

ПОЛОЖЕНИЕ

о работе с персональными данными контрагентов

1. Общие положения

1.1. Настоящее положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных), Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 1 ноября 2012 г. № 1119, и иными нормативными актами в области защиты персональных данных, действующими на территории Российской Федерации.

1.2. Настоящее положение устанавливает порядок обработки персональных данных контрагентов МАУК "ГДК" 680030, Хабаровский край, г. Хабаровск, ул. Ленина, д. 85, ИНН 2721186404 (далее - учреждение), основные цели, принципы обработки и требования к безопасности персональных данных.

1.3. Настоящее положение разработано в целях регулирования порядка сбора, систематизации, хранения, передачи и уничтожения персональных данных контрагентов учреждения.

2. Понятие и состав персональных данных

2.1. В целях настоящего положения под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.2. К персональным данным контрагента относятся:

- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения и др.);
- паспортные данные;
- адрес регистрации;
- адрес места жительства;
- номер телефона;
- иные данные, предусмотренные данным Положением.

2.3. Документы, в которых содержатся персональные данные контрагентов учреждения, включают в себя: данные (п. 2.2. Положения).

2.4. Указанные сведения и документы являются конфиденциальными. Учреждение как оператор персональных данных не вправе распространять

персональные данные без согласия контрагента, если иное не предусмотрено федеральным законом.

3. Обработка персональных данных и гарантии их защиты

3.1. Под обработкой персональных данных понимается 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.

3.2. В целях обеспечения прав и свобод человека и гражданина учреждение при обработке персональных данных контрагента соблюдает следующие общие требования:

- обработка персональных данных контрагента осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, *в целях исполнения договора со своим контрагентом для ведения своей деятельности согласно законодательству Российской Федерации и Уставу учреждения;*

- при определении объема и содержания обрабатываемых персональных данных контрагента учреждение руководствуется Конституцией Российской Федерации и иными федеральными законами;

- все персональные данные контрагента следует получать у него самого. Если персональные данные контрагента возможно получить только у третьей стороны, то контрагент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Учреждение сообщает контрагенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа контрагента дать письменное согласие на их получение;

- учреждение не вправе получать и обрабатывать персональные данные контрагента о его политических, религиозных и иных убеждениях и частной жизни;

- учреждение не вправе получать и обрабатывать персональные данные контрагента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.3. Защита персональных данных контрагента от неправомерного их использования или утраты обеспечивается учреждением за счет ее средств в порядке, установленном федеральными законами и настоящим положением.

3.4. Контрагенты учреждения, при заключении договора, самостоятельно знакомятся с документами учреждения, устанавливающими порядок обработки персональных данных контрагентов, а также об их правах и обязанностях в этой области на официальном сайте учреждения <http://mayk-gdk.ru>.

Передающий оператор (Контрагент) гарантирует соблюдение им требований ст. 18 Закона № 152-ФЗ.

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

3.6. Учреждение осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Закону о персональных данных, требованиям к защите персональных данных, политике учреждения в отношении обработки персональных данных, настоящему положению.

3.7. Учреждение знакомит работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучает указанных работников.

3.8. Учреждение обеспечивает безопасность персональных данных контрагента следующими способами:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей 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.

3.9. Учреждение обрабатывает в информационных системах с использованием средств автоматизации следующие категории персональных

данных контрагента, обеспечивает их защиту с учетом определенного типа угроз безопасности и уровня защищенности персональных данных:

Цель обработки персональных данных: *защита персональных данных клиентов, контрагентов и пользователей сайта учреждения от несанкционированного доступа и разглашения.*

3.10. При 3-м уровне защищенности персональных данных учреждение:

- обеспечивает режим безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечивает сохранность носителей персональных данных;

- утверждает перечень работников, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;

- назначает должностное лицо (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

3.11. Учреждение обрабатывает без использования средств автоматизации следующие категории персональных данных контрагентов, обеспечивает их защиту, которые хранятся на бумажных носителях:

Цель обработки персональных данных: *защита персональных данных контрагентов учреждения от несанкционированного доступа и разглашения.*

3.12. Учреждение при обработке персональных данных контрагента на бумажных носителях в целях обеспечения их защиты:

- назначает должностное лицо (работника), ответственного за обработку персональных данных;

- ограничивает допуск в помещения, в которых хранятся документы, содержащие персональные данные контрагентов.

3.13. В целях обеспечения конфиденциальности документы, содержащие персональные данные контрагентов, оформляются, ведутся и хранятся только у:

- руководителя;

- бухгалтерии;

- контрактного управляющего;

- ответственного за складской учет.

3.14. Работники, допущенные к персональным данным контрагентов, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных контрагентов не допускаются.

3.15. Персональные данные контрагентов на бумажных носителях хранятся в помещении архива учреждения.

3.16. Персональные данные контрагентов в электронном виде хранятся в локальной компьютерной сети учреждения, в электронных папках и файлах в персональных компьютерах и работников (п. 3.16.), допущенных к обработке персональных данных контрагентов.

4. Передача персональных данных

4.1. При передаче персональных данных контрагента учреждение соблюдает следующие требования:

- не сообщать персональные данные контрагента третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью контрагента, а также в других случаях, установленных федеральными законами;
- не сообщать персональные данные контрагента в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные контрагента, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные контрагента, обязаны соблюдать режим секретности (конфиденциальности);
- разрешать доступ к персональным данным контрагентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные контрагентов, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья контрагентов.

