ПРИЛОЖЕНИЕ № 6
к приказу генерального директора
АО «Комиавтотранс»
от 02.03.2021 № 05/17

ПОЛОЖЕНИЕ
об обработке персональных данных

г. Сыктывкар
2021

Оглавление

1. Основные понятия и определения

Для целей настоящего Положения об обработке персональных данных (далее – Положение), обрабатываемых в АО «Комиавтотранс» (далее – Общество) используются следующие основные понятия и определения:

1.1. **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

1.2. **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 цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

1.3. **обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

1.4. **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

1.5. **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

1.6. **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

1.7. **блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

1.8. **уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

1.9. **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

1.10. **информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

1.11. **конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным

лицом требование не допускать их раскрытия третьим лицам и распространения без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

1.12. **документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

1.13. **средство защиты информации** – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации;

1.14. **субъект персональных данных** – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;

1.15. **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

1.16. **контролируемая зона** – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посетителей, а также транспортных, технических и иных материальных средств.

2. Общие положения

2.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2.2. Цели разработки Положения:

– определение принципов и порядка обработки персональных данных субъектов персональных данных в Обществе;

– обеспечение защиты прав и свобод субъектов персональных данных Общества при обработке их персональных данных, а также установление ответственности лиц, обрабатывающих персональные данные, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2.3. Объем обрабатываемых персональных данных, категории субъектов персональных данных которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований определяются Перечнем персональных данных, обрабатываемых в АО «Комиавтотранс» (далее – Перечень), Перечнем информационных систем персональных данных и Политикой в отношении обработки персональных данных (далее – Политика).

2.4. В Обществе обрабатываются персональные данные следующих категорий физических лиц (субъектов персональных данных):

– работников (в т.ч. уволенных работников) Общества;
– близких родственников работников;
– соискателей на вакантные должности;
– контрагентов (физических лиц, индивидуальных предпринимателей, представителей юридических лиц);
– граждан, обратившихся с жалобами, заявлениями и предложениями;
– посетителей.

2.5. Общество обрабатывает следующие категории персональных данных:

2.5.1. Работников (в т.ч. уволенных работников) Общества: фамилия, имя, отчество; место рождения; год, месяц и дата рождения; пол; адрес и дата регистрации; адрес места жительства; гражданство; контактные данные (номер телефона, email); паспортные данные (серия, номер, кем и когда выдан) или данные иного документа, удостоверяющего личность; сведения об идентификационном номере налогоплательщика; сведения о номере и серии страхового свидетельства государственного пенсионного страхования; номер расчетного (лицевого) счета (номер карты); трудовой стаж (места работы, должности, период работы, причины увольнения); сведения о трудовой книжке (серия, номер, дата выдачи, записи в ней); справка с основного места работы; сведения о временной нетрудоспособности; должность; структурное подразделение; сведения о приеме на работу, перемещении по должностям, увольнении; сведения о повышении квалификации, переподготовке или аттестации (серия, номер, дата выдачи документа о повышении квалификации, переподготовке или аттестации, наименование и местоположение образовательного учреждения); сведения о трудовом договоре (содержание и реквизиты); сведения о командировках, отпусках; табельный номер; семейное положение; состав семьи; сведения о социальном статусе; сведения о социальных льготах; тарифная ставка (оклад); надбавка; данные о начисленных суммах (заработной платы, материальной помощи, премии и иных); тип и сумма налогового вычета; статус налогоплательщика; данные о суммах удержаний и перечислений из заработной платы работника согласно его заявлению или исполнительному листу; банковские расчетные счета; сведения о сумме выплат и иных вознаграждений и страховом стаже застрахованного лица; уровень образования; наименование образовательного учреждения; сведения о документах, подтверждающих образование (наименование, номер, дата выдачи); специальность; квалификация; номер и дата выдачи удостоверения о дополнительном образовании; сведения о поощрениях и наградах; сведения о воинском учете; справка о годности к работе; сведения о нахождении в отпуске по беременности и родам, уходу за ребенком; материалы по внутренним служебным расследованиям в отношении работников; фотография (на пропуске).

