ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«СПб центр системного анализа»

УТВЕРЖДЕНО
Приказом
от 01 февраля 2017 года № 01-04/01
Генеральный директор
_____ Н.Н. Сисина

ПОЛОЖЕНИЕ
О защите персональных данных слушателей

1. Общие положения

1.1. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления, хранения и защиты сведений, отнесенных к персональным данным слушателя ООО «СПБЦСА» (далее по тексту – Учреждение).

1.2. Целью настоящего Положения является определение порядка обработки персональных данных слушателя Учреждения, нормативное закрепление системы организационно-правовых и технических средств защиты персональных данных слушателя Учреждения от несанкционированного доступа и разглашения, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований, регулирующих получение, учет, обработку и защиту персональных данных.

1.3. Действие настоящего Положения не распространяется на отношения, возникшие при:

- организации хранения, комплектования, учета и использования содержащих персональные данные архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.4. Настоящее Положение разработано в соответствии с:

- Конституцией Российской Федерации;
- Федеральным законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных»;

- Указом Президента Российской Федерации от 06.03.1997г. № 188 (в ред. От 13.07.2015г.) «Об утверждении перечня сведений конфиденциального характера»;
- Постановлением Правительства РФ от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства РФ от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- иными нормативными правовыми актами Российской Федерации;
- Уставом Учреждения и другими локальными нормативными документами.

1.5. Основной задачей настоящего Положения является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.6. Настоящее Положение вступает в силу с момента утверждения его Генеральным директором Учреждения и действует бессрочно до замены его новым Положением.

1.7. Все изменения и дополнения в настоящее Положение действительны только в том случае, если они утверждены приказом Генерального Директора.

2. Основные понятия и определения

2.1. Под персональными данными слушателя понимается 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, а также сведения о фактах, событиях и обстоятельствах жизни слушателя, позволяющая идентифицировать его личность.

2.2. Под субъектом персональных данных в части данного Положения понимается физическое лицо - это слушатель, а также иное лицо, с кем Учреждение имеет договорные отношения по образовательной деятельности.

2.3. Оператор - юридическое или физическое лицо, организующие и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

2.4. В рамках настоящего Положения Оператором по обработке, хранению, передаче, защите персональных данных слушателей выступает Общество с ограниченной ответственностью «Институт профессионального развития».

2.5. Под обработкой персональных данных следует понимать сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных.

2.6. Конфиденциальность персональных данных - это обязательное для соблюдения ответственным лицом, получившим доступ к персональным данным слушателя Учреждения, требование не допускать их распространение без согласия слушателя или наличия иного законного основания;

2.7. Под распространением персональных данных следует понимать действия, направленные на передачу персональных данных слушателя определенному кругу лиц или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных слушателя в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным слушателя каким-либо иным способом.

2.8. Использование персональных данных - это действия (операции) с персональными данными, совершаемые специалистами Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении слушателя либо иным образом затрагивающих их права и свободы или права и свободы других лиц.

2.9. Под блокированием персональных данных принято понимать временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных слушателя Учреждения, в том числе их передачи.

2.10. Под уничтожением персональных данных следует понимать действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных слушателя Учреждения или в результате которых уничтожаются материальные носители персональных данных слушателя.

2.11. Обезличивание персональных данных - это действия, в результате которых невозможно определить принадлежность персональных данных конкретному слушателю.

2.12. Общедоступные персональные данные - это персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия слушателя или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.13. Автоматизированная обработка данных - обработка с помощью средств вычислительной техники.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных осуществляется на законной и справедливой основе.

3.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

3.3. Не допускается при обработке персональных данных объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

3.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

3.6. 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;

3.7. 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 является субъект персональных данных.

3.8. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Получение и обработка персональных данных слушателя

4.1. Обработка персональных данных слушателей осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, в связи с обучением субъекта персональных данных в Учреждения.

4.2. В состав персональных данных слушателя входят:

- Фамилия, имя, отчество;
- Дата, место рождения;
- Сведения о гражданстве;
- Паспортные данные;
- Сведения о предыдущем образовании;
- Сведения о форме обучения;
- Сведения об образовательной программе обучения;
- Сведения об основе обучения (договор);
- Сведения о движении слушателя (выписки из приказов);
- Сведения об успеваемости слушателя.

4.3. Во время прохождения слушателем обучения может возникнуть необходимость в предоставлении сведений относительно лиц, осуществляющих оплату за обучение слушателя в Учреждения.

4.4. В перечень таких сведений включаются следующие данные:

- Фамилия, имя, отчество (для контактного лица);
- Наименование организации (учреждения, предприятия) (для юридического лица);
- ИНН/КПП;
- Банковские реквизиты;
- Местонахождение в соответствии с регистрацией (ЕГРЮЛ)

4.5. При поступлении в Учреждения слушатель заполняет анкету с указанием своих персональных данных. Все графы анкеты должны быть полностью заполнены, в точном соответствии с представленными слушателем

документами, содержать полные и достоверные ответы на поставленные вопросы. Исправления, зачеркивания, прочерки и помарки при заполнении анкеты не допускаются.

