

Бюджетное учреждение социального обслуживания для детей-сирот и детей, оставшихся без попечения родителей, Вологодской области «Харовский центр помощи детям, оставшимся без попечения родителей»

Утверждаю:

И.о. директора  Т.С. Лукьянова
« 28 » 02 20 25 г.

ПОЛОЖЕНИЕ

о порядке обработки персональных данных контрагентов по договорам
и гарантиях их защиты

1. Общие положения

1.1. Настоящее Положение разработано в целях защиты персональных данных контрагентов по договорам (далее по тексту – контрагент) Учреждения БУ СО ВО «Харовский центр помощи детям, оставшимся без попечения родителей» (далее по тексту – Учреждение) от несанкционированного доступа.

1.2. Настоящее Положение разработано в соответствии с требованиями Конституции РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" и определяет особенности обработки персональных данных контрагентов.

1.3. Сбор персональных данных осуществляется для исполнения договорных обязательств.

1.4. Персональные данные не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;
- затруднения реализации прав и свобод граждан Российской Федерации.

1.5. Настоящее Положение утверждается директором Учреждения и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным контрагентов.

2. Основные понятия

В настоящем Положении используются следующие основные понятия:

2.1 персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год,

месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

2.2 обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

2.3 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;

2.4 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;

2.5 блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

2.6 уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

2.7 обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

2.8 информационная система персональных данных – 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;

2.9 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;

2.10 трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

2.11 общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

3. Состав персональных данных

3.1. Персональные данные контрагента – информация, необходимая Учреждению в связи с исполнением договорных обязательств и касающиеся конкретного контрагента. Под информацией о контрагенте понимаются сведения о фактах, событиях и обстоятельствах жизни контрагента, позволяющие идентифицировать его личность.

3.2. В соответствии Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", локальными нормативными актами Учреждения, контрагент, заключающий договор, предъявляет Учреждению следующие документы, содержащие его персональные данные:

- паспорт, удостоверяющий личность;
- свидетельство о государственной регистрации в налоговом органе;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учет в налоговом органе;
- банковские реквизиты (если перечисление денежных средств происходит на банковский счет).

Запрещается запрашивать другие документы при заключении договора, если иное не предусмотрено законодательством РФ.

3.3. Состав персональных данных контрагента:

- паспортные данные;
- идентификационный номер налогоплательщика;
- номер и серия страхового свидетельства;
- банковские реквизиты;
- адрес места жительства, номер контактного телефона.

3.4. Данные документы являются конфиденциальными.

4. Обработка персональных данных контрагента

4.1. Под обработкой персональных данных контрагента понимается получение, хранение, передача или любое другое использование персональных данных контрагента.

4.2. В целях обеспечения прав и свобод человека и гражданина Учреждение и его сотрудники при обработке персональных данных контрагентов обязаны соблюдать следующие общие требования:

- обработка персональных данных контрагентов может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, выполнения договорных обязательств;

- при определении объема и содержания обрабатываемых персональных данных контрагентов Учреждение должно запрашивать только ту информацию, которая потребуется для исполнения обязанностей по договору и при этом руководствоваться ГК РФ и иными федеральными законами;

- персональные данные контрагента следует получать у него самого;
- при принятии решений, затрагивающих интересы контрагента, Учреждение

не имеет права основываться на персональных данных контрагентов, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4.3. К обработке, передаче и хранению персональных данных контрагентов могут иметь доступ следующие сотрудники Учреждения:

- директор Учреждения;
- заместители директора;
- руководители структурных подразделений, непосредственно работающих с контрагентами;
- экономист, специалист по персоналу и специалист по закупкам;
- юрисконсульт;
- документовед.

4.4. Передача персональных данных контрагента возможна только с согласия контрагента или в случаях, прямо предусмотренных законодательством.

4.4.1. При передаче персональных данных контрагента Учреждение должно соблюдать следующие требования:

- не сообщать персональные данные контрагента третьей стороне без письменного согласия контрагента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью контрагента, а также в случаях, установленных федеральным законом;
- предупреждать лица, получающие 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 контрагента только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные контрагента, которые необходимы для выполнения конкретных функций.

4.5. Все меры конфиденциальности при сборе, обработке и хранении персональных данных контрагента распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

4.6. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

4.7. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

5. Права и обязанности контрагента

5.1. Контрагент обязан:

- передавать учреждению или его представителю комплекс достоверных, документированных персональных данных;
- своевременно сообщать об изменении своих персональных данных.

5.2. Контрагент имеет право:

- получения полной информации о хранении и обработке его персональных данных (в том числе автоматизированной);

- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства РФ и настоящего Положения;

- заявить в письменной форме о своем несогласии (с соответствующим обоснованием такого несогласия) в случае отказа оператора исключить или исправить персональные данные контрагента;

- требовать извещения Учреждением всех лиц, которым ранее были сообщены неверные или неполные персональные данные контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- свободного бесплатного доступа к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;

- определять своих представителей для защиты своих персональных данных;

- обжаловать в суд любые неправомерные действия или бездействие учреждения или уполномоченного им лица при обработке и защите персональных данных контрагента.

5.3. Контрагент не должен отказываться от своих прав на сохранение и защиту тайны.

6. Доступ к персональным данным контрагентов

6.1. Внутренний доступ (доступ внутри организации):

6.1.1. Право доступа к персональным данным контрагентов имеют:

- директор учреждения;
- заместители директора;
- руководители структурных подразделений, непосредственно работающих с контрагентами;

- экономист, специалист по персоналу и специалист по закупкам;

- юрисконсульт;

- документовед.

- сам контрагент, носитель данных;

- другие сотрудники Учреждения при выполнении ими своих служебных обязанностей.

6.2. Внешний доступ:

6.2.1. К числу массовых потребителей персональных данных вне Учреждения можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;

- правоохранительные органы;

- организации, принимающие и отправляющие платежи по договорам с контрагентами.

6.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

7. Защита персональных данных

7.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

7.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

7.3. Защита персональных данных представляет собой жестко регламентированный и динамически развивающийся технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Учреждения.

7.4. Защита персональных данных контрагентов от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет собственных средств в порядке, установленном федеральным законом.

7.5. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами Учреждения.

7.6. Внутренняя защита:

7.6.1. Для обеспечения внутренней защиты персональных данных контрагента необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников Учреждения, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при которых исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудником требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных (договоры содержатся в сейфах или закрывающихся шкафах);
- своевременное выявление нарушений требований разрешительной системы доступа сотрудниками Учреждения;
- воспитательная и разъяснительная работа с сотрудниками Учреждения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача персональных данных контрагентов на рабочие места руководителей.

к персональным данным контрагентов.

Директор Учреждения вправе вносить изменения и дополнения в Положение. Сотрудники Учреждения должны быть поставлены в известность о вносимых изменениях и дополнениях за 5 дней до вступления их в силу посредством издания директором приказа и ознакомления с ним всех сотрудников Учреждения.