2.5.2. Близких родственников работников: фамилия, имя, отчество; год, месяц и дата рождения; адрес места жительства; степень родства; сведения из свидетельства о рождении; паспортные данные (серия, номер, кем и когда выдан) или данные иного документа, удостоверяющего личность; справка с места учебы.

2.5.3. Соискателей на вакантные должности: фамилия, имя, отчество; год, месяц и дата рождения; адрес места жительства; место рождения; гражданство; контактные данные (номер телефона); трудовой стаж (места работы, должности, период работы); семейное положение; уровень образования; сведения о дополнительном образовании (курсы, переподготовка, стажировка); наименование образовательного учреждения; специальность; квалификация.

2.5.4. Контрагентов (физических лиц, индивидуальных предпринимателей, представителей юридических лиц): фамилия, имя, отчество; полное наименование индивидуального предпринимателя; адрес и дата регистрации; юридический адрес; контактные данные (номер телефона, email); паспортные данные (серия, номер, кем и когда выдан) или данные иного документа, удостоверяющего личность; сведения об идентификационном номере налогоплательщика; номер расчетного (лицевого) счета.

2.5.5. Граждан, обратившихся с жалобами, заявлениями и предложениями: фамилия, имя, отчество; адрес места жительства; контактные данные (номер телефона, email).

2.5.6. Посетителей: фамилия, имя, отчество; цель пребывания; объект посещения; срок действия пропуска; дата и время выдачи.

2.6. Категории персональных данных, которые субъект может сделать общедоступными, описывается Перечнем и определяется в Согласии на обработку персональных данных субъектов персональных данных.

2.7. Порядок ввода в действие и изменения Положения:

2.7.1. Пересмотр пунктов настоящего Положения, Перечня и Политики производится ответственным (лицом, комиссией) за организацию обработки персональных данных по мере необходимости (при изменении организационно-штатной структуры; при изменении законодательства Российской Федерации о персональных данных; при изменении условий и порядка обработки персональных данных субъектов персональных данных Общества и т.п.), но не реже 1 (одного) раза в год.

2.7.2. Настоящее Положение вступает в силу с момента его утверждения приказом генерального директора Общества и действует бессрочно, до замены его новым Положением.

2.8. Контроль соблюдения требований настоящего Положения и контроль принятых организационных и технических мер осуществляет ответственный за организацию обработки персональных данных, назначенный приказом генерального директора Общества (в случае его отсутствия – иное лицо, уполномоченное от имени Общества).

2.9. Все работники Общества, имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением под роспись.

3. Правовое основание обработки персональных данных

3.1. Необходимость обработки персональных данных с использованием средств

автоматизации, а также без использования таких средств обусловлена сложившейся практикой обработки документов, содержащих персональные данные и рядом нормативно-правовых актов Российской Федерации.

3.2. Обработка персональных данных в Обществе осуществляется, руководствуясь следующими нормативно-правовыми актами:

– Конституцией Российской Федерации;

– Трудовым кодексом Российской Федерации;

– Гражданским кодексом Российской Федерации;

– Налоговым кодексом Российской Федерации;

– Федеральным законом от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

– Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

– Федеральным законом от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе»;

– Федеральным законом от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;

– Федеральным законом от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда»;

– Федеральным законом от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

– Федеральным законом 25.12.2008 № 273-ФЗ «О противодействии коррупции»;

– Постановлением Правительства Российской Федерации от 16.04.2003 г. № 225 «О трудовых книжках»;

– Постановлением Государственного комитета по статистике от 05.01.2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;

– Согласием субъекта персональных данных на обработку персональных данных;

– Уставом акционерного общества «Комиавтотранс».

4. Права и обязанности субъектов персональных данных

4.1. Права субъектов персональных данных:

4.1.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (за исключением случаев, предусмотренных ч. 8 ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»), в том числе содержащей:

– подтверждение факта обработки персональных данных Обществом;

– правовые основания и цели обработки персональных данных;

– цели и применяемые Обществом способы обработки персональных данных;

– наименование и место нахождения Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к персональным

данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

4.1.2. Эти сведения должны быть предоставлены субъекту персональных данных Обществом в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4.1.3. Эти сведения предоставляются субъекту персональных данных или его представителю Обществом при обращении либо при получении запроса от субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Запрос должен содержать:

– номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;

– сведения о дате выдачи указанного документа и выдавшем его органе;

– сведения, подтверждающие участие субъекта персональных данных в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Обществом;

– подпись субъекта персональных данных или его представителя.

