|  |  |
| --- | --- |
|  | УТВЕРЖДЕНО  Приказом № 04-6/О от 18.05. 2015 г.,  Приказом №\_\_\_ от 30.06.2017г.  Генеральный директор  Д.В. Журавлев \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Положение**

**об обработке и обеспечении безопасности персональных данных при их обработке в информационных системах ООО «ИРЦ «Дубна»**

**Раздел 1. Общие положения**

**1.1.** Настоящее положение устанавливает требования к обеспечению безопасности (защите) персональных данных физических лиц (клиентов, абонентов, потребителей и т.д.) при их обработке в смешанных информационных системах, применяемых ООО «ИРЦ «Дубна» (далее Общество), а также информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных с использованием средств автоматизации.

**1.2**. Целью Положения является защита персональных данных клиентов - физических лиц от несанкционированного доступа, неправомерного их использования и утраты.

**1.3**. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случае обезличивания или по истечении сроков хранения, установленного законодательством, и их уничтожения.

**1.4**. Положение утверждается и вводится в действие приказом генерального директора и является обязательным для исполнения всеми сотрудниками Общества, имеющими доступ к персональным данным.

**1.5.** Положение разработано на основании Конституции РФ, Федерального закона от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006г. № 152–ФЗ «О защите персональных данных, Постановления Правительства РФ от 01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», [Приказа ФСТЭК России №21 от 18.02.2013г.](http://fstec.ru/component/attachments/download/562), нормативно-правовых документов федеральных органов власти, Устава Общества, и определяет порядок обработки и защиты персональных данных субъектов персональных данных-клиентов.

**1.6.** Основные термины и определения, применяемые в настоящем Положении.

**1.6.1.** **Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе:

Фамилия, имя, отчество; год, месяц и дата рождения; место рождения; сведения о составе семьи; паспортные данные; адрес места жительства; сведения об отношении к жилому помещению (наниматель, собственник); другая относящаяся информация, которая может использоваться при исполнении Обществом договорных условий с управляющими организациями (УК, ТСЖ, ТСН, ЖСК, ЖК, РСО и т.д.) и гражданами.

**1.6.2. Обработка 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.

**1.6.3. Распространение персональных данных** – распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**1.6.4. Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия (подготовки к принятию) решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других физических лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных.

**1.6.5. Оператор** – юридическое лицо, организующее и осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных: ООО «ИРЦ «Дубна» (Общество).

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

**1.6.7. Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе или в результате которых уничтожаются материальные носители персональных данных.

**1.6.8. Обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**1.6.9. Информационная система персональных данных** – информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**1.6.10. Конфиденциальность персональных данных** – обязательное соблюдение оператором или иным, получившим доступ к персональным данным, лицом требование не допускать их распространение без согласия субъекта персональных данных или без наличия иного законного основания.

Предоставление конфиденциальных сведений, содержащих персональные данные о физическом лице допускается на основании федеральных законов:

а) по запросам органов, осуществляющих оперативно-розыскную деятельность (органы внутренних дел РФ; органы федеральной службы безопасности (в том числе органы пограничной службы); федеральные органы государственной охраны; таможенные органы; органы службы внешней разведки);

б) по запросам (постановлениям) прокуратуры и следственных органов;

в) по судебным запросам (решениям, определениям, постановлениям).

Данный перечень исчерпывающий и не может быть изменен иначе, как федеральным законом.

**1.6.11. Клиенты (физические лица)** – лица, вступившие в правоотношения с Оператором в силу договоров с управляющими организациями (УК, ТСЖ, ТСН, ЖСК, ЖК, РСО и т.д.) на основании законодательства и других нормативно-правовых актов Российской Федерации в области регистрационного учета граждан РФ по месту пребывания и по месту жительства, паспортно-визового режима, а также жилищного права, как специальной отрасли гражданского права.

**1.7.** Персональные данные не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;

- создания затруднений в реализации прав и свобод граждан.

**Раздел 2. Перечень документов, в которых содержатся сведения, отнесенные законом к персональным данным.**

**2.1**. Документы, предъявляемые клиентами в отдел регистрации и учета движения населения для постановки на регистрационный учет по месту пребывания и по месту жительства и снятия с учета граждан РФ.

**2.2.** Документы, предъявляемые в отдел по расчетам жилищно-коммунальных услуг для учета движения граждан как плательщиков за потребленные жилищные и коммунальные услуги, услуги телевещания, Интернет, страхования жилья, охраны жилья (домофоны), начисления субсидий и мер социальной поддержки (льгот).

