Приложение № 1
к приказу от « 07 » августа 2017 г. № 26/2

Положение о защите персональных данных Общества с ограниченной ответственностью «ИНФАМЕД»

1. Общие положения

1.1. Положение о защите персональных данных (далее - Положение) определяет основные принципы, цели и порядок хранения, защиты, передачи персональных данных субъектов персональных данных Общества с ограниченной ответственностью «ИНФАМЕД» (далее - Общество, Оператор, ООО «ИНФАМЕД»).

1.2. Настоящее Положение разработано с целью защиты персональных данных от несанкционированного доступа и распространения.

1.3. Настоящее Положение разработано в соответствии с:

- Конституция Российской Федерации от 12.12.1993;
- Трудовым кодексом Российской Федерации от 30.12.2001 № 197-ФЗ;
- Гражданским кодексом Российской Федерации от 30.11.1994 № 51-ФЗ
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказом Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- Учредительным документом (Устав) ООО «ИНФАМЕД»;
- Политикой обработки и защиты персональных данных в ООО «ИНФАМЕД»;
- согласием субъекта персональных данных на обработку персональных данных
- иными нормативными правовыми актами Российской Федерации и нормативными документами уполномоченных органов государственной власти.

2. Термины, определения и принятые сокращения

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

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 средств вычислительной техники.

Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Персональные данные, сделанные общедоступными субъектом персональных данных – персональные данные, доступ неограниченного круга лиц к которым, предоставлен субъектом персональных данных либо по его просьбе.

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

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.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Оператор – юридическое лицо, самостоятельно или совместно с другими лицами осуществляющая обработку персональных данных, а также определяющая цели обработки персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Оператором является Общество, зарегистрированное по адресу: 142700, Московская область, Ленинский район, г. Видное, территория Промзона ОАО ВЗ ГИАП, стр. 473, эт. 2, пом. 9.

3. Цели, принципы обработки и классификация персональных данных

3.1. Персональные данные обрабатываются в Обществе в целях:

- обеспечения соблюдения Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Оператора;
- осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Оператора, в том числе по предоставлению персональных данных в органы государственной власти;
- ведения кадровой работы и бухгалтерского учета;
- регулирования трудовых и иных, непосредственно связанных с ними отношений;
- подготовки, заключения, исполнения и прекращения договоров с контрагентами;
- исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- осуществления прав и законных интересов Оператора в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Оператора, или третьих лиц либо достижения общественно значимых целей;
- информирования потребителей о новых продуктах Оператора, а также об их качестве, эффективности и безопасности;
- организация профессиональных мероприятий и приглашение субъектов персональных данных к участию в данных мероприятиях;
- получения информации о подозреваемой неблагоприятной побочной реакции или подозрении о неэффективности продуктов Оператора, в том числе осуществления мониторинга эффективности и безопасности продуктов Оператора;
- в иных законных целях.

3.2. Обработка персональных данных Оператором осуществляется с учетом необходимости обеспечения защиты прав и свобод работников Оператора и других субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

- обработка персональных данных осуществляется Обществом на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- обработке подлежат только персональные данные, которые отвечают целям их обработки;

- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;

- при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Обществом принимаются необходимые меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных персональных данных;

- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того 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.

3.3. Классификация персональных данных.

Персональные данные классифицируются на следующие категории:

- 1 категория – специальные персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

- 2 категория - биометрические персональные данные, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, за исключением персональных данных, относящихся к категории 1;

- 3 категория - общедоступные персональные данные, полученные из общедоступных источников персональных данных (в том числе справочники, адресные книги).

- 4 категория – иные персональные данные, персональные данные не указанные в 1, 2, 3 категории.

4. Хранение персональных данных

4.1 Персональные данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.2. Персональные данные, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, сейфах либо в запираемых помещениях с ограниченным правом доступа.

4.3. Персональные данные субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в ИСПД.

4.4. Не допускается хранение и размещение документов, содержащих персональные данные, в открытых электронных каталогах (файлообменниках).

4.5. Персональные данные, обрабатываемые в информационных сетях Общества, обрабатываются на серверах Общества и хранятся на дублированных жестких дисках, объединенных в рейд-массивы. Резервное копирование баз данных происходит в ежедневном режиме на внешнее дисковое хранилище.

4.6. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.7. Сроки хранения персональных данных субъектов определяются в соответствии с нормативными правовыми актами Российской Федерации, локальными нормативными актами Оператора.

4.8. Лица, обрабатывающие персональные данные, имеют доступ только к тем персональным данным, которые необходимы для выполнения конкретных трудовых функций, заданий.

5. Защита персональных данных

5.1. Обеспечение защиты персональных данных достигается:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением правовых, 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;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 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;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

5.2. Лица, отвечающие за защиту информации и обеспечение безопасности персональных данных в информационной системе персональных данных, обязаны принимать необходимые организационные и технические меры для защиты персональных данных от несанкционированного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.

5.3. Лица, отвечающие за защиту информации и обеспечение безопасности персональных данных в информационной системе персональных данных, осуществляют контроль за:

а) **управление доступом:**

идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов с ограниченного перечня терминальных устройств;

б) **регистрацию и учет:**

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и базы данных. Регистрация выхода из системы не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная – несанкционированная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа. Также подлежат регистрации действия пользователя по изменению информации в информационной системе и по обновлению структуры информационной системы.

Использование для обработки персональных данных, машинных носителей информации, не поставленных на учет, запрещается.

в) **обеспечение целостности:**

целостность средств защиты проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

проверка наличия средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности.