4.1.4. В случае, если указанные сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Обществу или направить ему повторный запрос в целях получения указанных сведений и ознакомления с персональными данными не ранее чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной

которого является субъект персональных данных.

4.1.5. Субъект персональных данных вправе обратиться повторно к Обществу или направить ему повторный запрос в целях получения указанных сведений, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока (30 (тридцати) дней) в случае, если такие сведения и (или) обрабатываемые персональные днные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос дополнительно должен содержать обоснование направления повторного запроса.

4.1.6. Общество вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 4.1.4 и 4.1.5 настоящего Положения. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Обществе.

4.1.7. Субъект персональных данных вправе требовать от Общества уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4.1.8. Запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам регистрируются в Журнале учета обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных АО «Комиавтотранс» (Приложение № 2 к настоящему Положению) (далее – Журнал). Данный Журнал ведется в подразделениях, где осуществляется обработка персональных данных. Журнал хранится в течение 5 (пяти) лет с момента внесения последней записи, после чего уничтожается ответственным (лицом, комиссией) за организацию обработки персональных данных.

4.1.9. Если субъект персональных данных считает, что Общество осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе подать жалобу на действия или бездействие Общества в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций об изменении сведений или в судебном порядке.

4.1.10. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

4.2. Обязанности субъектов персональных данных:

4.2.1. Субъект персональных данных обязан предоставлять полную и достоверную информацию о себе.

4.2.2. В случае изменений сведений, содержащих персональные данные субъект персональных данных обязан в течение 3 (трех) рабочих дней сообщить Обществу об изменениях и дополнениях своих персональных данных.

5. Права и обязанности работодателя и работников Общества, работающих с персональными данными

5.1. Общество имеет право:

5.1.1. отстаивать свои интересы в судебных органах;

5.1.2. предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством Российской Федерации (правоохранительные, налоговые органы и др.), а также связано с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;

5.1.3. отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством Российской Федерации;

5.1.4. использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством Российской Федерации.

5.2. Работники Общества, допущенные к персональным данным, несут ответственность за точное выполнение требований, предъявляемых к ним в целях обеспечения сохранности указанных сведений. До получения доступа к работе, связанной с обработкой персональных данных, им необходимо изучить настоящее Положение и дать письменное Обязательство о неразглашении персональных данных (конфиденциальной информации).

5.3. Работники Общества, допущенные к обработке персональных данных, должны:

5.3.1. не разглашать персональные данные;

5.3.2. о ставшей им известной утечке персональных данных сообщать непосредственному руководителю и ответственному за организацию обработки персональных данных Общества;

5.3.3. знакомиться только с теми документами и выполнять только те работы, к которым они допущены;

5.3.4. соблюдать правила пользования документами, содержащими персональные данные;

5.3.5. не допускать их необоснованной рассылки;

5.3.6. выполнять требования режима, исключающие возможность ознакомления с персональными данными посторонних лиц, включая и работников Общества, не имеющих к указанным документам прямого отношения;

5.3.7. использовать информационные ресурсы Общества только для достижения целей деятельности Общества (не использовать в личных целях);

5.3.8. при ведении деловых переговоров с представителями сторонних организаций или частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения.

5.4. Обязанности Общества:

5.4.1. Общество и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральными законами Российской Федерации.

5.4.2. Общество обязано принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Общество самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами. К таким мерам могут, в частности, относиться:

– назначение ответственного за организацию обработки персональных данных;

– издание документов, определяющих политику Общества в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Общества в отношении обработки персональных данных, локальным актам Общества;

– оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– ознакомление работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации, в том числе требованиями к защите персональных данных, документами, определяющими политику Общества в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

5.4.3. Общество обязано опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении

обработки персональных данных.

5.4.4. Общество обязано предоставить документы и локальные акты, указанные в пункте 5.4, и (или) иным образом подтвердить принятие мер, указанных в пункте 5.4.2. по запросу уполномоченного органа по защите прав субъектов персональных данных.

5.4.5. Общество обязано предоставить работнику необходимые условия для выполнения требований по охране конфиденциальных сведений, к которым допускается работник.

