

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ООО «ПР-ЛИЗИНГ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение устанавливает порядок сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения персональных данных сотрудников, бывших сотрудников, претендентов на работу, клиентов, контрагентов и т.д. ООО «ПР-Лизинг» (далее – «Общество»).

1.2. Целью данного Положения является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации.

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

1.5. Должностные лица (Операторы), в обязанность которых входит ведение персональных данных сотрудников, претендентов на работу, клиентов, контрагентов обязаны обеспечить каждому Субъекту персональных данных 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. Операторы, осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных, 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 Российской Федерации «О персональных данных».

1.9. Положение утверждается директором Общества и является обязательным для исполнения всеми Сотрудниками, имеющими доступ к персональным данным Субъектов персональных данных.

2. НОРМАТИВНЫЕ ССЫЛКИ

- Конституция РФ
- «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных"
- письмо Минфина России от 10.04.2009 № 03-02-07/1-177,
- письмо Минфина России от 06.07.2009 № 03-02-07/1-340,
- письмо Минфина России от 31.12.2008 № 03-02-07/2-231;
- письмо ФНС России от 11.02.2010 № 3-7-07/84;
- Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»
- приказ Росфинмониторинга от 17.02.2011 № 59 «Об утверждении Положения о требованиях к идентификации клиентов, представителей клиентов и (или) выгодоприобретателей, в том числе с учетом степени (уровня) риска совершения клиентом операций в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма».
- Федеральный закон от 29.07.2004 № 98-ФЗ "О коммерческой тайне"
- Постановление Правительства от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- Постановление Правительства от 1.11.2012 № 119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Персональные данные – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу – субъекту персональных данных.

Персональные данные сотрудника – это любая информация, касающаяся конкретного сотрудника и его деловых (профессиональных и личностных) качеств, обрабатываемая работодателем в связи с осуществлением трудовой функции сотрудника в установленных законодательством целях, в отношении которой работодателем принимаются меры защиты, и устанавливается соответствующий правовой режим.

Субъект персональных данных – это физическое лицо, персональные данные которого обрабатываются Обществом в связи с осуществлением его деятельности (сотрудники, бывшие сотрудники, претенденты на работу, клиенты, должностные лица контрагентов и т.д.) (далее – «Субъект»)

Сотрудник – это физическое лицо, имеющее трудовые отношения с Обществом.

Оператор – должностное лицо Общества, в обязанность которого входит ведение персональных данных Субъектов персональных данных.

Контрагент – индивидуальные предприниматели и юридические лица, связанные с Обществом обязательствами по договору, сотрудничающие в процессе выполнения договора.

Посторонние лица - любые лица, не имеющие непосредственного отношения к деятельности компании, посетители.

Обезличивание персональных данных – это действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – это любые действия с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, распространение, передачу, обезличивание, блокирование, комбинирование, уничтожение персональных данных.

Неавтоматизированная обработка персональных данных – это действия по использованию, уточнению (обновлению, изменению), распространению или уничтожению персональных данных, осуществляемые при непосредственном участии человека в отношении каждого Субъекта персональных данных.

Автоматизированная обработка персональных данных – это обработка, включающая в себя операции, осуществляемые полностью или частично с помощью автоматизированных средств, а именно: хранение данных, осуществление логических и (или) арифметических операций с персональными данными, их изменение, уничтожение, поиск или распространение.

4. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Состав персональных данных Субъекта:

- анкетные и биографические данные;
- образование;
- сведения о трудовом стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес прописки и места жительства;
- домашний 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;
- личное дело и трудовая книжка;
- основания к приказам по личному составу;
- материалы по повышению квалификации и переподготовке;
- характеристики, аттестации и материалы к служебным расследованиям;
- отчеты, направляемые в органы статистики.

5. ОБЯЗАННОСТИ ОБЩЕСТВА

5.1. Обработка персональных данных Субъекта – получение, хранение, комбинирование, передача или любое другое использование персональных данных Субъекта. При обработке персональных данных Субъекта Общество и его представители (Операторы) обязаны соблюдать следующие общие требования:

5.1.1. При определении объема и содержания обрабатываемых персональных данных Субъекта Общество должно руководствоваться Конституцией Российской Федерации, Трудовым Кодексом РФ, Федеральным Законом РФ ФЗ - № 152 от 27 июля 2006 г «О персональных данных» и иными федеральными законами;

5.1.2. Общество не имеет права обрабатывать персональные данные Субъекта, касающиеся его политических, религиозных и иных убеждений и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации Общество вправе обрабатывать данные о частной жизни Субъекта только с его письменного согласия;

5.1.3. Общество не имеет право обрабатывать персональные данные Субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

5.1.4. Общество не имеет право запрашивать информацию о состоянии здоровья Субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения Субъектом трудовой функции;

5.1.5. Субъекты персональных данных и их представители должны быть ознакомлены под роспись с документами Общества, устанавливающими порядок обработки персональных данных Сотрудников, а также об их правах и обязанностях в этой области;

5.1.6. При сборе персональных данных Общество обязано предоставить Субъекту по его просьбе информацию, предусмотренную частью 4 статьи 14 Федерального закона Российской Федерации «О персональных данных» (ФЗ-№152 от 27 июля 2006 г.).

