

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение устанавливает порядок сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения персональных данных клиентов в ООО «Юридическая компания Аксиома».

1.2. Целью данного 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.

1.3. Сбор, хранение, использование и распространение информации о частной жизни клиента без его письменного согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации.

1.4. Должностные лица (операторы), в обязанность которых входит ведение обработки персональных данных клиента, обязаны обеспечить каждому субъекту персональных данных возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.5. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

1.6. Операторы, осуществляющие обработку персональных данных клиента, а также определяющие цели и содержание обработки персональных данных, в соответствии со своими полномочиями владеющие информацией о клиентах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

1.7. Настоящее положение утверждается Генеральным директором ООО «Юридическая компания Аксиома» и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным клиентов.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные клиента - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), необходимая оператору в связи с договором оказания услуг.

2.2. Состав персональных данных клиента:

- ФИО;
- дата и место рождения;
- семейное положение;
- данные документа, удостоверяющего личность;
- адрес места жительства, регистрации;
- номер телефона;
- сведения о месте работы, должности, трудовом стаже, образовании;
- сведения о размере дохода;
- сведения о наличии/отсутствии имущества в собственности;
- и иные, которые необходимы для оказания юридических услуг.

3. ОБЯЗАННОСТИ ОПЕРАТОРА

3.1. В целях обеспечения прав и свобод человека и гражданина оператор при обработке персональных данных клиента обязан соблюдать следующие общие требования:

3.1.1. При определении объема и содержания обрабатываемых персональных данных клиента оператор должен руководствоваться Конституцией Российской Федерации, Федеральным Законом РФ «О персональных данных» и иными федеральными законами.

3.1.2. Все персональные данные клиента следует получать у него самого.

3.1.3. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральным законом;

3.1.4. Клиенты и их представители должны быть ознакомлены с документами организации, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

3.2. При сборе персональных данных организация обязана предоставить клиенту по его просьбе информацию, предусмотренную частью 4 статьи 14 Федерального закона Российской Федерации «О персональных данных».

3.3. В случае, если обязанность предоставления персональных данных установлена федеральным законодательством, оператор обязан разъяснить клиенту юридические последствия отказа предоставить свои персональные данные.

3.4. В целях устранения нарушений законодательства, допущенных при обработке персональных данных, а также уточнения, блокирования и уничтожения персональных данных, организация обязана:

3.4.1. При выявлении недостоверных персональных данных или неправомерных действий с ними по запросу клиента, его представителя, либо уполномоченного органа по защите прав субъектов персональных данных, осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

3.4.2. В случае подтверждения факта недостоверности персональных данных, на основании документов, представленных клиентом, его представителем или уполномоченным органом по защите прав субъектов персональных данных, уточнить персональные данные и снять их блокирование.

3.4.3. При выявлении неправомерных действий с персональными данными клиентов, в срок не превышающий трех рабочих дней с даты выявления, устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений - уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных, уведомить клиента или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, указанный орган.

3.4.4. При достижении 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.

3.4.5. В случае отзыва клиентом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено законодательством. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

4. ОБЯЗАННОСТИ КЛИЕНТА

4.1. Передавать организации комплект необходимый для оказания юридических услуг.

4.2. Своевременно сообщать организации об изменении своих персональных данных.

5. ПРАВА КЛИЕНТА

5.1. Клиент имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к нему, а также на ознакомление с такими персональными данными, за исключением случаев, предусмотренных пунктом

5.2. Сведения о наличии персональных данных должны быть предоставлены клиентом оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

5.3. Доступ к своим персональным данным предоставляется клиенту или его законному представителю оператором при обращении либо при получении от него соответствующего запроса. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя.

5.4. Клиент имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей: - подтверждение факта обработки персональных данных оператором, 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.

6. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных клиентов - получение, хранение, комбинирование, передача или любое другое использование персональных данных клиента.

6.2. К обработке, передаче и хранению персональных данных клиента могут иметь доступ: - руководство предприятия; - сотрудник, обеспечивающий поддержку клиентов

6.3. При передаче персональных данных клиента оператор должен соблюдать следующие требования: - не сообщать персональные данные клиента в коммерческих целях без его письменного согласия; - разрешать доступ к персональным данным клиентов только специально уполномоченным лицам.

6.4. Передача персональных данных от оператора внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.5. При передаче персональных данных клиента за пределы предприятия оператор не должен сообщать эти данные третьей стороне без письменного согласия клиента.

6.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных клиента распространяются как на бумажные, так и на электронные носители информации.

6.7. Категорически запрещается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

7. ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Внутренний доступ (доступ внутри организации).

7.1.1. Право доступа к персональным данным клиента имеют: - руководство предприятия; - сотрудник, обеспечивающий поддержку клиентов.

7.2. Внешний доступ.

7.2.1. Потребителей персональных данных вне предприятия являются государственные и негосударственные функциональные структуры:

- правоохранительные органы;
- другие уполномоченные органы.

7.2.2. Контролирующие органы имеют доступ к информации только в сфере своей компетенции.

8. СОХРАНЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. 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.

8.2. 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.

8.3. Защита персональных данных представляет собой жестко регламентированный и динамически 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 организации.

8.4. Защита персональной информации внутри предприятия

8.4.1. Для регламентации доступа персонала организации к конфиденциальным сведениям, документами и базами данных в целях исключения несанкционированного доступа третьих лиц и защиты персональных данных клиентов необходимо соблюдать: - строгое избирательное и обоснованное распределение документов и информации между работниками; - рациональное размещение рабочих мест работников, при котором исключается бесконтрольное использование защищаемой информации; - знание работником требований нормативно - методических документов по защите информации и сохранении тайны; - определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника с базами данных; - организация порядка уничтожения информации; - своевременное выявление нарушения требований разрешительной системы доступа к конфиденциальной информации; воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты и разглашению сведений при работе с конфиденциальными документами;

8.4.2. Все папки на электронных носителях, содержащие персональные данные клиентов, должны быть защищены паролем.

9. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.

9.1. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

9.2. Лица, виновные в нарушение установленного законом порядка сбора, хранения, использования или распространения информации о клиентах (персональных данных) несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законом.