5.4. Работники Общества, отвечающие за информационную безопасность, обеспечивают следующие меры по защите информации:

- ограничение сетевого доступа для определенных пользователей;
- ограничение доступа к информационной системе;
- организацию работы всех компьютеров пользователей и серверов в отдельном защищенном сегменте сети;
- организацию физического ограничения несанкционированного доступа к серверному и сетевому оборудованию, средствам управления (терминальной консоли) в серверной комнате;
- организацию контроля технического состояния серверов и уровней защиты и восстановления информации;
- использование доверенных сертификатов для сетевых подключений к межсетевому экрану;
- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- контроль целостности программной и информационной части;
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- проведение регулярного копирования информации на носители как указано в пункте 4.5.;
- ведение аудита действий пользователей и своевременное обнаружение фактов несанкционированного доступа к информации;

Автоматизированная система должна быть настроена таким образом, чтобы осуществлять возможность восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней, на любую дату в течение последней недели.

5.5. На персональных компьютерах работников Общества, имеющих доступ к персональным данным обязательно наличие:

- установленного и включенного брандмауэра;
- установленного и используемого лицензированного и сертифицированного корпоративного антивирусного ПО (с обновлением баз вирусов);
- установленного обновления операционной системы.

5.6. При пользовании доступом в сеть Интернет работники Общества обязаны принимать максимальные меры по обеспечению безопасности, не открывать подозрительные веб-сайты.

5.7. Работники Общества, обрабатывающие персональные данные, получают доступ к необходимым категориям персональных данных на срок выполнения ими соответствующих должностных обязанностей.

5.8. Доступ к персональным данным третьих лиц, не являющихся работниками Общества, без согласия субъекта персональных данных, запрещен, за исключением доступа представителей государственных органов власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти.

5.9. Доступ работника Общества к персональным данным прекращается с даты прекращения трудовых отношений, либо даты изменения должностных обязанностей работника и/или исключения работника из перечня лиц, имеющих право доступа к персональным данным. В случае увольнения работника, имеющего доступ к персональным данным, все носители, содержащие персональные данные, должны быть переданы непосредственному руководителю.

5.10. Порядок обращения с носителями, содержащими персональные данные.

5.10.1. Персональные данные субъектов, обрабатываемые Оператором на бумажных и иных носителях, хранятся в подразделениях, имеющих доступ к обработке соответствующих персональных данных.

5.10.2. Работники обязаны незамедлительно сообщать непосредственному руководителю об утрате или недостаче носителей информации, содержащих персональные данные, а также о причинах и условиях возможной утечки персональных данных или о попытке посторонних лиц получить от работника персональные данные, обрабатываемые в Обществе.

5.10.3. При работе с персональными данными в Обществе запрещается передача носителей персональных данных, а также демонстрация форм, содержащих персональных данных, в том числе с экрана дисплея (монитора) персонального компьютера лицам, не имеющим соответствующего допуска.

6. Передача персональных данных

6.1. При передаче персональных данных работники Общества, имеющие доступ к персональным данным, должны соблюдать следующие требования:

6.1.1. Не сообщать персональные данные третьим лицам без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации, иными федеральными законами, нормативными актами.

Учитывая, что Трудовой кодекс РФ не определяет критерии ситуаций, представляющих угрозу жизни или здоровью работника, Оператор в каждом конкретном случае дает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных работника, либо отсутствует письменное согласие работника на предоставление его персональных сведений, либо, по мнению Оператора, отсутствует угроза жизни или здоровью работника, Оператор обязан отказать в предоставлении персональных данных лицу.

6.1.2. Предупредить лиц, получающих персональные данные, 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.

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

7. Обязанности и ответственность лиц, обрабатывающих персональные данные

7.1. Ответственные лица обязаны:

- не разглашать персональные данные субъектов персональных данных;
- в случае попытки посторонних лиц несанкционированно получить персональные данные, немедленно сообщать об этом своему непосредственному руководителю;
- не использовать доступ к персональным данным для занятий деятельностью не связанную с выполнением должностных обязанностей;
- при увольнении из Общества сдать все носители персональных данных, которые у них находились в связи с выполнением должностных обязанностей, ответственному лицу;
- немедленно сообщать непосредственному руководителю об утрате или недостаче носителей персональных данных и других фактах, которые могут привести к нарушению конфиденциальности, целостности или доступности персональных данных, а также о причинах и условиях возможной утечки персональных данных;
- использовать установленные на рабочем месте технические средства обработки персональных данных исключительно для выполнения своих обязанностей.

7.2. Ответственность лиц, допущенных к обработке персональных данных.

7.2.1. Ответственные лица, несут персональную ответственность за сохранность носителя и конфиденциальность информации, в том числе за разглашение.

7.2.2. Ответственные лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.2.3. Ответственные лица, обязаны обеспечить каждому субъекту персональных данных возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено действующим законодательством.

8. Порядок уничтожения и обезличивания персональных данных

8.1. Уничтожение или обезличивание части персональных данных на бумажном носителе может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе, которые частичному уничтожению или обезличиванию не подлежат (удаление, вымарывание);

8.2. Персональные данные на бумажных носителях уничтожаются путем сожжения, переработки в бумагоперерабатывающей машине (шредере);

8.3. Персональные данные, размещенные в памяти ПЭВМ уничтожаются путем стирания программным способом (либо с помощью форматирования) без возможности восстановления;

8.4. Персональные данные, размещенные на флеш-карте, CD-диске, ином съемном носителе информации уничтожаются путем стирания программным способом без возможности восстановления или путем разрушения носителя.

9. Заключительные положения

9.1. Настоящее положение может дополняться и изменяться по мере выполнения требований защиты персональных данных, развития способов и средств реализации системы защиты персональных данных в Обществе.

9.2. Все изменения и дополнения в настоящее положение вносятся приказом руководителя Общества или уполномоченного им лица.

9.3. Настоящее положение вступает в силу с момента его утверждения.