4.6. Все персональные данные слушателя в хронологическом порядке формируются в его личное дело. Личное дело слушателя ведется на протяжении образовательного периода. Личному делу слушателя присваивается номер личного дела.

4.7. Личное дело слушателя после его формирования хранится в образовательном подразделении. Личное дело слушателя хранится в подразделении в течение всего периода обучения слушателя в Учреждения, по окончании обучения дело передаётся в архив.

4.8. Личное дело по запросу может быть выдано сотрудникам Учреждения, ответственным за их обработку, что фиксируется в соответствующих документах. Лицо, ответственное за хранение личного дела слушателя вправе отказать в выдаче личного дела, в случае отсутствия обоснования цели, ради которой запрашивается личное дело слушателя. Личное дело слушателя выдается под подпись на срок, не превышающий трех суток. Работник, получивший личное дело слушателя обязан вернуть его в установленные сроки.

4.9. Все персональные данные слушателя следует получать у него самого. Перед зачислением в Учреждение слушатель дает согласие на обработку представленных им персональных данных, что отражено в договоре на оказание образовательных услуг. В согласии указываются фамилия, имя, отчество слушателя, его дата и место рождения, адрес регистрации и фактического места жительства, паспортные данные, а также цели обработки его персональных данных, перечень персональных данных, на обработку которых дается согласие, перечень действий, на которые дается согласие, срок, в течение которого действует это согласие, порядок его отзыва. Учреждение предупреждает слушателя о последствиях отказа в предоставлении согласия на обработку персональных данных, а также об ответственности за их недостоверность. Согласие не требуется в том случае, если обработка персональных данных осуществляется:

- на основании федерального закона, устанавливающего его цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке;
- в целях исполнения договора;
- для статистических или научных целей при условии обязательного обезличивания персональных данных;
- для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение его согласия невозможно.

4.10. Если персональные данные слушателя возможно, получить только у третьей стороны, то слушатель должен быть уведомлен о соответствующем запросе заранее и от него должно быть получено на это письменное согласие. Учреждение должен сообщить слушателю о целях, предполагаемых источниках и способах получения персональных данных, а также о характере

подлежащих получению персональных данных и последствиях отказа слушателя дать письменное согласие на их получение.

4.11. Слушатель должен представлять Учреждению достоверные сведения о себе. Учреждение вправе сверять достоверность сведений, предоставленных слушателем, с имеющимися у него документами. При изменении своих персональных данных каждый слушатель обязан уведомить Учреждения о таких изменениях в срок, не превышающий один месяц. Представленные изменения вносятся Учреждением в информационную базу данных, личное дело слушателя.

4.12. Учреждение не имеет права получать и обрабатывать персональные данные слушателя о его политических, религиозных и иных убеждениях, частной жизни.

4.13. Учреждение не имеет права без письменного согласия слушателя передавать обрабатываемые персональные данные третьим лицам, размещать в средствах массовой информации, на сайтах глобальной сети интернет, в справочниках, брошюрах и др., за исключением случаев, предусмотренных законодательством Российской Федерации.

4.14. Учреждение не имеет права получать и обрабатывать персональные данные слушателя о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

4.15. При принятии решений, затрагивающих интересы слушателя, Учреждение не имеет права основываться на персональных данных слушателя, полученных исключительно в результате их автоматизированной обработки. Учреждение также не имеет права принимать решения, затрагивающие интересы слушателя, основываясь на персональных данных, допускающих двоякое толкование. В случае если на основании имеющихся персональных данных слушателя невозможно достоверно установить какой-либо факт, Учреждение предлагает слушателю представить письменные объяснения о причинах расхождения персональных данных.

4.16. Во всех случаях отказ от своих прав на сохранение и защиту тайны недействителен.

5. Хранение и использование персональных данных

5.1. Персональные данные слушателя хранятся на бумажном носителе, которым является его личное дело. Ответственное хранение личных дел слушателей осуществляет ответственное лицо, уполномоченное на то приказом Генерального директора. Все личные дела слушателей должны оформляться в отдельные папки, где каждый документ сшит и пронумерован. После окончания обучения все дела слушателей передаются в архив Учреждения. Личные дела слушателей хранятся в специальных шкафах, расположенных в специально отведенных помещениях, запирающихся на ключ, оборудованных системами пожаротушения и сигнализацией, доступ посторонних лиц в которые ограничен.

5.2. Персональные данные слушателя могут также храниться в электронном виде в локальной компьютерной сети. Ответственные лица, ведущие учет, обработку данных слушателей Учреждения в электронном виде, должны обеспечиваться индивидуальными паролями для доступа к указанным электронным базам данных.

5.3. Внутренний доступ к персональным данным слушателя имеют: Генеральный директор, специалисты, осуществляющие прием и зачисление слушателей в Учреждение.

5.4. Делать выписки, копии документов, содержащих персональные данные слушателя допустимо только сотрудникам, отвечающим за образовательный процесс слушателя и только с разрешения Генерального директора.

