем Вам, что компания ООО «Форк ИТ» не обрабатывает Ваши персональные данные.

_____ _____ _____
(должность) (подпись) (ФИО)

"___" _____ 20__ г.

### 7) Уведомление субъекта об обработке персональных данных

Уважаемый(ая) _____ (Ф.И.О.), в связи с поступившим от Вас заявлением сообщаем Вам, что компания ООО «Форк ИТ» обрабатывает Ваши следующие персональные данные:_____
_____
_____

Целью обработки Ваших персональных данных является взаимодействие в рамках выполнения требований законодательства; обработка ведется с применением автоматизированных и не автоматизированных средств.
Сроки обработки Ваших персональных данных, в том числе сроки их хранение осуществляется в течение срока действия договора и 5 лет после расторжения договора.
Ваши персональные данные могут передаваться третьим лицам при наличии Вашего согласия.

_____
(должность) (подпись) (ФИО)

"___" _____ 20__ г.

### 8) Уведомление о наименовании организации и адресе Компании.

### Уведомление

Уважаемый(ая) _____ (Ф.И.О.), в связи с поступившим от Вас заявлением сообщаем Вам, что Ваши персональные данные обрабатываются нашей компанией на основании, Федерального закона «О персональных данных». Наше наименование и местонахождение: ООО «Форк ИТ» 624090, Свердловская область, Г.О. Верхняя Пышма, г. Верхняя Пышма, ул. Орджоникидзе, д. 22, каб.106

_____ _____ _____
(должность) (подпись) (ФИО)

"___" _____ 20__ г.

**Приложение № 4**
к Положению «Обработка и защита
персональных данных»

**Формы образцов актов уничтожения персональных данных субъекта**

**1) АКТ об уничтожении персональных данных на бумажных носителях.**

**Утверждаю**
Генеральный директор_____

_____ _____

**АКТ**
**об уничтожении персональных данных**

г. Москва _*ДД.ММ.ГГГГ*_

Учетный номер Акта _____

Мы, ниже подписавшиеся, составили настоящий Акт об уничтожении бумажных носителей, содержащих персональные данные в количестве _*указать кол-во*___ шт. Процедура уничтожения выполнена на основании _____
_____
(указать основание/ предписание/обращение и т.п)

Настоящий Акт хранить в _____ в течение 5 лет, затем уничтожить.

| | | |
|---|---|---|
| (должность) | (подпись) | (ФИО) |
| (должность) | (подпись) | (ФИО) |
| (должность) | (подпись) | (ФИО) |

**2) Акт об уничтожение персональных данных в IT системах.**

**АКТ № X-УПДн-YYYY-MM-DD**
**об уничтожении персональных данных**
**в ИС _____**

г. Москва DD month YYYY г.

Комиссия в составе: _____
_____
_____
_____

настоящим Актом подтверждает, что в период с DD месяц по DD месяц YYYY года в соответствии с распоряжением №_____ были проведены работы по уничтожению в ИС _____ персональных данных.

Результаты названных работ отражены в файлах-реестрах идентификаторов документов и записей, перечень которых приведен в Приложении к настоящему Акту; файлы-реестры записаны на CD диск, который маркирован номером настоящего Акта.

Настоящий Акт является основанием для уничтожения соответствующих данных в хранилищах (архивах) оригиналов документов.

Подписи:

| | | |
|---|---|---|
| (должность) | (подпись) | (ФИО) |
| (должность) | (подпись) | (ФИО) |
| (должность) | (подпись) | (ФИО) |

**Приложение № 5**
к Положению «Обработка и защита
персональных данных»

СОГЛАСИЕ
на обработку персональных данных

Я, субъект персональных данных: _____ (Ф.И.О. полностью), основной документ, удостоверяющий личность: _____ (наименование, серия, номер, дата выдачи, выдавший орган), зарегистрированного(-ой) по адресу: _____, в лице представителя субъекта персональных данных (заполняется в случае получения согласия от представителя субъекта персональных данных) _____ (Ф.И.О. полностью), основной документ, удостоверяющий личность: _____ (наименование, серия, номер, дата выдачи, выдавший орган), зарегистрированный(-ая) по адресу: _____, _____ (реквизиты доверенности или иного документа, подтверждающего полномочия представителя), в соответствии со ст. 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" даю конкретное, предметное, информированное, сознательное и однозначное согласие на обработку своих персональных данных Обществу с ограниченной ответственностью «Форк ИТ» ИНН 7718177230, находящемуся по адресу: 624090, Свердловская область, г Верхняя Пышма, ул Орджоникидзе, д. 22, каб. 106, с целью: _____ (цель обработки персональных данных).

Перечень моих персональных данных, на обработку которых я даю согласие: фамилия, имя, отчество, гражданство, пол, возраст, дата и место рождения, номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе, адрес регистрации по месту жительства, адрес фактического проживания, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, номер телефона, адрес электронной почты.

Разрешаю оператору производить автоматизированную, а также осуществляемую без использования средств автоматизации обработку моих персональных данных, а именно: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Согласие действует до его отзыва либо до завершения цели обработки, в зависимости от того, что наступит раньше. Субъект персональных данных вправе отозвать настоящее согласие на обработку своих персональных данных, письменно уведомив об этом оператора.

Субъект персональных данных:

_____ /_____/
(подпись) (Ф.И.О.)

"__"_____ ____ г.