5.1.7. Оператор обязан разъяснить Субъекту юридические последствия отказа предоставить свои персональные данные.

5.2. Порядок получения персональных данных

5.2.1. 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 также о характере подлежащих получению персональных данных и последствиях отказа Субъекта дать письменное согласие на их получение;

5.2.2. 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;

5.3. Использование и передача персональных данных

5.3.1. Внутренний доступ (доступ внутри Общества).

Доступ к персональным данным Субъекта могут иметь:

- руководство Общества;
- сотрудники службы управления персоналом;
- сотрудники бухгалтерии;
- руководство структурного подразделения;
- руководство профсоюзной организации;
- сотрудники службы собственной безопасности Общества

5.3.2. Внешний доступ.

5.3.2.1. Потребителями персональных данных вне Общества являются государственные и негосударственные функциональные структуры:

- инспекции ФНС;
- правоохранительные органы;
- органы статистики;
- страховые компании;
- военные комиссариаты;
- органы социального страхования;
- пенсионные фонды в т.ч. негосударственные;
- банки;
- подразделения муниципальных органов управления;

5.3.2.2. Указанные в п. 5.3.2.1. организации имеют доступ к информации только в сфере своей компетенции.

5.3.2.3. Иные организации, в которые Субъект может осуществлять перечисления денежных средств (благотворительные организации, микрофинансовые организации и пр.), могут получить доступ к персональным данным Субъекта только в случае его письменного разрешения.

5.3.2.4. Иные организации могут получить сведения о Субъекте только с письменного согласия Субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта, а также в других случаях, предусмотренных ТК РФ или иными федеральными законами.

5.4. Защита и сохранение конфиденциальности персональных данных

5.4.1. 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 Общества.

5.4.2. Защита персональной информации внутри Общества:

5.4.2.1. Для регламентации доступа Сотрудников Общества к конфиденциальным сведениям, документам и базам данных, в целях исключения несанкционированного доступа третьих лиц и защиты персональных данных Субъектов необходимо соблюдать:

- ограничение и регламентацию состава Сотрудников, имеющих доступ к персональным данным, указанных в п. 5.3.1;
- строгое избирательное и обоснованное распределение документов и информации внутри Общества;
- рациональное размещение рабочих мест Сотрудников, при котором исключается бесконтрольное использование защищаемой информации;
- знание Сотрудниками требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа к конфиденциальной информации;

- воспитательная и разъяснительная работа с Сотрудниками по предупреждению утраты и разглашению сведений при работе с конфиденциальными документами;
- 5.4.2.2. Для защиты персональных данных Субъектов должны соблюдаться:
- порядок приема, учета и контроля деятельности посетителей;
 - пропускной режим Общества;
 - учет и порядок выдачи удостоверений;
 - технические средства охраны, сигнализации;
 - порядок охраны территории, зданий, помещений, транспортных средств;
 - требования к защите информации при интервьюировании и собеседованиях.

5.4.2.3. Все папки на электронных носителях, содержащие персональные данные Субъекта, должны быть защищены паролем

5.4.3. Защита персональной информации от воздействия внешних факторов:

5.4.3.1. 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.

5.4.3.2 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.

5.4.3.3. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

5.4.3.4. Проведение комплекса мероприятий по исключению несанкционированного доступа к информационным ресурсам с целью предотвращения овладения конфиденциальными сведениями, их использованием, а также видоизменения, уничтожения, внесения вирусов, подмены, фальсификации содержания, реквизитов документа и пр.

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

5.4.5. По возможности персональные данные обезличиваются.

5.5. В целях **устранения нарушений законодательства**, допущенных при обработке персональных данных, а также уточнения, блокирования и уничтожения персональных данных, Общество обязано:

5.5.1. При выявлении недостоверных персональных данных или неправомерных действий с ними по запросу Субъекта, его представителя, либо уполномоченного органа по защите прав Субъектов, осуществить блокирование персональных данных, относящихся к соответствующему Субъекту, с момента такого обращения или получения такого запроса на период проверки.

5.5.2. В случае подтверждения факта недостоверности персональных данных, на основании документов, представленных Субъектом, его представителем или уполномоченным органом по защите прав Субъектов, уточнить персональные данные и снять их блокирование.

