

УТВЕРЖДЕНА  
приказом АО "Росагролизинг"  
от "13" февраля 2015 № 18



## Политика в области защиты персональных данных АО "Росагролизинг"

### 1. Общие положения

1.1. Настоящая Политика защиты персональных данных АО "Росагролизинг" (далее – Политика) разработана с целью закрепления основных принципов и подходов к обеспечению защиты персональных данных, реализуемых АО "Росагролизинг" (далее – Общество) в отношении обеспечения безопасности персональных данных работников и контрагентов Общества.

1.2. Политика разработана в соответствии с требованиями Конституции Российской Федерации, Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981, Трудового кодекса Российской Федерации, Гражданского кодекса Российской Федерации, Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее – Закон о персональных данных), постановления Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", а также иными нормативными правовыми (в том числе ведомственными) актами Российской Федерации, содержащими нормы о защите персональных данных, локальными нормативными актами Общества.

1.3. Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих в Обществе вопросы защиты персональных данных работников Общества и других субъектов персональных данных.

1.4. В соответствии с Законом о персональных данных Политика должна размещаться на сайте Общества [www.rosagroleasing.ru](http://www.rosagroleasing.ru) в общем доступе как документ, определяющий политику Общества в отношении защиты персональных данных субъектов персональных данных.

1.5. Работники Общества подлежат ознакомлению с Политикой в соответствии с требованиями локальных нормативных актов.

## 2. Термины, определения, сокращения

Термины, сокращения	Определения
Общество	АО "Росагролизинг"
Защита персональных данных	Принимаемые Оператором правовые, организационные и технические меры, призванные защищать персональные данные от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных
Информация	Сведения (сообщения, данные) независимо от формы их представления
Доступ к информации	Возможность получения информации и ее использования
Оператор	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие меры защиты персональных данных. Для целей настоящей Политики оператором является Общество
Персональные данные, ПДн	Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)
Субъект персональных данных, субъект ПДн	Физическое лицо, информация о котором относится к персональным данным и подлежит защите в соответствии с требованиями законодательства, настоящей Политики и локальных нормативных актов Общества
Информационная система ПДн, ИСПДн	Совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств
Обработка ПДн	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн
Распространение ПДн	Действия, направленные на раскрытие ПДн неопределенному кругу лиц
Предоставление ПДн	Действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц
Блокирование ПДн	Временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн)
Уничтожение ПДн	Действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн
Обезличивание ПДн	Действия, в результате которых становится невозможно без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн
Работник Общества	Лицо, выполняющее работу на основании трудового договора с Обществом, а также лица, выполняющие работу по гражданско-правовому договору

Термины, сокращения	Определения
Контрагент	Юридическое (уполномоченный представитель юридического лица) или физическое лицо, с которым Обществом заключен договор, либо имеющее намерение вступить в правоотношения с Обществом (потенциальный контрагент)
Ответственный работник	Работник Общества, на которого должностной инструкцией или распорядительным документом Общества возложена ответственность за обработку и защиту ПДн
Уполномоченный орган по защите прав субъектов персональных данных	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

### 3. Обработка персональных данных

3.1. Общество в качестве оператора ПДн осуществляет обработку ПДн субъектов ПДн, полученных в порядке, установленном законодательством Российской Федерации.

3.2. Обработка ПДн в ИСПДн осуществляется Обществом в целях:

1) осуществления лизинговой деятельности и иной деятельности, предусмотренной Уставом Общества и действующим законодательством Российской Федерации;

2) заключения, исполнения и прекращения договоров с физическими и юридическими лицами;

3) организации кадрового учета работников Общества и ведения кадрового делопроизводства.

3.3. Перечень ПДн, обрабатываемых в Обществе, определен и утвержден локальными нормативными актами.

3.4. В целях максимально эффективной реализации мер защиты ПДн в Обществе действуют следующие принципы обработки персональных данных:

1) законность целей и способов обработки ПДн;

2) соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Общества;

3) соответствие объема, характера, способов обработки ПДн целям обработки ПДн;

4) достоверность и актуальность ПДн;

5) достаточность ПДн для целей обработки;

6) недопустимость обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;

7) недопустимость объединения созданных для несовместимых между собой целей баз данных ИСПДн.

