



ПРИКАЗ

БОЕРЫК

«27» августа 2020 г

№ 29

**Об утверждении политики
безопасности обработки
персональных данных Агентства
инвестиционного развития
Республики Татарстан**

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ
«Об информации, информационных технологиях и о защите информации»

ПРИКАЗЫВАЮ:

1. Утвердить политику безопасности обработки персональных данных Агентства инвестиционного развития Республики Татарстан, в соответствии с приложением к настоящему приказу.

2. Контроль за исполнением настоящего приказа возложить на заместителя Агентства инвестиционного развития Республики Татарстан М.Г. Епифанцеву.

Руководитель

Т.И. Минуллина

УТВЕРЖДЕНА
Приказом Агентства инвестиционного
развития Республики Татарстан
№ 29

« 24 » августа 2020 г.

ПОЛИТИКА
безопасности обработки персональных данных Агентства
инвестиционного развития Республики Татарстан

1. Основные термины и определения

Для целей настоящей Политики применяются следующие термины и определения:

Оператор персональных данных (далее – 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;

Субъект персональных данных – физическое лицо, к которому относятся персональные данные;

Работник Оператора - физическое лицо, состоящие в трудовых и иных гражданско-правовых отношениях с Оператором.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

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;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Конфиденциальность персональных данных – операторы 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 федеральным законодательством;

Санкционированный доступ к информации – доступ к информации, не нарушающий правила разграничения доступа;

Несанкционированный доступ (далее - НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

Уровень защищенности персональных данных - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных.

2. Общие положения

2.1. Настоящая Политика определяет порядок сбора, обработки и защиты персональных данных работников Агентства инвестиционного развития Республики Татарстан (далее – Агентство) и граждан, обратившихся в Агентство с жалобой или заявлением.

2.2. Основанием для разработки настоящей политики являются:

- Конституция Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

- Федеральный закон от 25 декабря 2008 года № 273-ФЗ «О противодействии коррупции»;
- Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
- Трудовой кодекс Российской Федерации;
- Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Закон Республики Татарстан от 16 января 2003 года № 3-ЗРТ «О государственной гражданской службе Республики Татарстан» и иные нормативные правовые акты в области защиты персональных данных.

2.3. Целью настоящей Политики является определение безопасного порядка обработки персональных данных граждан, обратившихся в Агентство, а также работников Агентства, обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц Агентства, имеющих доступ к персональным данным, за невыполнение требований и норм, регулирующих обработку и защиту персональных данных.

Обработка персональных данных в Агентстве осуществляется с соблюдением принципов и условий, предусмотренных настоящей Политикой и законодательством Российской Федерации в области персональных данных.

Персональные данные граждан относятся к категории конфиденциальной информации.

3 Общие принципы и условия обработки персональных данных субъектов персональных данных

3.1 Обработка персональных данных субъектов персональных данных осуществляется на основе следующих принципов:

3.1.1. Обработка персональных данных должна осуществляться на

законной и справедливой основе.

3.1.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.1.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.1.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

3.1.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.1.6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Агентство должно принимать необходимые меры, либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных.

3.1.7. 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, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению или обезличиванию по достижении целей обработки, а также в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законодательством.

3.2 В целях обеспечения прав и свобод человека и гражданина, Агентство и его представители при обработке персональных данных гражданина или работника обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных работников Агентства и членов их семей может осуществляться исключительно в целях обеспечения соблюдения законодательства Российской Федерации в области персональных данных и иных нормативных правовых актов с учетом положений Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», оформления трудовых отношений, расчета и выдачи заработной платы или других доходов, налоговых и пенсионных отчислений, содействия работникам в трудоустройстве, обучении, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы, обеспечения сохранности имущества Агентства сбора и обработки деклараций о доходах, движимом и недвижимом имуществе работников и членов их семей.

3.2.2. Все персональные данные субъекта персональных данных следует получать у него самого или у его полномочного представителя. Если

персональные данные субъекта персональных данных возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие;

3.2.3. При определении объема и содержания обрабатываемых персональных данных Агентство должно руководствоваться Конституцией Российской Федерации, Трудовым кодексом, законодательством Российской Федерации в сфере защиты персональных данных, противодействия коррупции и государственной гражданской службы, иными нормативными актами в области защиты персональных данных.

3.2.4. Агентство не имеет права получать и обрабатывать персональные данные субъекта персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных федеральными законами. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, Агентство вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

3.2.5. В Агентстве запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъектов персональных данных или иным образом затрагивающих их права и законные интересы, за исключением случаев, предусмотренных федеральными законами.

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

3.2.7. Агентство обязано разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов.

3.2.8. Агентство обязано рассмотреть возражение субъекта персональных данных в течение тридцати дней со дня регистрации письменного обращения и уведомить его о результатах рассмотрения такого возражения.

