

Общество с ограниченной ответственностью  
«Аурум плюс»

---

**ПРИКАЗ**

26 июня 2017 года

№ 01/06-2017

г. Северодвинск  
Архангельская область

**Об утверждении положения об обработке и защите персональных данных**

Во исполнение требований Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», а также прочих нормативных документов по защите информации **приказываю:**

1. Утвердить прилагаемое Положение об обработке и защите персональных данных в ООО «Аурум плюс» (далее - Положение).
2. Ознакомить с настоящим приказом и Положением работников ООО «Аурум плюс».
3. Обеспечит неограниченный доступ к Положению и опубликовать Положение в сети Интернет на официальном сайте ООО «Аурум плюс».
4. Контроль исполнения настоящего приказа оставляю за собой.

Директор



И. Н. Покид

## Положение об обработке и защите персональных данных

### 1. Общие положения

1.1. Настоящее Положение отвечает требованиям Конституции Российской Федерации, Федерального закона «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 года, Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006 года и другим нормативно правовым актам.

1.2. Основные понятия, используемые в Положении:

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

— **оператор** – юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

— **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;

— **автоматизированная обработка персональных данных** - обработка персональных данных с помощью вычислительной техники;

— **неавтоматизированная обработка персональных данных** - обработка персональных данных ручным способом;

— **блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уничтожения персональных данных);

— **использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

— **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

— **распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

— **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;

— **защита персональных данных** – деятельность оператора, направленная на предотвращение утечки защищаемых персональных данных, несанкционированных и непреднамеренных воздействиях на защищаемые персональные данные.

— **конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

1.3. Настоящее Положение об обработке и защите персональных данных действует в отношении всех персональных данных, обрабатываемых в ООО «Аурум плюс» (далее – Оператор) и распространяется на всех сотрудников оператора, а также на сотрудников сторонних организаций, взаимодействующих с оператором на основании соответствующих нормативных, правовых и организационно-распорядительных документов.

1.4. Целью Положения является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

1.5. Оператор обрабатывает персональные данные в соответствии со следующими нормативными и правовыми документами:

- Конституцией Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- Федеральным законом от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом от 29.11.2010 №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации».

1.6. Персональные данные обрабатываются в целях исполнения требований Российской Федерации, защиты законных прав и интересов граждан в связи с трудовыми отношениями, а также при оказании медицинской помощи и медицинских услуг, проведении медицинских осмотров и установления медицинского диагноза, исполнения договорных обязательств перед организациями, заключившими договора на оказание медицинских услуг.

1.6. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод субъекта.

1.7. Настоящее Положение утверждается директором ООО «Аурум плюс» и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

## **2. Состав и получение персональных данных**

2.1. Категории субъектов, персональные данные которых обрабатываются:

- физические лица (сотрудники), состоящие в трудовых отношениях с Оператором;

– физические лица (население) персональные данные которых обрабатываются в пределах полномочий и задач Оператора;

2.2. Оператор обрабатывает следующие персональные данные сотрудников:

- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения, место рождения);
- паспортные данные;
- адрес регистрации и места жительства;
- данные о трудовом договоре;
- информацию об образовании, повышении квалификации, аттестации;
- информацию о трудовом стаже;
- семейное положение и состав семьи;
- контактная информация (номера телефонов, адрес электронной почты);
- сведения о регистрации в налоговом органе (ИНН);
- СНИЛС;
- сведения о состоянии здоровья;
- информацию о негосударственном пенсионном обеспечении;
- сведения о воинском учете.

2.3. Оператор обрабатывает следующие персональные данные населения:

- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения, место рождения);
- паспортные данные;
- адрес регистрации и места жительства;
- СНИЛС;
- реквизиты полиса ДМС / ОМС;
- данные о состоянии здоровья (история болезни);
- результаты выполняемых медицинских исследований.

2.4. Все персональные данные Оператор получает непосредственно от субъекта персональных данных либо от законного представителя субъекта персональных данных.

