

УТВЕРЖДАЮ:

Директор ООО УК «Дом плюс»



18.04.2015г. Кисленко М.Д.

## Положение о защите персональных данных работников

«Общество с ограниченной ответственностью ООО УК «Дом плюс»

### 1. Общие положения

1.1. Настоящее положение о защите персональных данных устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников «ООО УК «Дом плюс» (далее «Организация»)

1.2. Под работниками подразумеваются лица, имеющие трудовые отношения с Организацией.

1.3. Настоящее положение о защите персональных данных является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся у работодателя, посредством планомерных действий по совершенствованию организации труда.

### 2. Понятие и состав персональных данных.

2.1. Под персональными данными сотрудников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

2.2. К персональным данным относятся:

- все биографические сведения работника;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т2) и трудовые книжки работника;
- основания к приказам по личному составу;

- дела, содержащие материалы по повышению квалификации и переподготовке работника, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии;
- и т.п.

2.3. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

2.4. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом. Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал сотрудником) или изъявил желание вступить в трудовые отношения с работодателем. Субъект персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных.

2.5. Держателем персональных данных является работодатель, которому работник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

2.6. Права и обязанности работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным работодателем. Указанные права и обязанности он может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

2.7. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

### **3. Принципы обработки персональных данных**

3.1. Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.

3.2. Получение, хранение, комбинирование, передача или любое другое использование персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работника, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.3. Все персональные данные работника получаются у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.4. Не допускается получение и обработка персональных данных работника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности.

3.5. Пакет анкетно - биографических и характеризующих материалов (далее «Личная карточка») работника формируется в «Личную карточку» после издания приказа о его приеме на работу. «Личная карточка» обязательно содержит личную карточку формы Т2, а также может содержать документы, содержащие персональные данные работника, в порядке, отражающем процесс приема на работу: заявление о приеме на работу; анкета; характеристика-рекомендация; результат медицинского обследования на предмет годности к осуществлению трудовых обязанностей; копия приказа о приеме на работу; расписка об ознакомлении с документами организации, устанавливающими порядок обработки персональных данных работников, а также об его правах и обязанностях в этой области; расписка об ознакомлении его с локальными нормативными актами организации. Все документы хранятся в файлах, файлы содержатся в папках в алфавитном порядке фамилий сотрудников. Анкета является документом «Личной карточки», представляющим собой перечень вопросов о биографических данных работника, его образовании, выполняемой работе с начала трудовой деятельности, семейном положении, месте прописки или проживания и т.п. Анкета заполняется самостоятельно при оформлении приема на работу. При заполнении анкеты работник должен заполнять все ее графы, на все вопросы давать полные ответы, не допускать исправлений или зачеркивания, прочерков, помарок, в строгом соответствии с записями, которые содержатся в его личных документах. В графе "Ближайшие родственники" перечисляются все члены семьи работника с указанием степени родства (отец, мать, муж, жена, сын, дочь, родные брат и сестра); далее перечисляются близкие родственники, проживающие совместно с сотрудником. Указываются фамилия, имя, отчество и дата рождения каждого члена семьи.

3.6. При заполнении анкеты и личной карточки Т2 используются следующие документы:

- паспорт;
- трудовая книжка;
- военный билет;
- документы об образовании.

3.7. «Личная карточка» пополняется на протяжении всей трудовой деятельности работника в данной организации. Изменения, вносимые в карточку Т2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

Сотрудник отдела кадров, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами. При обработке персональных данных работодатель в лице Генерального директора вправе определять способы обработки, документирования, хранения и защиты персональных данных работников Организации на базе современных информационных технологий.

3.8. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен ТК РФ;
- своевременно сообщать работодателю об изменении своих персональных данных.

3.9. Работник имеет право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные. Доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия.

#### **4. Доступ к персональным данным**

4.1. Персональные данные добровольно передаются работником непосредственно держателю этих данных и потребителям внутри Организации исключительно для обработки и использования в работе.

4.2.1. Внешний доступ. К числу массовых потребителей персональных данных вне Организации можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

4.2.2. Внутренний доступ. Внутри Организации к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- все сотрудники отдела кадров;
- все сотрудники бухгалтерии;
- руководители структурных подразделений.

4.3. В кадровом секторе хранятся личные карточки работников, работающих в настоящее время. Для этого используются специально оборудованные шкафы или сейфы, которые запираются. Личные карточки располагаются в алфавитном порядке. После увольнения документы по личному составу передаются на хранение.

#### **5. Передача персональных данных.**

5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

5.1.1. Передача внешнему потребителю.

- Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.
- При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы Организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника.
- Ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения руководителя и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений.
- Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.
- Сведения передаются в письменной форме и должны иметь гриф конфиденциальности.
- По возможности персональные данные обезличиваются.

5.1.2. Передача внутреннему потребителю.

- Работодатель вправе разрешать доступ к персональным данным работника только специально уполномоченным лицам, перечисленным в п.2 гл.4.
- Потребители персональных данных должны подписать обязательство о неразглашении персональных данных.

## **6. Защита персональных данных.**

6.1. 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.

6.1.1. 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.

6.2. 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 компании.

### **6.2.1. «Внутренняя защита».**

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами организации. Для защиты персональных данных работников необходимо соблюдать ряд мер:

- 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 работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работниками требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении 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;
- воспитательная и разъяснительная работа с работниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел работников на рабочие места. Личные дела могут выдаваться на рабочие места только руководителю, и в исключительных случаях, по письменному разрешению руководителя, должностному лицу;
- персональные компьютеры, на которых содержатся персональные данные, должны быть защищены паролями доступа.

### **6.2.2. «Внешняя защита».**

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 ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др. Под посторонним лицом понимается любое лицо, не имеющее непосредственного

отношения к деятельности организации, посетители, сотрудники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

6.3. Для защиты персональных данных работников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим Организации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

## 7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными.

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

7.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

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

7.4. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

С положением о защите персональных данных ознакомлены:

Директор		Киселев М.Д.
Должность	подпись	Ф.И.О.
Зам. директора		Тесник Д.З.
Должность	подпись	Ф.И.О.
гл. инженер		Галанов У.В.
Должность	подпись	Ф.И.О.
транспортист		Торбека А.
Должность	подпись	Ф.И.О.
Техник		Головнев А.И.
Должность	подпись	Ф.И.О.
инженер-электр.		Забородина
Должность	подпись	Ф.И.О.
бухгалтер		Сушанова С.В.
Должность	подпись	Ф.И.О.
с.л. - сантехник		Олег
Должность	подпись	Ф.И.О.
Должность	подпись	Ф.И.О.