#### **4. Организация защиты персональных данных**

4.1. Общество принимает необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн в соответствии с требованиями законодательства Российской Федерации в части обработки ПДн в отношении следующих категорий субъектов ПДн:

1) работников Общества (в том числе бывших работников, кандидатов на замещение вакантных должностей, а также близких родственников перечисленных лиц);

2) контрагентов Общества (физических лиц) (включая потенциальных контрагентов, имеющих намерение вступить в правоотношения с Обществом);

3) уполномоченных представителей контрагентов (включая потенциальных контрагентов) – юридических лиц (руководителей, работников).

4.2. Организационные меры по защите ПДн включают в себя следующие меры безопасности:

1) физическую защиту помещений, где производится обработка ПДн (пожарно-охранная сигнализация, внутриобъектовый режим, определение границ контролируемой зоны и т.д.);

2) рациональное размещение рабочих мест работников Общества, при котором исключается угроза утечки ПДн;

3) учет материальных носителей ПДн;

4) знание и соблюдение работниками Общества требований Закона о персональных данных, локальных нормативных актов Общества по защите ПДн;

5) организацию регулярных проверок соблюдения работниками Общества требований законодательства Российской Федерации и локальных документов Общества по защите ПДн;

6) утверждение перечня уполномоченных лиц или подразделений, ответственных за обеспечение защиты ПДн в Обществе;

7) разработку локальных нормативных актов, определяющих политику Общества в отношении обработки ПДн, а также иных документов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в сфере защиты ПДн, а также устранение последствий таких нарушений;

8) осуществление внутреннего контроля и аудита соответствия обработки ПДн требованиям законодательства Российской Федерации и принятым в соответствии с ним нормативными актами, требованиям к защите ПДн, политикой Общества в отношении обработки ПДн и другими локальными актами;

9) проведение оценки вреда, который может быть причинен субъектам ПДн в случае нарушения Закона о персональных данных, выявление соотношения

указанного вреда и принимаемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных.

4.3. Технические меры по защите ПДн должны приниматься в соответствии с разработанной в Обществе моделью угроз и включать в себя следующие меры безопасности:

1) определение, выполнение и регистрация процедур контроля целостности и обеспечения доверенной загрузки программного обеспечения, в том числе программного обеспечения технических защитных мер, на средствах вычислительной техники, входящих в ИСПДн;

2) определение, выполнение, регистрация и контроль процедур доступа к эксплуатационной документации и архивным файлам, содержащим параметры настройки ИСПДн, в том числе настройки применяемых технических защитных мер;

3) определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления ПДн;

4) определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления программного обеспечения, в том числе программного обеспечения технических защитных мер, входящего в состав ИСПДн;

5) идентификация и аутентификация устройств, используемых для осуществления доступа;

6) размещение технических средств, предназначенных для администрирования ИСПДн, автоматизированных мест пользователей и серверных компонентов ИСПДн в отдельных выделенных сегментах локальных вычислительных сетей;

7) мониторинг сетевого трафика, выявление вторжений и сетевых атак и реагирование на них;

8) определение, выполнение, регистрация и контроль процедур обновления сигнатурных баз технических защитных мер;

9) определение, выполнение, регистрация и контроль процедур использования коммуникационных портов, устройств ввода-вывода информации, съемных машинных носителей и внешних накопителей информации;

10) определение, выполнение, регистрация и контроль процедур доступа к архивам ПДн;

11) организация защиты периметров сегментов локальной вычислительной сети, в которых расположены ИСПДн, и контроля информационного взаимодействия между сегментами локальных вычислительных сетей.

## **5. Права и обязанности субъектов персональных данных**

5.1. Субъект обязан предоставлять Обществу достоверные сведения о себе и своевременно информировать Общество об изменении своих ПДн.

5.2. Общество проверяет достоверность представленных сведений любыми законными способами.

5.3. Предоставление субъектом ПДн подложных документов или заведомо ложных сведений является основанием для прекращения правоотношений между Обществом и субъектом.

5.4. Сведения о ПДн должны быть предоставлены субъектом в письменном виде и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

5.5. Передача информации, содержащей ПДн субъектов, осуществляемая посредством любых средств связи (по телефону, факсу, электронной почте), без письменного согласия субъекта недопустима.