3.2.9. Защита персональных данных субъекта персональных данных от неправомерного их использования или утраты должна быть обеспечена

Агентством за счет своих средств, в порядке, установленном федеральным законодательством и другими нормативными документами.

4. Получение персональных данных субъекта персональных данных

4.1 Получение персональных данных преимущественно осуществляется путем представления их самим субъектом персональных данных, на основании его письменного согласия, за исключением случаев, предусмотренных законодательством Российской Федерации.

В случаях, предусмотренных федеральным законодательством, обработка персональных данных осуществляется только с согласия субъекта персональных данных в письменной форме. равнозначным содержащему собственноручную подпись согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие субъекта персональных данных в письменной форме на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) полное наименование и адрес Агентства;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Агентством способов обработки персональных данных;

7) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено Федеральным законодательством;

8) подпись субъекта персональных данных.

4.2 Обработка персональных данных Агентством не требует получения письменного согласия субъекта персональных данных в следующих случаях:

1) обработка персональных данных необходима для достижения целей, предусмотренных федеральными законами, для осуществления и выполнения возложенных законодательством Российской Федерации на Агентство функций, полномочий и обязанностей;

2) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем,

по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

3) обработка персональных данных необходима для осуществления прав и законных интересов Агентства или третьих лиц при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

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

5) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен самим субъектом персональных данных либо по его просьбе (общедоступных персональных данных);

6) Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.3. Обработка специальных категорий персональных данных, биометрических персональных данных, трансграничная передача персональных данных без письменного согласия субъекта персональных данных осуществляются Агентством только в случаях, предусмотренных федеральными законами.

5 Хранение и обработка персональных данных

5.1 Персональные данные хранятся и обрабатываются Агентством с соблюдением требований действующего законодательства о защите персональных данных.

5.2 Обработка персональных данных в Агентстве осуществляется смешанным способом: неавтоматизированным и автоматизированным.

5.3 Персональные данные субъектов персональных данных хранятся и обрабатываются в Агентстве на бумажных носителях и в электронном виде.

5.4 Хранение и обработка бумажных документов, содержащих персональные данные, осуществляется Агентством в соответствии с требованиями Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденными постановлением Правительства Российской Федерации от 15.09.2008 г. № 687, иными нормативными документами, регламентирующими специальный порядок хранения отдельных категорий документов.

5.5 Хранение и обработка персональных данных в электронном виде осуществляется Агентством в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119.

5.6 Хранение персональных данных как в электронном, так и на бумажных носителях в Агентстве осуществляется не дольше, чем этого требуют цели их обработки. Персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5.7 Хранение документов, содержащих персональные данные субъектов персональных данных, осуществляется в течение сроков хранения, установленных нормативными актами. По истечении установленных сроков хранения документы подлежат уничтожению способом, исключающим несанкционированный доступ третьих лиц к уничтожаемым документам.

6. Защита персональных данных

6.1 Агентство при обработке персональных данных обязано принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, предусмотренные статьей 19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

6.2 Обеспечение безопасности персональных данных субъектов персональных данных в Агентстве достигается следующими мероприятиями:

1) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применение организационных и технических мер по обеспечению безопасности персональных данных;

3) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учет машинных носителей персональных данных;

6) обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;

9) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

7 Передача персональных данных субъектов персональных данных третьим лицам

7.1 Передача персональных данных третьим лицам Агентством осуществляется только с письменного согласия субъекта персональных данных за исключением случаев, предусмотренных статьей 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»:

1) передача персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или федеральным законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Агентство функций, полномочий и обязанностей;

2) передача персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих обязательному исполнению в соответствии с законодательством Российской Федерации;

3) передача персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

4) передача персональных данных необходима для защиты жизни и здоровья или иных жизненно важных интересов субъекта персональных данных, если получение его согласия невозможно;

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

6) передача общедоступных персональных данных;

7) передача персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

8) в иных случаях, прямо предусмотренных федеральным законодательством.

8 Общедоступные источники персональных данных субъектов персональных данных

8.1 Включение персональных данных субъекта персональных данных в общедоступные источники персональных данных возможно только при наличии его письменного согласия.

8.2 В целях информационного обеспечения Агентства могут создаваться общедоступные источники персональных данных для ознакомления с ними неопределенного круга лиц (в том числе сайты в сети

Интернет, телефонные справочники, информационные стенды и т.д.) В общедоступные источники персональных данных могут включаться только те персональные данные, которые указаны в письменном согласии субъекта персональных данных.

8.3 Персональные данные могут быть исключены из общедоступных источников персональных данных по требованию субъекта персональных данных, по достижении целей их размещения в общедоступных источниках персональных данных, либо по решению суда или иных уполномоченных государственных органов.

9 Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных субъектов персональных данных

9.1. Работники Агентства, виновные в нарушении правил обработки персональных данных, повлекших за собой разглашение, утерю, искажение персональных данных или иные нарушения прав субъектов персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.