ПРИЛОЖЕНИЕ № 6

Утверждаю :
Директор ООО «Центр Лидер»
Ибрагимов М.У.

«09» января 2017 года

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ООО «ЦЕНТР ЛИДЕР»

1. Общие положения

1.1. Цель данного Положения - защита в ООО «Центр Лидер» (далее – Общество) персональных данных от несанкционированного доступа.

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

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

1.4. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому 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. 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.

1.7. 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.

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

2. Понятие и состав персональных данных.

2.1. Персональные данные – информация о физических лицах (далее – субъекты), необходимая Обществу 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

3.1. В целях обеспечения прав и свобод человека и гражданина Общество и его представители при обработке персональных данных обязаны соблюдать следующие общие требования:

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

3.1.2. При определении объема и содержания обрабатываемых персональных данных Общество должно руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами;

3.1.3. 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;

3.1.4. Общество 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, Общество вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

3.1.5. При принятии решений, затрагивающих интересы Субъекта, Общество не имеет права основываться на персональных данных Субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения;

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

3.1.7. Работники и их представители должны быть ознакомлены под расписку с документами Общества, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

3.1.8. Субъекты не должны отказываться от своих прав на сохранение и защиту тайны.

4. Обязанности работников Общества

4.1. Передавать Обществу или его представителю комплекс достоверных документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

4.2. Своевременно сообщать Обществу об изменении своих персональных данных.

4.3. Соблюдать все требования Общества по защите персональных данных.

5. Права Субъекта персональных данных

5.1. Требовать исключения или исправления неверных или неполных персональных данных;

5.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

5.3. Персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

5.4. Определять своих представителей для защиты своих персональных данных;

5.5. 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 получено письменное согласие. Общество должно 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. Общество 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, Общество вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

6.3. Обработка, передача и хранение персональных данных Субъекта.

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

- директор Общества;
- главный бухгалтер;
- администратор.

6.4. При передаче персональных данных Субъекта Общество должно 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 федеральным законом;
- 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 Субъекта 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.

6.5. 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.

6.6. При передаче персональных данных Субъекта потребителям (в том числе и в коммерческих целях) за пределы Общества, Общество не должно 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 федеральным законом.

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

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

6.9. По возможности персональные данные обезличиваются.

7. Доступ к персональным данным

7.1. Внутренний доступ (доступ внутри Общества).

Право доступа к персональным данным имеют:

- директор Общества;
- главный бухгалтер;
- администратор;
- любой работник, в отношении своих персональных данных.

7.2. Внешний доступ.

7.2.1. К числу массовых потребителей персональных данных вне Общества 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. Компании, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные Компании, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

7.2.4. Другие Компании.

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

7.2.5. 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).

8. 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.

8.1. «Внутренняя защита».

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 предупреждению утраты ценных сведений при работе с документами, содержащими персональные данные;
- не допускается выдача личных дел сотрудников на рабочие места руководителей.

Личные дела могут выдаваться на рабочие места только руководителю Общества и главному бухгалтеру.

8.1.1. Защита персональных данных на электронных носителях.

- Все папки, содержащие персональные данные, должны быть защищены паролем, который сообщается руководителю Общества.

8.2. «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 Общества, 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.

8.2.1. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

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

8.2.2. 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.

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

9.Ответственность за разглашение персональных данных, связанной с персональными данными.

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

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

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

9.4.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 федеральным законом.

Приложение 1.

Пример соглашение о неразглашении
Персональных данных

Я, _____, паспорт серии _____, номер _____, выданный _____ «____» _____ _____ года, понимаю, что получаю доступ к персональным данным физических лиц, обрабатываемым в ООО «Наша компания». Я также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором, обработкой и хранением персональных данных сотрудников.

Я понимаю, что разглашение такого рода информации может нанести ущерб сотрудникам Компании как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сбором, обработкой и хранением) с персональными данными сотрудника соблюдать все описанные в «Положении о защите персональных данных» требования.

Я подтверждаю, что не имею права разглашать сведения:

- 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.

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

С «Положением о защите персональных данных сотрудника» ознакомлен(-а).

_____ _____ _____ “ ” _____20__ г.

(должность) (ФИО) (подпись)