

ПОЛОЖЕНИЕ

Об обработке персональных данных в ООО "ДентоГрад"

1. Общие положения

1.1. Настоящее Положение регулирует отношения, связанные с обработкой персональных данных, определяет общие правила защиты персональных данных от несанкционированного доступа, неправомерного их использования или утраты, прав (неприкосновенность частной жизни, личная и семейная тайна) физического лица - работника и/или пациента-субъекта персональных данных, а также проведение контроля за соблюдением конфиденциальности обработки персональных данных

1.2. Цель настоящего Положения – обеспечение в соответствии с законодательством Российской Федерации защиты прав и свобод сотрудников (работников) и пациентов ООО "ДентоГрад" при обработке и хранении их персональных данных, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных. Установление ответственности должностных лиц, имеющих доступ к персональным данным субъектов, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, а также Федерального закона «Об информации, информатизации и защите информации», Федерального закона "О персональных данных", Федерального закона

«Об основах охраны здоровья граждан». Данное Положение определяет:

- цели обработки персональных данных;
- перечень (состав) персональных данных;
- действия (операции), совершаемые с персональными данными;
- категории лиц, которые организуют и/или осуществляют обработку персональных данных;
- права доступа к персональным данным;
- носители для сбора персональных данных.

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение утверждается и вводится в действие приказом руководителя ООО "ДентоГрад" и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

2. Понятие и состав персональных данных

2.1. Термины и определения

Персональные данные - любая информация, относящаяся прямо или косвенно к определенному физическому лицу (субъекту персональных данных).

Субъект персональных данных – физическое лицо.

Оператор – юридическое лицо, организующее и/или осуществляющее обработку персональных данных.

Обработка персональных данных - сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (*распространение, предоставление, доступ*), *обезличивание, блокирование, удаление, уничтожение* и/или любое другое действие (операция), совершаемое с использованием средств автоматизации или без использования таких средств с персональными данными.

Обработка персональных данных с использованием средств автоматизации – обработка персональных данных с помощью информационных технологий и технических средств.

Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

Персональные данные пациента – информация необходимая для оказания медицинской помощи пациенту.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному кругу лиц.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному физическому лицу;

Блокирование персональных данных - временное прекращение обработки персональных данных.

Уничтожение персональных данных - действие, в результате которого уничтожаются все персональные данные физического лица на любых носителях, после чего становится невозможным восстановить их содержание.

Информационная система персональных данных – база персональных данных или совокупность баз, содержание и обработку которой обеспечивают информационные технологии и технические средства.

2.2. В состав персональных данных работника входят:

- фамилия, имя, отчество (в т.ч. предыдущие);
- данные о трудовом договоре (номер трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, номер и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- дата рождения, возраст и место рождения;
- паспортные данные;
- данные загранпаспорта;
- семейное положение;
- данные о составе и членах семьи - ФИО детей/супруга, количество, возраст детей;
- гражданство;
- адрес регистрации/фактического проживания, дата регистрации;
- номер контактного телефона;
- стаж работы, трудовая деятельность до приема на работу (в т.ч. на государственной службе)/по основному месту работы;
- уголовная/административная ответственности;
- идентификационный номер о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации (ИНН);
- данные страхового номера индивидуального лицевого счета (СНИЛС);

- данные обязательного медицинского полиса;
- отношение к воинской обязанности и иные сведения военного билета/приписного удостоверения;
- данные документов о профессиональном образовании, о повышении квалификации, о профессиональной переподготовке, о стажировке, о подтверждении специальных знаний;
- данные документов о присвоении ученой степени, ученого звания;
- список научных трудов и изобретений;
- сведения о награждении государственными наградами Российской Федерации, Почетной грамотой Президента Российской Федерации, об объявлении благодарности Президента Российской Федерации, присвоении почетных, воинских и специальных званий, присуждении государственных премий (если таковые имеются);
- уровень знания иностранных языков;
- реквизиты расчетного счета в банке/номер карты;
- сведения о социальных льготах;
- информация о негосударственном пенсионном обеспечении;
- данные документов об инвалидности работника и родственников;
- данные заключения медицинского осмотра;
- должность, квалификационный уровень;
- сведения о заработной плате (доходах);
- фотографии в личном деле.