5.5. Работник разрешает Обществу производить контроль использования им информационных ресурсов Общества, а также использования им технических средств обработки, хранения и передачи информации, предоставленных Обществом для выполнения работником договорных обязанностей.

5.6. Общество оставляет за собой право, но не принимает каких-либо обязательств контролировать использование работником информационных ресурсов, технических средств обработки, хранения и передачи информации, а также соблюдения мер по охране конфиденциальных сведений.

6. Порядок сбора, хранения, использования и передачи персональных данных

6.1. Сбор, обработка

6.1.1. Обработка персональных данных допускается в следующих случаях:

– обработка осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

– обработка необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– обработка необходима для исполнения договора, стороной которого является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных;

– обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

– обработка необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

– обработка необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

– обработка осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных;

– осуществляется обработка персональных данных, сделанных общедоступными субъектом персональных данных;

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

– в иных случаях, описанных в ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

6.1.2. Сбор персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений, настоящим Положением и иными локальными правовыми актами Общества.

6.1.3. Все персональные данные субъекта персональных данных следует получать у него самого либо его законных представителей. Должностное лицо Общества должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, куда могут передаваться персональные данные и последствиях отказа дать письменное согласие на их получение и обработку.

6.1.4. Если получение персональных данных является обязательным в соответствии с федеральным законом, Общество обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

6.1.5. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных пунктом 6.1.6 настоящего Положения, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

– наименование либо фамилия, имя, отчество и адрес Общества или его представителя;

– цель обработки персональных данных и ее правовое основание;

– предполагаемые пользователи персональных данных;

– установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» права субъекта персональных данных;

– источник получения персональных данных.

6.1.6. Общество освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные пунктом 6.1.5 настоящего Положения, в случаях если:

– субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

– персональные данные получены Обществом на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;

– персональные данные сделаны общедоступными субъектом персональных

данных или получены из общедоступного источника;

– Общество осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

– предоставление субъекту персональных данных сведений, предусмотренных пунктом 6.1.5 настоящего Положения, нарушает права и законные интересы третьих лиц.

6.1.7. Общество не обрабатывает персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях. В соответствии со ст. 24 Конституции Российской Федерации Общество вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

6.1.8. Ввод персональных данных в автоматизированные информационные системы персональных данных Общества осуществляется работником в соответствии с его должностными обязанностями.

6.1.9. Работники, осуществляющие ввод и обработку данных с использованием автоматизированных информационных систем персональных данных Общества, несут ответственность за полноту введенной информации и не должны вносить изменения, противоречащие информации, полученной непосредственно от субъекта персональных данных.

6.2. Согласие на обработку персональных данных

6.2.1. В следующих случаях Общество получает от субъекта согласие на обработку его персональных данных:

– поручение обработки персональных данных другому лицу;

– раскрытие третьим лицам или распространение персональных данных, если иное не предусмотрено федеральным законом;

– обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;

– включение персональных данных субъекта в общедоступные источники персональных данных, в том числе публикация в средствах массовой информации и в сети Интернет;

– обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

– обработка сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются Обществом для установления личности субъекта персональных данных (согласие в письменной форме);

– трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных (согласие в письменной форме);

– принятие решения на основании исключительно автоматизированной обработки персональных данных субъекта, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы (согласие в письменной форме).

6.2.2. Работник Общества, либо лицо, поступающее на работу в Общество, являясь субъектом персональных данных, своей волей и в своем интересе принимает решение о предоставлении своих персональных данных и дает письменное согласие на их обработку («Согласие на обработку персональных данных работника АО «Комиавтотранс» (Приложение № 1а к настоящему Положению)).

6.2.3. Соискатель, являясь субъектом персональных данных, своей волей и в своем интересе принимает решение о предоставлении своих персональных данных и дает согласие на их обработку («Согласие на обработку персональных данных соискателей (Приложение № 1б к настоящему Положению))

6.2.4. Субъекты, персональные данные которых Общество обрабатывает без заключения с ними договора, должны дать согласие на обработку их персональных данных (Приложение № 1в к настоящему Положению)).

6.2.5. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

6.2.6. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Общество вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пункте 6.1 и Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных».