5.5. Внешний доступ к персональным данным слушателя распространяется на следующие органы государственной и исполнительной власти, причем только в части, касающейся их законных полномочий:

- Налоговые органы;
- Правоохранительные органы;
- ФСБ и прокуратура;
- Военкоматы.

5.6. Доступ третьих лиц к персональным данным слушателя, в том числе родственников допустим только с его письменного согласия.

6. Передача персональных данных

6.1. При передаче персональных данных слушателей в целях их сохранности и конфиденциальности Учреждение должен соблюдать следующие требования:

- Не сообщать персональные данные третьей стороне без письменного согласия слушателя за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья субъекта персональных данных, а также в случаях, установленных федеральным законом. В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом или настоящим Положением на получение информации, относящейся к персональным данным слушателя, Учреждение обязан отказать лицу в выдаче информации; при этом лицу, обратившемуся с запросом, письменно выдается отказ в выдаче информации, содержащей персональные данные слушателя; предупредить лиц, получающих персональные данные слушателя 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 слушателя, обязаны соблюдать конфиденциальность;
- Разрешать доступ к персональным данным, только специально уполномоченным лицам при этом указанные лица должны иметь право получить только те персональные данные, которые необходимы для выполнения конкретных функций;

– Не запрашивать информацию о состоянии здоровья слушателя, за исключением тех сведений, которые относятся к вопросу о возможности обучения слушателя по соответствующей программе.

6.2. Запрашиваемые в отношении слушателя сведения, содержащие персональные данные рассматриваются и обрабатываются только в том случае, когда они выполнены в письменном виде. Объем предоставляемых сведений по письменному запросу не должен превышать объема запрашиваемой информации.

6.3. Передача информации, содержащей сведения о персональных данных слушателя, по телефону, факсу, электронной почте без письменного согласия слушателя не допускается.

7. Права и обязанности слушателя

7.1. Слушатель имеет право:

– На полную информацию о своих персональных данных и обработке этих данных;
– На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации;
– Требовать от Учреждения уточнения, исправления своих персональных данных, их блокирования или уничтожения в случаях, если данные являются устаревшими, неполными, недостоверными, незаконно полученными, или не являются необходимыми для заявленной цели обработки;
– На защиту своих прав и законных интересов в судебном порядке.

7.2. Слушатель обязан:

– Предоставлять на обработку только достоверные персональные данные;
– Своевременно уведомлять Учреждению обо всех изменениях своих персональных данных в период своего обучения.

8. Безопасность персональных данных при их обработке с использованием технических средств

8.1. Под техническими средствами, позволяющими осуществить обработку персональных данных слушателя, понимаются средства вычислительной техники, информационновычислительные комплексы и сети, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

8.2. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к

персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий. Для этого на каждое техническое средство, содержащее персональные данные слушателя устанавливается пароль для индивидуального пользователя.

8.3. Такие технические средства при взаимодействии с глобальной сетью «Интернет» должны быть снабжены антивирусными программами, защищены брандмауэром или файрволом, снабжены системами доступа с использованием двухфакторной авторизации (например, логин и пароль)

8.4. Помещения, в которых находятся такие технические средства, должны быть оборудованы системами охранной и пожарной сигнализациями, доступ в такие помещения должен находиться под видеонаблюдением.

8.5. При обработке персональных данных в информационной системе Учреждения должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущения воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянный контроль над обеспечением уровня защищенности персональных данных;
- возможность незамедлительного восстановления уничтоженных персональных данных.

8.6. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных;
- проверку готовности средств защиты информации к использованию;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- выявление фактов несоблюдения условий хранения персональных данных на электронных носителях, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;

принятие мер по предотвращению возможно опасных последствий подобных нарушений.

9. Гарантии конфиденциальности

9.1. Информация, относящаяся к персональным данным слушателя, является служебной тайной и охраняется законом. Режим конфиденциальности персональных данных снимается в случаях обезличивания этих данных или по истечении 75-летнего срока и хранения, если иное не предусмотрено действующим законодательством Российской Федерации.

9.2. В целях обеспечения сохранности и конфиденциальности персональных данных слушателя Учреждения все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только уполномоченными специалистами.

9.3. Учреждение принимает на себя обязательство вносить необходимые изменения в персональные данные слушателя, уничтожать или блокировать соответствующие персональные данные, если эти данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

9.4. В случае выявления неправомерных действий с персональными данными Учреждение в кротчайшие сроки обязуется устранить допущенные нарушения. При невозможности устранить допущенные нарушения Учреждение обязуется уничтожить персональные данные.

9.5. В случае отзыва слушателем своих персональных данных Учреждение прекращает обработку персональных данных и уничтожает их в течение 3-х рабочих дней со дня получения такого отзыва.

10.Ответственность

10.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

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

11.Заключительные положения

11.1. Настоящее Положение вступает в силу с момента утверждения его Генеральным директором.

11.2. Настоящее Положение может быть изменено либо дополнено. Все изменения или дополнения действительны только после утверждения их Приказом Генерального директора.

11.3. Сотрудники Учреждения, на которых данное Положение распространяет свое действие, должны быть ознакомлены с ним под подпись и руководствоваться им в своей деятельности.