2.3. В состав персональных данных пациентов входит, любая информация, относящаяся прямо или косвенно к нему, в том числе:

- фамилия, имя, отчество (последнее - при наличии);
- пол;
- дата и место рождения;
- адрес регистрации/фактического проживания;
- контактный телефон;
- адрес электронной почты;
- паспортные данные;
- номер полиса обязательного/добровольного медицинского страхования застрахованного лица (при наличии);
- данные о состоянии здоровья, заболеваниях;
- случаи обращения за медицинской помощью;
- данные о составе семьи;
- данные о проведенных оплатах;
- место работы/гражданство (по необходимости);
- идентификационный номер о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации (ИНН);
- данные диагностических исследований (в т.ч. рентгенодиагностические снимки);
- фотофиксация в процессе осуществления лечения;
- анамнез;
- диагноз;
- вид оказанной медицинской помощи;
- условия оказания медицинской помощи;
- сроки оказания медицинской помощи;
- объем оказанной медицинской помощи;
- результат обращения за медицинской помощью;

- серия и номер выданного листка нетрудоспособности (при наличии);
- сведения об оказанных медицинских услугах;
- примененные стандарты медицинской помощи.

2.4. Под персональными данными кандидатов на замещение вакантных должностей понимается:

- фамилия, имя, отчество;
- дата рождения, возраст и место рождения;
- паспортные данные;
- семейное положение;
- данные о составе семьи/количество, возраст детей;
- гражданство;
- адрес регистрации/фактического проживания;
- номер контактного телефона;
- образование;
- трудовая деятельность до приема на работу (в т.ч. на государственной службе);
- сведения о государственных/ведомственных наградах;
- данные документов о присвоении ученой степени, ученого звания;
- уголовная/административная ответственности;
- уровень знания иностранных языков (по необходимости);
- данные заключения медицинского осмотра.

2.5. Под персональными данными контрагентов понимается:

- фамилия, имя, отчество;
- дата рождения, возраст и место рождения;
- паспортные данные;
- гражданство;
- адрес регистрации/фактического проживания, дата регистрации;
- номер контактного телефона;
- идентификационный номер о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации (ИНН);
- данные страхового номера индивидуального лицевого счета (СНИЛС);
- данные документов о профессиональном образовании, о повышении квалификации, о профессиональной переподготовке, о стажировке, о подтверждении специальных знаний;
- данные документов о присвоении ученой степени, ученого звания;
- список научных трудов и изобретений;
- сведения о награждении государственными наградами Российской Федерации, Почетной грамотой Президента Российской Федерации, об объявлении благодарности Президента Российской Федерации, присвоении почетных, воинских и специальных званий, присуждении государственных премий (если таковые имеются);
- реквизиты расчетного счета в банке/номер карты;
- сведения о социальных льготах;
- данные заключения медицинского осмотра.

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

3. Обработка персональных данных

3.1. Организация является оператором осуществляющий обработку персональных данных физических лиц с использованием средств автоматизации, в том числе информационных систем и/или без использования средств автоматизации.

3.2. Целью обработки персональных данных является выполнение возложенных на организацию функций, полномочий и обязанностей:

3.2.1. Обработка персональных данных субъекта может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

3.2.2. При определении объема и содержания обрабатываемых персональных данных работника, пациента ООО "ДентоГрад" должно руководствоваться Конституцией Российской Федерации, Трудовым Кодексом, Федеральным законом «Об основах охраны здоровья граждан» и иными федеральными законами.