6.2.7. Отзыв согласия на обработку персональных данных происходит по письменному заявлению субъекта персональных данных на имя генерального директора Общества с указанием причин отзыва. При подаче заявления необходимо предъявить основной документ, удостоверяющий личность. После отзыва согласия все персональные данные, содержащиеся в информационных системах персональных данных, в течение 10 (десяти) дней уничтожаются без возможности восстановления, о чем уведомляется субъект персональных данных, если иное не

установлено законодательством Российской Федерации. Данные, находящиеся на бумажных носителях, передаются в архив и хранятся в течение сроков, установленных законодательством.

6.3. Передача персональных данных

6.3.1. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

6.3.2. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

6.3.3. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

6.3.4. При передаче персональных данных субъекта Обществу необходимо соблюдать следующие требования:

– не сообщать персональные данные субъекта третьей стороне без согласия субъекта, за исключением случаев, предусмотренных пунктом 6.1.1 настоящего Положения, а также в случаях, установленных федеральным законодательством;

– предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц исполнения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– разрешать доступ к персональным данным только уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции;

– передавать персональные данные субъекта представителям субъектов в порядке, установленном Трудовым кодексом Российской Федерации, Семейным кодексом Российской Федерации, и ограничивать эту информацию только теми

персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций.

6.3.5. В соответствии с законодательством Российской Федерации персональные данные, обрабатываемые Обществом, могут быть переданы правоохранительным, судебным органам, органам социальной защиты и другим Обществам, которые имеют на это право на основании федерального законодательства, а также в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороноспособности страны и безопасности государства без получения согласия субъекта персональных данных.

6.3.6. Решение о передаче информации, содержащей персональные данные, обрабатываемые в Обществе, третьим лицам, за исключением указанного в пункте 6.3.5 настоящего Положения, принимается генеральным директором Общества только на основании мотивированного письменного запроса, если иное не предусмотрено договором или федеральным законодательством. Мотивированный запрос должен быть подписан уполномоченным должностным лицом, содержать указание цели и правовое основание предоставления персональных данных, срок предоставления этой информации, если иное не установлено федеральными законами.

6.3.7. Порядок передачи информации, содержащей персональные данные, обрабатываемые Обществом, внутри Общества определяется должностными обязанностями работников и/или локальными нормативными актами Общества, в соответствии с законодательством Российской Федерации.

6.4. Хранение и уничтожение

6.4.1. Персональные данные могут храниться в бумажном и(или) электронном виде в подразделениях Общества с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации и локальными нормативными актами мер по защите персональных данных. Право на доступ к местам хранения персональных данных предоставляется работникам структурных подразделений и(или) должностным лицам, определенным настоящим Положением, а также приказами о доступе к персональным данным, распорядительными документами или письменными указаниями генерального директора Общества.

6.4.2. Хранение персональных данных в информационных системах персональных данных осуществляется на серверах и автоматизированных рабочих местах Общества с использованием специализированного программного обеспечения.

6.4.3. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является субъект персональных данных.

6.4.4. Обрабатываемые персональные данные подлежат уничтожению (либо обезличиванию) в следующих случаях:

– по достижении целей обработки или в случае утраты необходимости в

достижении этих целей, если иное не предусмотрено федеральным законом;

– по требованию субъекта персональных данных, его представителя или уполномоченного органа по защите прав субъектов персональных данных, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными, неправомерно обрабатываемыми или не являются необходимыми для заявленной цели обработки;

– отзыв субъектом персональных данных согласия на обработку его персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между Обществом и субъектом персональных данных либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

6.4.5. В случае достижения целей обработки персональных данных, обработка персональных данных прекращается и персональные данные (или их материальные носители) подлежат уничтожению в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Обществом и субъектом персональных данных, либо если Общество не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством Российской Федерации.

6.4.6. Уничтожение носителей персональных данных производится ответственным лицом после поступления от руководителей структурных подразделений, обрабатывающих персональные данные, перечня подлежащих уничтожению носителей персональных данных (в том числе в электронном виде) с указанием основания для их уничтожения.

6.4.7. Уничтожение персональных данных на машинных носителях информации производится после истечения сроков хранения персональных данных ответственным с использованием специального программного обеспечения или средств гарантированного уничтожения информации.