Перечень персональных данных представлен в **Приложении 1** к настоящему Положению.

**Раздел 3. Принципы обработки персональных данных.**

**3.1.** В целях обеспечения прав и свобод человека и гражданина обработка персональных данных клиентов должна осуществляться оператором на основе следующих принципов:

- законности и справедливости;

- ограничения достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

- недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- допустимость обработки только тех персональных данных, которые отвечают целям их обработки;

- соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

- обеспечение точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных.

- обеспечения принятия необходимых мер по удалению или уточнению неполных, или неточных данных.

**3.2**. Получение персональных данных может осуществляться только путем представления их самим клиентом. Субъект персональных данных является собственником своих персональных данных и самостоятельно решает вопросы передачи оператору своих персональных данных.

**3.3.** 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, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

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.

**3.4**. Оператор не имеет права получать и обрабатывать персональные данные клиента о его политических, религиозных и иных убеждениях и частной жизни. Информация о жизнедеятельности в сфере семейных, бытовых, личных отношений может быть получена и обработана только с письменного согласия субъекта персональных данных.

**3.5**. К обработке персональных данных клиента могут иметь доступ сотрудники (уполномоченные лица):

- отдела регистрации и учета движения населения;

- отдела по расчетам жилищно-коммунальных платежей, включая группу по работе с населением;

- группы информационно-методического обеспечения и сервисного обслуживания, - каждый в пределах только своих должностных обязанностей и при условии наличия в должностных инструкциях требований о соблюдении режима конфиденциальности при работе с персональными данными субъектов персональных данных. Уполномоченные лица определяются приказом по организации. Список подразделений, обрабатывающих персональные данные клиентов - физических лиц представлен в **Приложении 2**.

**3.6.** Передача персональных данных от оператора (его представителей) внешнему потребителю допускается в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине запроса таких данных.

**3.7**. Все меры конфиденциальности при обработке персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

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

**Раздел 4. Доступ к персональным данным клиента.**

**4.1.** Внутренний доступ (внутри организации).

4.1.1. Право доступа к персональным данным клиента имеют:

- руководители структурных подразделений по направлениям деятельности **(Приложение 3)**

- сотрудники структурных подразделений при выполнении ими своих служебных функций и обязанностей.

**4.2.** Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне организации относятся:

- правоохранительные органы;

- надзорно-контрольные органы (в сфере своей компетенции);

- судебные органы;

- государственные и муниципальные органы управления (только в сфере своей компетенции);

- военкоматы (только в сфере своей компетенции);

- органы статистики (только в сфере своей компетенции).

4.2.2. Персональные данные клиента могут быть представлены родственникам или членам его семьи только с письменного разрешения самого клиента. Иным лицам – только на основании нотариально заверенной доверенности (в том числе, в случае развода бывшему супругу или супруге).

**Раздел 5. Защита персональных данных.**

**5.1.** Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

**5.2.** Риск угрозы 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.

**5.3.** 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 деятельности организации – оператора.

**5.4.** Защита персональных данных субъекта персональных данных от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств, в порядке, установленном федеральными нормативно-правовыми актами.

**5.5.** Для персональных данных, обрабатываемых в информационной системе ООО «ИРЦ «Дубна» необходимо обеспечение 4-го уровня защищенности, согласно утвержденному Акту классификации ИС.

**5.6.** В соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства РФ от 01.11.2012г. №1119, [Приказа ФСТЭК России №21 от 18.02.2013г.](http://fstec.ru/component/attachments/download/562) для обеспечения указанного уровня защищенности персональных данных при их обработке в информационной системе ООО «ИРЦ «Дубна» необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение генеральным директором документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Для выполнения указанных требований в ООО «ИРЦ «Дубна» организована внутренняя и внешняя защита персональных данных.

**5.7. Внутренняя защита.**

**5.7.1**. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных. Предназначена для разграничения полномочий между руководителями и специалистами.

**5.7.2.** Для обеспечения внутренней защиты персональных данных необходимы:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

- строгое избирательное и обоснованное распределение документов и информации между работниками;

- рациональное размещение рабочих мест, при котором исключается бесконтрольное использование защищаемой информации;

- знание работниками требований нормативно-методических документов по защите информации и отнесения ее к конфиденциальной информации;

- наличие необходимых условий в помещении оператора для работы с конфиденциальными документами и базами данных;

- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

- организация порядка уничтожения информации;

- своевременное выявление нарушения требований разрешительной системы доступа работниками структурных подразделений;

- воспитательная и разъяснительная работа с сотрудниками, допущенными к работе с персональными данными по предупреждению утраты сведений при работе с конфиденциальной информацией.