### **3. Обработка и хранение персональных данных**

3.1. Обработка персональных данных Оператором заключается в получении, записи, систематизации, накоплении, хранении, уточнении (обновлении, изменении), использовании, распространении, обезличивании, блокировании, уничтожении и в защите от несанкционированного доступа персональных данных.

3.2. Согласие на обработку персональных данных не требуется, в случае, если заключен договор и обработка персональных данных осуществляется в целях исполнения договора, в иных случаях обработка персональных данных осуществляется при наличии письменного согласия на обработку персональных данных.

3.3. Обработка персональных данных ведется методом смешанной обработки.

3.4. К обработке персональных данных могут иметь доступ только сотрудники Оператора, допущенные к работе с персональными данными для исполнения своих должностных обязанностей и с соблюдением принципов персональной ответственности.

3.5. Прекращение обработки персональных данных субъекта и уничтожение документов, содержащих персональные данные, осуществляется в сроки, установленные законом, или по письменному требованию субъекта персональных данных.

3.6. Персональные данные на бумажных носителях хранятся в запираемых шкафах (в сейфах), доступ к которым является ограниченным.

3.7. Персональные данные в электронном виде хранятся в локальной компьютерной сети Оператора, в электронных папках и файлах в персональных компьютерах заместителя директора ООО «Аурум плюс», бухгалтера и сотрудников, допущенных к обработке персональных данных.

3.8. Передача информации, содержащей персональные данные субъектов персональных данных, третьим лицам осуществляется в организации, с которыми заключены договора на оказание медицинских услуг, в налоговые органы, ПФР РФ, ФСС РФ, органы статистики с согласия субъекта персональных данных с использованием автоматизированных систем по закрытым сертифицированным средствам криптографической защиты каналам связи и методом физической доставки адресату в распечатанном виде;

#### **4. Использование и передача персональных данных**

4.1. Использование персональных данных о состоянии здоровья субъекта осуществляется Оператором исключительно в целях установления медицинского диагноза и оказания медицинских услуг при этом использование персональных данных осуществляется лицами, профессионально занимающимися медицинской деятельностью и обязанными в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

4.2. При передаче персональных данных субъекта Оператор должен соблюдать следующие требования:

4.2.1. Предупредить лиц, получающих персональные данные субъекта о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности. Данное Положение не распространяется в случае обезличивания персональных данных и в отношении общедоступных данных.

4.2.2. Разрешать доступ к персональным данным субъекта только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

4.3. Не допускается отвечать на вопросы, связанные с передачей информации, содержащей персональные данные, по телефону или факсу.

4.4. Оператор вправе предоставлять или передавать персональные данные субъекта третьим лицам в следующих случаях:

- если раскрытие этой информации требуется для соблюдения закона, выполнения судебного акта;

- для оказания содействия в проведении расследований, осуществляемых правоохранительными или иными государственными органами;

- для защиты законных прав субъекта и Оператора.

#### **5. Защита персональных данных от несанкционированного доступа**

5.1. Оператор обязан при обработке персональных данных принимать необходимые организационные и технические меры для защиты персональных данных от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

5.2. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных.

5.3. Для эффективной защиты персональных данных необходимо:

- определить состав сотрудников, функциональные обязанности которых требуют обработки персональных данных;
- ознакомить сотрудников с требованиями федерального законодательства и локальными нормативными документами по защите информации;
- обеспечить учет, хранение материальных носителей информации и их обращение;
- привлекать к дисциплинарной ответственности сотрудников, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных;
- использовать разрешительную систему доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- применять средства криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи;
- размещать технические средства обработки персональных данных в пределах охраняемой территории и поддержать технические средства охраны (сигнализацию) в состоянии постоянной готовности;

5.4. Защита доступа к электронным базам данных, содержащим персональные данные, обеспечивается:

- использованием лицензионных программных продуктов, предотвращающих несанкционированный доступ третьих лиц к персональным данным субъектов;
- разграничением прав доступа с использованием учетных записей;
- системой паролей, пароли устанавливаются системным администратором и сообщаются индивидуально сотрудникам, имеющим доступ к персональным данным.

5.5. Копировать и делать выписки персональных данных разрешается исключительно в служебных целях с письменного разрешения директора ООО «Аурум плюс».

