**Приложение №7 к Приказу от 24.10.2019г.**
**№04**

УТВЕРЖДАЮ
Генеральный директор
ООО "Пигато"
_____ Пирогов И.Е.

# ПОЛОЖЕНИЕ «О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕ С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ПИГАТО»

## 1. Общие положения

1.1. Настоящее Положение определяет состав персональных данных, порядок получения, учета, обработки, накопления и хранения документов и других носителей, содержащих сведения, отнесенные к персональным данным передаваемых в Общество с ограниченной ответственностью «Пигато» (далее — «Компания») для выполнения последним договорных отношений, гарантии конфиденциальности сведений, предоставленных третьей стороной Компании.

1.2. Цель разработки настоящего Положения — определение порядка обработки полученных персональных данных, их защита от несанкционированного доступа, неправомерного использования, разглашения или утраты.

1.3. Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускаются. Персональные данные требуют безопасной обработки.

1.4. Режим безопасной обработки персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.5. Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.6. 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.

1.7. 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.

1.8. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании статей 14 и 15 Федерального закона и законодательства о персональных данных.

1.9. Настоящее положение является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

**2. Понятие и состав персональных данных.**

2.1. Персональные данные — информация о физических лицах (далее – субъекты персональных данных), необходимая Компании в связи с исполнением трудовых и прочих договорных отношений и касающаяся конкретного гражданина.

2.2. Состав Персональных данных:

— анкетные и биографические данные;

— образование;

— сведения о трудовом и общем стаже;

— сведения о доходах и вознаграждениях;

— сведения о составе семьи;

— паспортные данные;

— сведения о воинском учете;

— сведения о заработной плате сотрудника;

— сведения о социальных льготах;

— специальность;

— занимаемая должность;

— наличие судимостей;

— адрес места жительства;

— домашний или мобильный телефон;

— место работы или учебы членов семьи и родственников;

— характер взаимоотношений в семье;

— 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 и трудовые книжки сотрудников;

— основания к приказам по личному составу;

— дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;

— копии отчетов, направляемые в органы статистики.

**3. Обязанности Компании**

В целях обеспечения прав и свобод человека и гражданина организация и её представители при обработке персональных данных обязаны соблюдать следующие общие требования:

— обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов;

— при определении объема и содержания обрабатываемых персональных данных организация должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами;

— все персональные данные следует получать у субъекта персональных данных. Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Необходимо сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение;

— организация не имеет права получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, организация вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

— при принятии решений, затрагивающих интересы субъекта, организация не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения;

— защита персональных данных субъекта от неправомерного их использования или утраты должна быть обеспечена организацией за счет его средств в порядке, установленном федеральным законом;

— работники и их представители должны быть ознакомлены под расписку с документами Компании, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

— субъекты не должны отказываться от своих прав на сохранение и защиту тайны.

**4. Обязанности работников Компании**

Работники Компании обязаны:

— передавать Компании или её представителю комплекс достоверных документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

— своевременно сообщать Компании об изменении своих персональных данных.

— соблюдать все требования Компании по защите персональных данных.

**5. Права субъекта персональных данных.**

Субъект персональных данных имеем 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. Сбор, обработка и хранение персональных данных**

6.1. Обработка персональных данных субъекта — получение, хранение, комбинирование, передача или любое другое использование персональных данных субъекта.

6.2. Порядок получения персональных данных.

6.2.1. Все персональные данные субъекта следует получать у него самого. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть письменное согласие. Организация должна сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

6.2.2. Компания не имеет права получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной

жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ, Компания вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

6.2.3. Обработка, передача и хранение персональных данных субъекта.

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

а) Генеральный Директор Компании;

б) сотрудники отдела кадров Компании;

в) сотрудники юридического отдела Компании;

г) сотрудники ИТ-служб Компании при выполнении своих должностных обязанностей;

д) сотрудники бухгалтерии Компании.

6.2.4. При передаче персональных данных субъекта организация должны соблюдать следующие требования:

— не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральными законами;

— не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

— предупредить лиц, получающих персональные данные субъекта 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 субъекта, обязаны соблюдать режим безопасности. Данное положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами;

— разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций;

— не запрашивать информацию о состоянии здоровья субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения субъектом трудовой функции;

— передавать персональные данные субъекта представителям субъектов в порядке, установленном законом, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций.

6.2.5. Передача персональных данных от субъекта или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.2.6. При передаче персональных данных субъекта потребителям (в том числе и в коммерческих целях) за пределы Компании, Компания не должна сообщать эти данные третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта или в случаях, установленных федеральными Законами.