6.4.8. Способ уничтожения носителей персональных данных должен исключать возможность восстановления уничтоженных персональных данных.

6.4.9. Уничтожению не подлежат персональные данные, для которых законодательством Российской Федерации предусмотрены иные сроки хранения.

6.4.10. Уничтожению (стиранию) может подвергаться только сама информация о субъекте персональных данных, хранящаяся на носителе, либо сам носитель персональных данных.

6.4.11. По всем фактам уничтожения персональных данных или носителей персональных данных составляется Акт об уничтожении персональных данных АО «Комиавтотранс» (Приложение № 3 к настоящему Положению).

6.4.12. Перед непосредственным уничтожением носителей персональных данных ответственным лицом осуществляется сверка документов и дел с описью, приведенной в Акте об уничтожении персональных данных АО «Комиавтотранс».
6.4.13. Бумажные носители персональных данных уничтожаются в присутствии ответственного лица, принимавшего участие в сверке (проверке) документов (дел), подлежащих уничтожению.
6.4.14. Уничтожение документов производится путем сожжения, дробления, растворения или химического разложения, превращения в бесформенную массу или порошок. Выбор разрешенных конкретных способов для уничтожения персональных данных и их носителей осуществляется ответственным.

6.5. Общедоступные персональные данные

6.5.1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.
6.5.2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

6.6. Правила работы с обезличенными данными

6.6.1. Обезличивание персональных данных может быть проведено с целью ведения статистических наблюдений, снижения потенциального ущерба от разглашения персональных данных и по достижению целей обработки персональных данных или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.
6.6.2. При проведении работ по обезличиванию необходимо руководствоваться Правилами работы с обезличенными персональными данными АО «Комиавтотранс» (Приложение № 5 к настоящему Положению)
6.6.3. Для обезличенных персональных данных нет необходимости обеспечения их конфиденциальности.
6.6.4. Для того, чтобы распространять, предоставлять третьим лицам, публиковать, передавать по незащищенным каналам связи и т.п. обезличенные персональные данные, необходимо (перед совершением этих действий) убедиться в правильности проведения процедуры обезличивания персональных данных. Процедура обезличивания считается проведенной успешно, если по обезличенным персональным данным становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. При этом необходимо обеспечить конфиденциальность той дополнительной информации, с помощью которой возможно определить принадлежность персональных данных конкретному

субъекту персональных данных.

7. Правила рассмотрения запросов субъектов персональных данных и их представителей

Таблица 1. Взаимодействие с субъектом персональных данн

№ п/п	Событие	Действие	Основания для отказа, исключени
1	Запрос субъекта персональных данных на получение информации, касающейся обработки его персональных данных	Предоставить субъекту персональных данных информацию по форме Справки об обработке персональных данных субъекта АО «Комиавтотранс» (Приложение № 5 к настоящему Положению) либо мотивированный отказ со ссылкой на п. 8 ст. 14 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» в течение 30 (тридцати) дней со дня получения запроса	см. п. 8 ст. 1 ФЗ от 27.07.2006 № 152-ФЗ «О персональны х данных»
2	Предоставление субъектом сведений, подтверждающих, что обрабатываемые персональные данные являются неполными, неточными или неактуальными	Немедленно блокировать или обеспечить блокирование персональных данных на период проверки. Внести необходимые изменения в персональные данные в течение 7 (семи) рабочих дней со дня получения сведений. Уведомить субъекта персональных данных о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы	см. п. 2 ст. 2 ФЗ от 27.07.2006 № 152-ФЗ «О персональны х данных»
3	Предоставление субъектом сведений, подтверждающих, что обрабатываемые персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки	В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Общество обязано уничтожить такие персональные данные	см. п. 3 ст. 20 ФЗ от 27.07.2006 № 152-ФЗ «О персональны х данных»
4	Запрос уполномоченного	Ответить на запрос в течение 30 (тридцати) дней со дня получения	см. п. 4 ст. 20 ФЗ от