4.2. Все сведения о передаче персональных данных контрагента учитываются для контроля правомерности использования данной информации лицами, ее получившими.

4.3. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия контрагента на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

4.4. Передача информации, содержащей сведения о персональных данных контрагента, по телефону, в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

4.5. Согласие на обработку персональных данных, разрешенных контрагентом для распространения, оформляется отдельно от иных согласий контрагента на обработку его персональных данных. Учреждение обеспечивает контрагенту возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных им для распространения.

4.6. В согласии на обработку персональных данных, разрешенных контрагентом для распространения, он вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных учреждением неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

4.7. Передача (распространение, предоставление, доступ) персональных данных, разрешенных контрагентом для распространения, должна быть прекращена в любое время по его требованию. Указанные в данном требовании персональные данные могут обрабатываться только учреждением.

5. Порядок уничтожения персональных данных

5.1. В случае выявления неправомерной обработки персональных данных при обращении контрагента учреждение осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому контрагенту, с момента такого обращения на период проверки.

5.2. В случае выявления неточных персональных данных при обращении контрагента учреждение осуществляет блокирование персональных данных, относящихся к этому контрагенту, с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы контрагента, или третьих лиц.

5.3. В случае подтверждения факта неточности персональных данных учреждение на основании сведений, представленных контрагентом, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

5.4. В случае выявления неправомерной обработки персональных данных, осуществляемой учреждением, учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных.

5.5. В случае если обеспечить правомерность обработки персональных данных невозможно, учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

5.6. Об устранении допущенных нарушений или об уничтожении персональных данных учреждение уведомляет контрагента.

5.7. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав контрагента, учреждение с момента выявления такого инцидента, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомляет уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав контрагента, и предполагаемой вреде, нанесенном правам контрагента, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о лице, уполномоченном учреждением на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5.8. В случае достижения цели обработки персональных данных учреждение прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий 10 рабочих дней с даты достижения цели обработки персональных данных.

5.9. В случае отзыва контрагентом согласия на обработку его персональных данных учреждение прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий 3-х рабочих дней с даты поступления указанного отзыва.

5.10. В случае обращения контрагента с требованием о прекращении обработки персональных данных учреждение в срок, не превышающий десяти рабочих дней с даты получения им соответствующего требования, прекращает их обработку, за исключением случаев, предусмотренных Законом о персональных данных.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления учреждением в адрес контрагента мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

5.11. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 5.4-5.10 настоящего положения, учреждение осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.12. Учреждение уведомляет Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав контрагентов, в порядке, утвержденном приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2022 г. № 187.

5.13. Учреждение передает в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, информацию о компьютерных инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) персональных данных, в порядке, установленном совместно федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и уполномоченным органом по защите прав субъектов персональных данных.

5.14. После истечения срока нормативного хранения документов, содержащих персональные данные контрагента, или при наступлении иных законных оснований документы подлежат уничтожению.

5.15. Учреждение для этих целей создает экспертную комиссию и проводит экспертизу ценности документов.

5.16. По результатам экспертизы документы, содержащие персональные данные контрагента и подлежащие уничтожению:

- на бумажном носителе - уничтожаются путем уничтожения: измельчения в шредере/сжигания;
- в электронном виде - стираются с информационных носителей либо физически уничтожаются сами носители, на которых хранится информация.

5.17. В случае если обработка персональных данных осуществлялась учреждением без использования средств автоматизации, документом,

подтверждающим уничтожение персональных данных контрагентов, является акт об уничтожении персональных данных.

5.18. В случае если обработка персональных данных осуществлялась учреждением с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных контрагентов, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации уничтожении персональных данных.

6. Права контрагентов в целях обеспечения защиты персональных данных

6.1. В целях обеспечения защиты персональных данных, хранящихся в учреждении, контрагенты имеют право на:

- полную информацию об их персональных данных и обработке этих данных, в том числе содержащую:
 - а. подтверждение факта обработки персональных данных учреждением; правовые основания и цели обработки персональных данных;
 - б. цели и применяемые учреждением способы обработки персональных данных;
 - в. сроки обработки персональных данных, в том числе сроки их хранения;
 - г. информацию об осуществленной или о предполагаемой трансграничной передаче данных;
 - д. информацию о способах исполнения учреждением обязанностей, установленных статьей 18.1 Закона о персональных данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные контрагента, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований Закона о персональных данных. При отказе учреждения исключить или исправить персональные данные контрагента он имеет право заявить в письменной форме учреждения о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера контрагент имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении учреждением всех лиц, которым ранее были сообщены неверные или неполные персональные данные контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия учреждения при обработке и защите персональных данных.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных контрагентов учреждения, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном федеральными законами РФ, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

7.2. Моральный вред, причиненный контрагенту вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральным законодательством, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных контрагентом убытков.

8. Заключительные положения

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

8.2. Учреждение обеспечивает неограниченный доступ контрагентов к настоящему документу.

8.3. Настоящее положение является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным контрагента, и доводится до их сведения персонально под подпись.