## **6. Обязанности Оператора**

6.1. Оператор обязан:

6.1.1. Осуществлять обработку персональных данных исключительно в целях оказания услуг.

6.1.2. Получать персональные данные непосредственно у субъекта персональных данных или его законного представителя. Сотрудники Оператора должны информировать о целях, предполагаемых источниках и способах получения персональных данных, а также о последствиях отказа дать письменное согласие на их получение.

6.1.3. Не получать и не обрабатывать персональные данные о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях за исключением случаев, предусмотренных законом.

6.1.4. Обеспечить хранение и защиту персональных данных субъекта от неправомерного их использования или утраты.

6.1.5. В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

6.1.6. В случае подтверждения факта недостоверности персональных данных Оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов

персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

6.1.7. В случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.1.8. В случае достижения цели обработки персональных данных Оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

## **7. Права и обязанности субъекта персональных данных**

7.1. Субъект персональных данных имеет право на:

— доступ к информации о самом себе, в том числе содержащей информацию подтверждения факта обработки персональных данных, а также цель такой обработки; способы обработки персональных данных, применяемые Оператором; сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых персональных данных и источник их получения, сроки обработки персональных данных, в том числе сроки их хранения; сведения о том, какие юридические последствия для субъекта может повлечь за собой обработка его персональных данных;

— запрет на распространение персональных данных без его согласия;

— изменение, уточнение, уничтожение информации о самом себе;

— обжалование неправомерных действий или бездействий по обработке персональных данных и соответствующую компенсацию в судебном порядке;

— иные права в соответствии с действующим законодательством.

7.2. Субъект персональных данных обязан:

— предоставлять достоверные персональные данные, необходимые для оказания услуг, идентификации субъекта персональных данных, исполнения договорных обязательств, а также в иных случаях, предусмотренных Федеральными законами Российской Федерации.

## **8. Конфиденциальность персональных данных**

8.1. Сведения о персональных данных субъекта являются конфиденциальными.

8.2. Оператор обеспечивает конфиденциальность персональных данных и обязан не допускать их распространения третьим лицам без письменного согласия субъекта либо наличия иного законного основания.

8.3. Лица, имеющие доступ к персональным данным, обязаны соблюдать режим конфиденциальности, они должны быть предупреждены о необходимости соблюдения режима секретности. В связи с режимом конфиденциальности информации персонального характера должны предусматриваться соответствующие меры безопасности для защиты данных от случайного или несанкционированного уничтожения, от случайной утраты, от несанкционированного доступа к ним, изменения или распространения.

8.4. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются на все носители информации как на бумажные, так и на автоматизированные.

8.5. Режим конфиденциальности персональных данных снимается в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено законом.

## **9. Ответственность за нарушение норм, регулирующих обработку персональных данных**

9.1. Оператор несет ответственность за персональные данные, которые находятся в у него в обработке и закрепляет персональную ответственность сотрудников за соблюдением установленного режима конфиденциальности.

9.2. Каждый сотрудник, получающий для работы документ, содержащий персональные данные субъекта, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

9.3. Субъект персональных данных вправе обратиться с жалобой на нарушение данного Положения, обращения по поводу несоблюдения требований Положения рассматриваются в течение 30 (тридцати) дней с момента получения.

9.4. Сотрудники Оператора обязаны на должном уровне обеспечивать рассмотрение запросов, заявлений и жалоб, а также содействовать исполнению требований компетентных органов.

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

## **10. Заключительные положения**

10.1. Контроль исполнения требований настоящего Положения осуществляется ответственными за организацию обработки персональных данных.

10.2. Все права и обязанности Оператора персональных данных, определяются Федеральным законом «О персональных данных» и иными нормативными правовыми актами в области защиты персональных данных.

10.3. Настоящее Положение может быть пересмотрено в результате изменения нормативных актов, регулирующих защиту персональных данных и деятельность ООО «Аурум плюс».

10.4. Настоящее Положение не заменяет собой действующего законодательства Российской Федерации, регулирующего общественные отношения в сфере обработки персональных данных и обеспечения их безопасности и конфиденциальности.