№ п/п	Событие	Действие	Основания для отказа, исключения
	органа по защите прав субъектов персональных данных	запроса, если иное не указано в запросе	27.07.2006 № 152-ФЗ «О персональных данных»
5	Обращение, запрос субъекта персональных данных либо уполномоченного органа по защите прав субъектов персональных данных о выявлении неправомерной обработки персональных данных	Прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение с составлением Акта об уничтожении персональных данных АО «Комиавтотранс». Уведомить субъекта персональных данных о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы	см. п. 3 ст. 21 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»
6	Получение персональных данных субъектов от третьих лиц	Уведомить субъекта об обработке его персональных данных либо убедиться, что третье лицо (на основании заключенного договора с этим лицом о получении персональных данных) получило согласие субъекта персональных данных на передачу его персональных данных	

8. Доступ к персональным данным субъектов

8.1. Доступ работников Общества к персональным данным осуществляется в соответствии со списками, которые утверждаются приказом генерального директора Общества. Руководитель, разрешающий доступ работника своего

подразделения к носителю персональных данных, несет персональну ответственность за данное разрешение.

8.2. Ознакомление лиц с персональными данными субъектов должн осуществляться только по необходимости и в тех объемах, которые необходимы дл выполнения возложенных на них функций.

9. Обработка персональных данных, осуществляемой без использования средств автоматизации

9.1. Обработка персональных данных, осуществляемая без использования средст автоматизации, должна осуществляться таким образом, чтобы в отношении каждо категории персональных данных можно было определить места хранени персональных данных (материальных носителей) и установить перечень лиц осуществляющих обработку персональных данных.

9.2. При хранении материальных носителей должны соблюдаться условия обеспечивающие сохранность персональных данных и исключающи несанкционированный к ним доступ. Лица, осуществляющие обработк персональных данных без использования средств автоматизации, должны быт проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правила осуществления такой обработки.

9.3. Персональные данные при их обработке, осуществляемой без использовани средств автоматизации, должны обособляться от иной информации, в частност путем фиксации их на отдельных материальных носителях персональных данных, специальных разделах или на полях форм (бланков).

9.4. При фиксации персональных данных на носителях не допускается фиксация н одном материальном носителе персональных данных, цели обработки которы заведомо не совместимы. Для обработки различных категорий персональны данных, осуществляемой без использования средств автоматизации, для каждо категории персональных данных должен использоваться отдельный носитель.

9.5. Уничтожение или обезличивание части персональных данных, если эт допускается носителем, может производиться способом, исключающи дальнейшую обработку этих персональных данных с сохранением возможност обработки иных данных, зафиксированных на материальном носителе (удалени вымарывание).

9.6. Уточнение персональных данных при осуществлении их обработки б использования средств автоматизации производится путем обновления ил изменения данных на носителе, а если это не допускается техническим особенностями носителя, - путем фиксации на том же носителе сведений вносимых в них изменениях либо путем изготовления нового носителя уточненными персональными данными.

9.7. Необходимо обеспечивать раздельное хранение персональных данны (носителей), обработка которых осуществляется в различных целях.

9.8. При хранении носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

10. Обеспечение безопасности персональных данных

10.1. Безопасность персональных данных при их обработке в информационных системах персональных данных обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе персональных данных информационные технологии.

10.2. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

10.3. Лица, получившие доступ к персональным данным, обязаны не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

10.4. В случае, если Общество на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности и безопасности персональных данных при их обработке.

10.5. Меры по обеспечению конфиденциальности персональных данных, принимаемые в Обществе, должны включать, но не ограничиваясь этим, следующее:

– определение перечня персональных данных и мест обработки таких данных;

– ограничение доступа к персональным данным, их носителям, путем установления порядка обращения с этими данными и носителями, контроля за соблюдением такого порядка;

– учет лиц, получивших доступ к персональным данным, и (или) лиц, которым такие данные были предоставлены или переданы;

– учет носителей (документов), содержащих персональные данные.

10.5.1. Организационные меры безопасности:

– инструктаж работников по правилам обеспечения безопасности обрабатываемых персональных данных;

– учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;

– мониторинг и реагирование на инциденты информационной безопасности, связанные с персональными данными, включая проведение внутренних проверок,

12

разбирательств и составление заключений;

– постоянный контроль за соблюдением требований по обеспечени безопасности персональных данных (реализуется путем внутренних аудитов).