**5.7.3.** Защита персональных данных на электронных носителях.

**5.8. Внешняя защита**

**5.8.1.** Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение конфиденциальными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания документа или его реквизитов и др.

**5.8.2.** Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности структурных подразделений Общества, посетители, работники других структурных подразделений.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления оформления, ведения и хранения документов и рабочих материалов. Поэтому, при приеме посетителей сотрудники должны быть бдительными и осмотрительными, не переговариваться между собой во всеуслышание, исключать возможность заглядывания в рабочую документацию и экран монитора.

**5.8.3.** Для обеспечения внешней защиты персональных данных необходимо:

- соблюдать установленный порядок приема, учета и контроля поведения посетителей;

- иметь технические средства охраны и сигнализации;

- соблюдать установленный порядок охраны территории, помещений;

- соблюдать требования к защите информации при собеседованиях, телефонных переговорах, даче интервью.

**5.9.** Все сотрудники Общества, связанные с получением, обработкой и защитой персональных данных обязаны подписать обязательство о неразглашении персональных данных клиентов – физических лиц.

**Раздел 6. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными.**

**6.1.** Персональная ответственность - одно из главных требований к организации работы системы защиты конфиденциальной информации и обязательное условие обеспечения эффективного функционирования этой системы.

**6.2.** Общество и сотрудники, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и обрабатывающие её, несут ответственность в соответствии с законодательством РФ за нарушение требуемого режима защиты, обработки и порядка использования такой информации.

**6.3.** Руководитель структурного подразделения, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за такое разрешение.

**6.4.** Каждый сотрудник Общества, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя информации и конфиденциальность его содержания.

**6.5.** Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных несут дисциплинарную, административную или уголовную ответственность в соответствии с федеральными законами РФ.

**6.6.** Лица, незаконными методами, получившие информацию, содержащую персональные данные, обязаны возместить, причиненные субъекту персональных данных, убытки, в том числе, моральный вред.

**6.7.** Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконный сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом информации, неправомерный отказ в предоставлении собранных в установленном порядке сведений персонального характера по запросу самого субъекта персональных данных или его законного представителя, установлена Уголовным Кодексом РФ.

|  |
| --- |
| **Приложение 1**  к Положению об обработке и обеспечении безопасности персональных данных при их обработке в информационных системах ООО «ИРЦ «Дубна» |

**Перечень персональных**

**данных клиентов - физических лиц**

Фамилия, имя, отчество

Информация о смене фамилии, имени, отчества

Пол,

Год, месяц, дата рождения

Место рождения

Гражданство

Данные документа, удостоверяющего личность (серия, номер, кем и когда выдан)

Место и дата регистрации по месту пребывания или месту проживания (предыдущие и настоящие)

Семейное положение (состояние в браке)

Состав семьи

Фамилия, имя, отчество родителей (при получении и замене паспорта)

Данные документа о рождении ребенка (от рождения до 14 лет)

Общая (жилая) площадь жилого помещения

Даты замены паспорта (20 лет, 45 лет)

Отношение к жилому помещению (собственник, наниматель)

Сведения об отношении совместно проживающих к нанимателю (собственнику) жилого помещения

Социальное положение (получатель мер социальной поддержки: ветеран, инвалид и т.д.)

|  |
| --- |
| **Приложение 2**  к Положению об обработке и обеспечении безопасности персональных данных при их обработке в информационных системах ООО «ИРЦ «Дубна» |

**Список подразделений,**

**обрабатывающих и обеспечивающих обработку**

**персональных данных**

**клиентов - физических лиц**

**1.** Отдел регистрации и учета движения населения.

**2.** Отдел по расчету жилищно-коммунальных платежей.

**3.** Отдел обслуживания

**4.** Группа информационно-методического обеспечения и сервисного обслуживания.

|  |
| --- |
| **Приложение 3**  к Положению об обработке и обеспечении безопасности персональных данных при их обработке в информационных системах ООО «ИРЦ «Дубна» |

**Список должностных лиц,**

**доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей**

**1**. Начальник отдела регистрации и учета движения населения

**2**. Начальник отдела по расчету жилищно-коммунальных платежей

**3**. Ведущий инженер группы информационно-методического обеспечения и сервисного обслуживания

**4.** Старший специалист отдела обслуживания