

УТВЕРЖДАЮ
директор ООО «СолоКом»
Гуртуев В. Ю.
01 августа 2015 г.

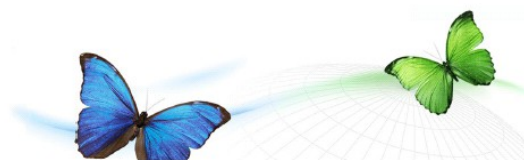
ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО «СолоКом»

1. Общие положения

- 1.1 Цель данного Положения - защита в ООО «СолоКом» (далее – организация) 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 сотрудников и контрагентов, 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 сотрудников и клиентов.

2. Понятие и состав персональных данных

- 2.1 Персональные данные – информация о физических лицах (далее – субъекты), необходимая организации в связи с исполнением трудовых и договорных отношений и касающаяся конкретного гражданина.
- 2.2 Состав Персональных данных сотрудников организации:
 - фамилия, имя, отчество;
 - дата рождения;
 - паспортные данные;
 - адрес регистрации;
 - образование;
 - сведения о трудовом и общем стаже;
 - сведения о доходах и вознаграждениях;
 - сведения о составе семьи;
 - сведения о воинском учете;
 - сведения о заработной плате сотрудника;



- сведения о социальных льготах;
- специальность,
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний и мобильный телефоны;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в ИФНС РФ;
- 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;
- подлинники и копии отчетов, направляемые в органы статистики;
- подлинники и копии отчетов, направляемые в Пенсионный фонд РФ.

2.3 Состав Персональных данных контрагентов организации:

- фамилия, имя, отчество;
- дата рождения;
- паспортные данные;
- адрес регистрации;
- адрес оказания услуги;
- домашний и мобильный телефоны;
- содержание заявления о заключении договора;
- содержание договора об оказании услуг, приложений и дополнительных соглашений к нему;
- содержание заявления о расторжении договора;
- содержание переписки между контрагентом и организацией, возникшей в период действия договора, в т. ч. запросов, претензий, информационных писем;
- физический адрес абонентского устройства;
- IP-адрес абонентского устройства;
- имя пользователя, пароль для доступа к услуге;
- тарифный план, по которому ведется оказание услуги;
- состояние лицевого счета.

3. Обязанности организации

3.1. В целях обеспечения прав и свобод человека и гражданина организация и её 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, а также обеспечения договорных обязательств по трудовым договорам и договорам об оказании услуг.

3.1.2. При определении объема и содержания обрабатываемых персональных данных организация руководствуется Конституцией Российской Федерации, Трудовым Кодексом, Федеральным законом «О связи», Федеральным законом «О персональных данных» 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. 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.

3.1.5. 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.

3.1.6. Защита персональных данных субъекта от неправомерного их использования или утраты должна быть обеспечена организацией за счет ее средств в порядке, установленном федеральным законом.

3.1.7. Работники и их представители должны быть ознакомлены под расписку с документами

организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

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

4. Обязанности работников и контрагентов организации

4.1 Обязанности сотрудников организации:

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

4.1.2 своевременно сообщать организации об изменении своих персональных данных;

4.1.3 соблюдать все требования организации по защите персональных данных.

4.2 Обязанности контрагентов организации:

4.2.1 передавать организации или её представителю комплекс достоверных документированных персональных данных, состав которых установлен договором об оказании услуг, Федеральным законом «О связи», Правилами оказания телематических услуг связи, Правилами оказания услуг связи по передаче данных, иными нормативно-правовыми актами, регулирующими заключение, исполнение и расторжение договоров между контрагентами и организацией;

4.2.2 своевременно сообщать организации об изменении своих персональных данных

5 Права субъекта персональных данных

5.1 Требовать исключения или исправления неверных или неполных персональных данных.

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

5.3 Определять своих представителей для защиты своих персональных данных.

5.4 Право на сохранение и защиту своей личной и семейной тайны.

5.5 Право на сохранение и защиту тайны связи.

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. 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 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 РФ, Организация вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

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

- бухгалтеры;
- сотрудники отдела продаж;
- сотрудники отдела клиентского обслуживания;
- сотрудники юридического отдела;
- сотрудники технического отдела.

6.4 При передаче персональных данных субъекта организация должна соблюдать следующие требования:

6.4.1 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 законодательством;

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

6.4.3 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;

6.4.4 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;

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

6.4.6 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 организации, организация 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 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.

6.10 При обработке персональных данных с использованием баз данных организация обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

7. Доступ к персональным данным

7.1 Внутренний доступ (доступ внутри организации).

Право доступа к персональным данным имеют:

- руководитель организации;
- руководители и специалисты структурных подразделений по направлению деятельности;
- при переводе из одного структурного подразделения в другое доступ к персональным данным сотрудника может иметь руководитель нового подразделения;
- любой работник, в отношении своих персональных данных.

7.2 Внешний доступ.

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

- органы ИФНС РФ;
- 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 персональным данным только в сфере своей компетенции.

7.2.3 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 только в случае его письменного согласия.

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

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

8. Защита персональных данных

8.1 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.

8.2 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.

8.3 Защита персональных данных представляет собой жестко регламентированный и динамический 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 организации.

8.4 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 исключается 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 и непосредственного доступа к рабочим местам, на которых происходит обработка персональных данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделений;
- воспитательная и разъяснительная работа с сотрудниками подразделений по предупреждению утраты ценных сведений при работе с документами, содержащими персональные данные.

8.5 Все компьютеры, содержащие на своих жестких дисках персональные данные, должны быть защищены паролем на вход в систему, который сообщается руководителю организации.

8.6 Для защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для постороннего лица, пытающегося совершить несанкционированный доступ и овладение информацией. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности организации, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения договоров с контрагентами, личных дел сотрудников и других документов, содержащих персональные данные субъектов.

8.7 Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- соблюдение порядка приема посетителей;
- технические средства охраны, сигнализации;
- соблюдение порядка охраны территории, зданий, помещений, транспортных средств.

8.8 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.

8.9 Все сотрудники организации, связанные с получением, обработкой и защитой персональных данных сотрудников и/или контрагентов организации обязаны заключить Соглашение о неразглашении персональных данных и/или контрагентов организации.

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

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

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

9.3 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.