5.6. Субъект имеет право на получение информации, касающейся обработки его ПДн, в том числе:

- 1) подтверждения факта обработки ПДн Обществом;
- 2) правовых оснований и целей обработки ПДн;
- 3) способов, применяемых Обществом для обработки ПДн;
- 4) полное наименование и местонахождение Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к ПДн или которым может быть предоставлен такой доступ на основании договора или в соответствии с действующим законодательством Российской Федерации (наименование и адрес юридического лица, осуществляющего обработку ПДн по поручению Общества, если обработка поручена или будет поручена такому лицу);
- 5) перечень обрабатываемых ПДн, относящихся к соответствующему субъекту, и источник их получения, если иной порядок представления таких данных не предусмотрен законодательством Российской Федерации;
- 6) сроков обработки ПДн, в том числе сроков их хранения;
- 7) информации об осуществленной или о предполагаемой трансграничной передаче данных.

5.7. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с действующим законодательством Российской Федерации, в том числе, если доступ субъекта к его ПДн нарушает права и законные интересы третьих лиц.

5.8. Субъект вправе требовать от Общества уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или если не являются необходимыми для заявленных Обществом целей обработки.

5.9. Субъект вправе требовать извещения Обществом всех лиц, которым ранее были сообщены неверные или неполные ПДн субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.10. Согласие на обработку ПДн может быть отозвано субъектом по его письменному запросу.

5.11. Субъект вправе обжаловать любые неправомерные действия или бездействия Общества при обработке и защите его ПДн в соответствии с законодательством Российской Федерации.

## **6. Права и обязанности Общества**

6.1. Ответственные работники и должностные лица Общества, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.

6.2. Общество имеет право:

- 1) защищать свои интересы в суде;
- 2) предоставлять ПДн субъектов третьим лицам, если это предусмотрено действующим законодательством Российской Федерации;
- 3) поручить обработку ПДн другому лицу на основании договора с согласия субъекта ПДн;
- 4) отказать в предоставлении ПДн в случаях, предусмотренных законодательством Российской Федерации;
- 5) продолжить обработку ПДн субъекта без его согласия, если обработка ПДн необходима для исполнения (заключения) договора, сторонами которого являются субъект ПДн и Общество, а также в иных случаях, предусмотренных законодательством Российской Федерации.

6.3. Обработка ПДн субъекта должна осуществляться исключительно в целях обеспечения соблюдения законодательства Российской Федерации, содействия работникам в трудоустройстве, обучении и продвижении по службе (включая выдвижение в кадровый резерв), исполнения условий договора контрагентами Общества.

6.4. В бизнес-процессах Общества не должно быть решений, принимаемых на основании исключительно автоматизированной обработки ПДн и порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных п. 6.5 настоящей Политики.

6.5. Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн только при наличии согласия в письменной форме субъекта ПДн или в случаях, предусмотренных законодательством Российской Федерации, устанавливающим также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.

6.6. Общество в качестве оператора ПДн обязано сообщать в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в срок, предусмотренный законодательством Российской Федерации.

6.7. В случае изменения сведений, указанных в ответе на запрос уполномоченного органа по защите прав субъектов ПДн об обработке Обществом ПДн, Общество обязано уведомить об этих изменениях уполномоченный орган по защите прав субъектов ПДн.

6.8. Общество вправе осуществлять обработку ПДн без уведомления уполномоченного органа по защите прав субъектов ПДн, если эта обработка ПДн связана с заключением договора, стороной которого является субъект ПДн, если ПДн не распространяются, а также не предоставляются третьим лицам без согласия субъекта и используются Обществом исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн.

## **7. Ответственность**

7.1. Общество несет ответственность за соответствие обработки и обеспечение безопасности персональных данных законодательству. Все работники Общества, осуществляющие обработку персональных данных, несут ответственность за соблюдение Политики и иных локальных нормативных актов Общества по вопросам защиты персональных данных.

7.2. Любой работник, которому стало известно о нарушении настоящей Политики или который подозревает о существовании такого нарушения, должен сообщить об этом лицу, ответственному за организацию обработки ПДн, в соответствии с действующими в Обществе процедурами.

7.3. Нарушение норм, регулирующих получение, обработку и защиту ПДн может повлечь гражданскую, уголовную, административную, дисциплинарную и иные виды ответственности, предусмотренные законодательством Российской Федерации.

7.4. Работники Общества, нарушающие требования Политики, несут персональную ответственность в соответствии с Трудовым Кодексом Российской Федерации.