3.2.3. Информация о персональных данных субъекта предоставляется оператору субъектом устно, либо путем заполнения личных карточек формы Т-2 для работников, медицинских карт для пациентов, которые хранятся в личном деле в отделе кадров, регистратуре/архиве. Персональные данные работника, пациента следует получать у него самого. Если персональные данные работника или пациента возможно получить только у третьей стороны, то работник/пациент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. ООО "ДентоГрад" должно сообщить работнику/пациенту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника/ пациента дать письменное согласие на их получение.

3.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника, пациента о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника, пациента (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны ООО "ДентоГрад" только с их письменного согласия.

3.2.6. ООО "ДентоГрад" не имеет право получать и обрабатывать персональные данные работника, пациента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:

- бухгалтерии;
- отдела кадров;
- регистратуры.

К обработке, передаче и хранению персональных данных пациента могут иметь доступ сотрудники:

- бухгалтерии;
- отдела кадров;
- регистратуры.

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.4.1. 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.

3.5. Передача персональных данных работника, пациента возможна только с согласия работника, пациента или в случаях, прямо предусмотренных законодательством.

3.5.1. При передаче персональных данных работника или пациента ООО "ДентоГрад" должно соблюдать следующие требования:

- не сообщать персональные данные работника, пациента третьей стороне без письменного согласия работника, пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, пациента, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника, пациента в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, пациента 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, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников, пациентов в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным работников, пациентов только специально уполномоченным лицам, определенным в Положении о разграничении прав доступа к персональным данным, при этом указанные лица должны иметь право получать только те персональные данные работника, пациента которые необходимы для выполнения конкретных функций;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.5.2. 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.

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

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

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

3.9. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

4. Доступ к персональным данным

4.1. Внутренний доступ.

4.1.1. Право доступа к персональным данным имеют:

- сам субъект персональных данных;
- другие сотрудники организации при выполнении ими своих служебных обязанностей.

4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, пациентов определен в Положении о разграничении прав доступа к персональным данным.

4.2. Внешний доступ.

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

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые компании/фонд ОМС;
- военкоматы;
- органы социального страхования;

- пенсионные фонды.

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

4.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника, пациента только в случае его письменного разрешения.

4.2.4. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

Персональные данные пациента могут быть предоставлены родственникам или членам его семьи только на основании норм российского законодательства (ФЗ «Об охране здоровья граждан»)

5. Защита персональных данных

5.1. 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.

5.2. 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.

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 и производственной деятельности компании.

5.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

5.5. Защита от внутренних нарушителей.

5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

5.5.2. Для обеспечения внутренней защиты персональных данных 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 работником 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 работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

5.5.3. Защита персональных данных сотрудника на электронных носителях.

Защита персональных данных сотрудника на электронных носителях осуществляется в соответствии с Инструкцией по обеспечению безопасности рабочих мест обработки персональных данных.

5.6. Защита от внешних нарушителей.

5.6.1. 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 ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности ООО "ДентоГрад", посетители, работники 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.

5.6.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- соблюдение порядка приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- использование технических средства охраны и сигнализации;
- использование технических средств защиты информации;
- соблюдение порядка охраны территории, зданий, помещений, транспортных средств;
- выполнения требований по защите информации при интервьюировании и беседах.

6. Права и обязанности работника

6.1. Все работники должны быть ознакомлены с настоящим Положением под роспись.

6.2. В целях защиты персональных данных, хранящихся в ООО "ДентоГрад", работник имеет право:

- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

6.3. Работник, пациент обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.
- своевременно сообщать ООО "ДентоГрад" об изменении своих персональных данных.
- соблюдать конфиденциальность персональных данных других работников и пациентов, ставших ему известными во время исполнения своих должностных обязанностей.

6.4. Работники, пациенты ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке/медицинской книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового учёного звания и пр.

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. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

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

7.4. Каждый сотрудник ООО "ДентоГрад", получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

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

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит обработка персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.