5.5.3. При выявлении неправомерных действий с персональными данными, в срок не превышающий трех рабочих дней с даты выявления, устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений - уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных, уведомить Субъекта или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав Субъектов, указанный орган.

6. ПРАВА ОБЩЕСТВА

6.1. Общество имеет право проверять на достоверность персональные данные Субъекта, запрашивать на основе представленных Субъектом данных дополнительную информацию у правоохранительных, налоговых, судебных, иных государственных органов, не являющихся государственной и/или служебной тайной без письменного разрешения Субъекта.

6.2. Проверка Контрагентов ведется в соответствии с письмами Минфина России от 10.04.2009 № 03-02-07/1-177, от 06.07.2009 № 03-02-07/1-340, от 31.12.2008 № 03-02-07/2-231; ФНС России от 11.02.2010 № 3-7-07/84; Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

6.3. При проведении идентификации Контрагента, представителя Контрагента, выгодоприобретателя, бенефициарного владельца, обновлении информации о них Общество имеет право требовать представления Контрагентом, представителем Контрагента и получать от Контрагента, представителя Контрагента документы, удостоверяющие личность, учредительные документы, документы о государственной регистрации юридического лица (индивидуального предпринимателя), а также иные документы, предусмотренные Федеральным законом от 07.08.2001 № 115-ФЗ и принимаемыми на его основе нормативными правовыми актами Российской Федерации и нормативными актами Банка России.

6.4. Общество вправе запрашивать персональные данные Контрагента и его собственников (участников, учредителей, акционеров, в том числе конечных бенефициаров), руководителя, главного бухгалтера от уполномоченного представителя Контрагента.

6.5. В случае отзыва Субъектом согласия на обработку персональных данных Общество вправе продолжить обработку персональных данных в соответствии со ст.18 п.4.2) Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» и приказа Росфинмониторинга от 17.02.2011 № 59 «Об утверждении Положения

о требованиях к идентификации клиентов, представителей клиентов и (или) выгодоприобретателей, в том числе с учетом степени (уровня) риска совершения клиентом операций в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма».

7. ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Передавать Обществу или его представителю (Оператору) комплект достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

7.2. Своевременно, но не позднее 30 дней с даты соответствующего изменения, сообщать Обществу об изменении своих персональных данных.

7.3. В случае неполучения Обществом/Оператором информации об изменении персональных данных Субъекта Общество использует имеющиеся персональные данные Субъекта, и Субъект не может предъявить каких-либо претензий Обществу в связи с последствиями такого использования персональных данных Субъекта.

7.4. Контрагенты обязаны предоставлять Обществу информацию, необходимую для исполнения Обществом требований Федерального закона от 07.08.2001 №115-ФЗ, включая информацию о своих выгодоприобретателях и бенефициарных владельцах, исполнительном органе (директор, бухгалтер).

8. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Субъект имеет право на получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к нему, а также на ознакомление с такими персональными данными, за исключением случаев, предусмотренных пунктом 6.5. настоящего положения. Субъект вправе требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.2. Сведения о наличии персональных данных должны быть предоставлены Обществу Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим Субъектам.

8.3. Доступ к своим персональным данным предоставляется Субъекту или его законному представителю Оператором при обращении либо при получении от него соответствующего запроса. Запрос должен содержать номер основного документа, удостоверяющего личность Субъекта или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись Субъекта или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

8.4. Субъект имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей: подтверждение факта обработки персональных данных Оператором, а также цель такой обработки; способы обработки персональных данных, применяемые Оператором; сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых персональных данных и источник их получения; сроки обработки персональных данных, в том числе сроки их хранения; сведения о том, какие юридические последствия для Субъекта может повлечь за собой обработка его персональных данных.

8.5. Право Субъекта на доступ к своим персональным данным ограничивается в случае, если: обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка; предоставление персональных данных нарушает конституционные права и свободы других лиц.

8.6. Согласие на обработку персональных данных может быть отозвано Субъектом в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

9. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Обязательным условием обеспечения высокой надежности и эффективности функционирования системы защиты информации, является личная ответственность каждого Оператора, осуществляющего обработку персональных данных.

9.2. Каждый Оператор, 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 персональных данных Субъекта несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

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

9.5. Операторы, связанные с получением, обработкой и защитой персональных данных Субъектов обязаны принять обязательство о неразглашении персональных данных Субъектов.

9.6. Бывшие Сотрудники Общества, выполнявшие роль Оператора, и Сотрудники, переведенные/назначенные на иную должность, не связанную с обработкой персональных данных, не имеют права разглашать персональные данные Субъектов.

10. ВНЕСЕНИЕ ИЗМЕНЕНИЙ

10.1. При выявлении недостаточно эффективных мер Положения Общества либо при изменении требований применимого законодательства Российской Федерации, директор Общества организует выработку и реализацию плана действий по актуализации Положения о защите персональных данных.