6.2.7. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта распространяется как на бумажные, так и электронные (автоматизированные) носители информации.

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

6.2.9. По возможности персональные данные обезличиваются.

**7. Доступ к персональным данным.**

7.1. Внутренний доступ (доступ внутри Компании)

Право доступа к персональным данным имеют:

а) Генеральный Директор Компании;

б) сотрудники отдела кадров Компании;

в) сотрудники юридического отдела Компании;

г) сотрудники ИТ-служб Компании при выполнении своих должностных обязанностей;

д) сотрудники бухгалтерии Компании.

7.2. Внешний доступ.

7.2.1. К числу массовых потребителей персональных данных вне Компании 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;

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

7.2.3. Субъект, его родственники и члены семей.

Персональные данные субъекта могут быть предоставлены самому субъекту или с его письменного разрешения его родственникам или членам его семьи.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия, (УК РФ).

7.2.4. Защита персональных данных

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.

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.

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.

7.2.4.1. «Внутренняя зашита».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных Регламентация доступа персонала к документам и базам данных с персональными сведениями входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами компании. Для защиты персональных данных субъектов 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 документами и базами данных с персональными сведениями;

— 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 предупреждение утраты ценных сведений при работе с документами, содержащими персональные данные;

— все файлы, папки, базы данных и т.п. содержащие персональные данные, должны быть защищены паролем, который сообщается сотрудникам наделенным соответствующим приказом правом на обработку персональных данных.

7.2.4.2. «Внешняя защита».

Для защиты персональных данных 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 компании, посетители, работники других организационных структур,

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел, рабочих материалов и баз данных в отделах обрабатывающих персональные данные.

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

— порядок приема, учета и контроля деятельности посетителей;

— пропускной режим компании;

— учет и порядок выдачи удостоверений;

— технические средства охраны, сигнализации;

— порядок охраны территории, зданий, помещений, транспортных средств;

— требования к защите информации при интервьюировании и собеседованиях.

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.

Все лица, связанные с получением, обработкой и защитой персональных данных обязаны заключить «Соглашение о неразглашении персональных данных».

**8. 0ответственость за разглашение персональных данных, информации связанной с персональными данными.**

8.1. Персональная ответственность — одно из главных требований к Компании функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

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

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

8.4. Лица, виновные в нарушении установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) несут дисциплинарную, административную, гражданско—правовую или уголовную ответственность в соответствии с федеральными законами

Приложение 1.

**Пример соглашение о неразглашении Персональных данных**

Я, _____,
паспорт серия _____, номер _____,
выданный _____

«_____»_____ _____года, понимаю, что получаю доступ к персональным данным физических лиц, обрабатываемым в ООО «Пигато». Я также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъекту персональных данных как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сбором, обработкой и хранением) с персональными данными субъекта персональных данных соблюдать все описанные в «Положении о персональных данных в обществе с ограниченной ответственностью «Пигато»»

Я подтверждаю, что не имею права разглашать сведения:

1) анкетные и биографические данные;

2) образование;

3) сведения о трудовом и общем стаже;

4) сведения о доходах и вознаграждениях;

5) сведения о составе семьи;

6) паспортные данные;

7) сведения о воинском учете;

8) сведения о заработной плате;

9) сведения о социальных льготах;

10) специальность,

11) занимаемая должность;

12) наличие судимостей;

13) адрес места жительства;

14) домашний или мобильный телефон;

15) место работы или учебы членов семьи и родственников;

16) характер взаимоотношений в семье;

17) содержание трудового договора;

18) состав декларируемых сведений о наличии материальных ценностей;

19) содержание декларации, подаваемой в налоговую инспекцию;

20) подлинники и копии приказов по личному составу;

21) личные дела и трудовые книжки сотрудников;

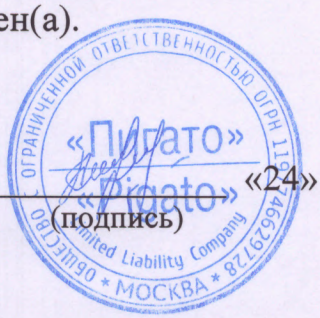
22) основания к приказам по личному составу;

23) дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;

24) копии отчетов, направляемые в органы статистики.

Я предупрежден(-а) о том, что в случае разглашения мной сведений, касающихся персональных данных субъекта персональных данных или их утраты, я несу ответственность в соответствии с федеральным законодательством.

С «Положении о персональных данных в обществе с ограниченной ответственностью «Пигато»» ознакомлен(а).




Генеральный директор Пирогов И.Е. _____ «24» октября 2019г.
(должность) (ФИО) (подпись) (дата)