10.5.2. Меры физической безопасности:

– ограничение доступа пользователей в помещения, где размещен технические средства, позволяющие осуществлять обработку персональны данных, а также хранятся носители информации. Приказом по Обществ устанавливается контролируемая зона Общества, вводятся в действие Спис помещений с ограниченным доступом и Список лиц, имеющих право посеща помещения Общества с ограниченным доступом. Лица, не указанные в Списке, том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремо оборудования и технических средств), при наличии необходимости могут посеща помещения с ограниченным доступом в сопровождении ответственных лиц;

– размещение технических средств, позволяющих осуществлять обработ персональных данных, в пределах охраняемой территории;

– организация физической защиты помещений и собственно техническ средств, позволяющих осуществлять обработку персональных данных.

10.5.3. Технические меры безопасности:

– разграничение доступа пользователей и обслуживающего персонала информационным ресурсам, программным средствам обработки (передачи) защиты информации;

– регистрация действий пользователей и обслуживающего персонала, контро доступа и действий пользователей, обслуживающего персонала и посторонних ли

– резервирование технических средств, дублирование массивов и носител информации;

– использование защищенных каналов связи;

– предотвращение внедрения в информационные системы вредоносны программ (программ-вирусов) и программных закладок.

11. Правила осуществления внутреннего контроля соответствия обработк персональных данных требованиям к защите персональных данных

11.1. Контроль выполнения работ по обеспечению безопасности персональны данных (далее – Контроль) в Обществе осуществляется путем проведен периодических контрольных мероприятий (в рамках внутренних аудитов) внутренних проверок по фактам произошедших инцидентов информационно безопасности.

11.2. В рамках проведения контрольных мероприятий в Обществе выполняются:

– проверка наличия и актуальности планов, регистрационных журналов, акто договоров, отчетов, протоколов и других свидетельств выполнения мероприятий обеспечению безопасности персональных данных;

– проверка осведомленности и соблюдения персоналом требований обеспечению безопасности персональных данных;

– проверка соответствия перечня лиц, которым предоставлен доступ к персональным данным, и их полномочий по доступу к определенным категориям персональных данных фактическому состоянию;

– проверка локальных актов, определяющих условия хранения материальных носителей, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ, перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер;

– проверка документов, определяющих места хранения персональных данных, перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

– проверка документов об информировании лиц, осуществляющих обработку персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

– проверка получения и передачи персональных данных третьим лицам с согласия субъекта персональных данных либо с последующим уведомлением субъекта о факте обработки его персональных данных;

– проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности персональных данных, в соответствии с требованиями эксплуатационной и технической документации;

– инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности персональных данных (при необходимости);

– проверка соответствия моделей угроз для информационных систем персональных данных условиям функционирования данных систем;

– проверка соответствия организационно-распорядительной документации по обеспечению безопасности персональных данных действующим требованиям законодательства Российской Федерации, руководящих документов ФСБ России, ФСТЭК России.

11.3. Все собранные в ходе проведения контрольных мероприятий в Обществе свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

11.4. Контрольные мероприятия проводятся как периодически в соответствии с планом и программой аудита, так и внепланово по решению руководства Общества и в случае возникновения инцидентов информационной безопасности.

11.5. Внутренние проверки в Обществе в обязательном порядке проводятся в случае выявления следующих фактов:

– нарушение конфиденциальности, целостности, доступности персональных данных;

– халатность и несоблюдение требований к обеспечению безопасност персональных данных;

– несоблюдение условий хранения носителей персональных данных;

– использование средств защиты информации, которые могут привести нарушению заданного уровня безопасности (конфиденциальность/целостност доступность) персональных данных или другим нарушениям, приводящим снижению уровня защищенности персональных данных.

11.6. Задачами внутренней проверки являются:

– установление обстоятельств нарушения, в том числе времени, места способа его совершения;

– установление лиц, непосредственно виновных в данном нарушении;

– выявление причин и условий, способствовавших нарушению.

12. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Общество, а также должностные лица, виновные в нарушении нор регулирующих получение, обработку и защиту персональных данных, нес дисциплинарную, гражданскую, административную, уголовную и ину ответственность, предусмотренную законодательством Российской Федерации.

Прошито, пронумеровано и скреплено печатью
14 (четырнадцать) лист 08
Генеральный директор АО «Комиавтотранс»

Лапин П.К. м.п.