

Федеральное государственное бюджетное учреждение «Всероссийский
научно-исследовательский институт метрологической службы»
(ФГБУ «ВНИИМС»)

Утверждаю
Директор ФГБУ «ВНИИМС»


_____ С.А. Денисенко

«07» апреля 2023 г.

ПОЛИТИКА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Москва 2023

1. Общие положения

1.1. Настоящая Политика защиты и обработки персональных данных в ФГБУ «ВНИИМС» (далее – Политика) разработана в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Политика действует в отношении всех персональных данных, которые обрабатывает ФГБУ «ВНИИМС» (далее – Оператор).

1.3. Политика распространяется на отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящей Политики.

1.4. Политика публикуется в свободном доступе на внутреннем портале Оператора и в информационно-телекоммуникационной сети Интернет на сайтах Оператора (<http://www.vniims.ru>, www.ktopoverit.ru).

1.5. Положения Политики являются обязательными для исполнения всеми работниками Оператора, осуществляющими обработку персональных данных.

1.6. Оператор имеет право вносить изменения в Политику. Изменения и дополнения к Политике утверждаются приказом директора ФГБУ «ВНИИМС».

2. Основные понятия

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

Оператор персональных данных (оператор) – ФГБУ «ВНИИМС» 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, данные которого обрабатываются.

Обработка персональных данных – любое действие (операции) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

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

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.

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.

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

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

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Субъект доступа – лицо или процесс, осуществляющий доступ к данным.

Объект доступа – единица информационного ресурса автоматизированной системы, к которой осуществляется доступ.

Защита персональных данных – необходимые правовые, организационные и технические меры, применяемые 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.

3. Цели сбора персональных данных

3.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

3.3. Обработка Оператором персональных данных осуществляется в следующих целях:

- обеспечение соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;
- осуществление своей деятельности в соответствии с Уставом Оператора;

- ведение кадрового делопроизводства и для выполнения всех требований трудового законодательства Российской Федерации;
- исчисления и уплаты, предусмотренных законодательством Российской Федерации налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- привлечение и отбор кандидатов для трудоустройства к Оператору;
- представления информации в государственные органы в рамках исполнения Оператором возложенных законодательством Российской Федерации обязанностей;
- осуществление гражданско-правовых отношений;
- противодействие коррупции;
- организации пропускного режима;
- издание полиграфической продукции;
- осуществление добровольного медицинского страхования работников Оператора;
- повышение квалификации работников Оператора в сторонних организациях.

3.4. Обработка персональных данных работников Оператора может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов и регламентируется Положением о работе с персональными данными работников ФГБУ «ВНИИМС».

4. Условия обработки персональных данных

4.1. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

4.2. Обработка персональных данных осуществляется Оператором следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

4.3. Оператор организует обработку персональных данных в следующем порядке:

4.3.1. Назначает ответственного за организацию обработки персональных данных (далее - ответственный ОПД), устанавливает перечень лиц, имеющих доступ к персональным данным.

4.3.2. Издает настоящую Политику, локальные акты по вопросам обработки персональных данных.

4.3.3. Применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных.

4.3.4. Осуществляет внутренний контроль соответствия обработки персональных данных Федеральному закону от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным актам Оператора.

4.4. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры, в том числе:

4.4.1. определяет угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

4.4.2. применяет организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

4.4.3. применяет, пропущенные в установленном порядке процедуру оценки соответствия, средства защиты информации;

4.4.4. учитывает машинные носители персональных данных;

4.4.5. обнаруживает факты несанкционированного доступа к персональным данным и принимает меры;

4.4.6. восстанавливает персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;

4.4.7. устанавливает правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных.

4.5. Запрещается хранение документов с персональными данными и их копий на рабочих местах и (или) в открытом доступе.

4.6. В электронном виде документы, содержащие персональные данные, разрешается хранить в специализированных базах данных или в специализированных отведенных для этого директориях с ограничением доступа. Копирование таких данных запрещено.

5. Порядок обработки персональных данных в информационных системах

5.1. Обработка персональных данных в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

5.2. Уполномоченному работнику (Уполномоченным работникам) Оператора, имеющему право осуществлять обработку персональных данных в

информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе.

5.3. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах, достигается путем исключения несанкционированного, доступа к персональным данным.

5.4. В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками Оператора незамедлительно принимаются меры по установлению причин нарушений и их устранению.

5.5. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и/или обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

6. Актуализация, исправление, удаление и уничтожение персональных данных, запросы субъектов персональных данных на доступ к своим персональным данным

6.1. Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в пункте 7 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», предоставляются Оператором субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

6.2. 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 Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;

- подпись субъекта персональных данных или его представителя.

6.3. Запрос субъекта персональных данных в отношении обработки персональных данных Оператором принимаются по юридическому адресу Оператора: 119361 г. Москва, вн. тер. г. муниципальный округ Очаково-Матвеевское, ул. Озерная, д.46. Также субъект персональных данных может направить свой запрос, подписанный усиленной квалифицированной электронной подписью на адрес электронной почты ответственного ОПД. Срок рассмотрения обращений не превышает 30 (тридцати) дней со дня обращения.

6.4. Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» все необходимые сведения или субъект не обладает правом доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

6.5. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с пунктом 8 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

6.6. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя, или по запросу Роскомнадзора. Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса, на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.7. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем, либо Роскомнадзором, или иных необходимых документов, уточняет персональные данные в течение семи рабочих дней, со дня представления таких сведений, и снимает блокирование персональных данных.

6.8. В случае выявления неправомерной обработки персональных данных при обращении (запросе) субъекта персональных данных или его представителя,

либо Роскомнадзора, Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения запроса.

6.9. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

- иное не предусмотрено договором, стороной которого выгодоприобретателем или поручителем, по которому является субъект персональных данных;

- Оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» или иными федеральными законами;

- иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

6.10. Порядок уничтожения персональных данных Оператором:

6.10.1. Условия и сроки уничтожения персональных данных Оператором:

- достижение цели обработки персональных данных либо утрата необходимости достигать эту цель - в течение 30 дней;

- достижение максимальных сроков хранения документов, содержащих персональные данные - в течение 30 дней;

- предоставление субъектом персональных данных (его представителем) подтверждения того, что персональные данные получены незаконно или не являются необходимыми для заявленной цели обработки - в течение 7 рабочих дней;

- отзыв субъектом персональных данных согласия на обработку его персональных данных, если их сохранение для цели их обработки более не требуется, - в течение 30 дней.

6.10.2. Уничтожение персональных данных осуществляют лица, ответственные за хранение персональных данных, назначенные приказом Оператора, если иное не установлено в локальных нормативных актах Оператора.

6.10.3. Способы уничтожения персональных данных устанавливаются в локальных нормативных актах Оператора.

7. Права и обязанности Оператора

7.1. Оператор имеет право:

7.1.1. Самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» и другими нормативными правовыми актами.

7.1.2. Поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным

законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством Российской Федерации.

7.1.3. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных».

7.2 Оператор обязан:

7.2.1. Организовывать обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

7.2.2. Отвечать на обращения и запросы субъектов персональных данных и их законных представителей в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

8. Права субъекта персональных данных

8.1 Субъект персональных данных имеет право:

8.1.1. Получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами.

8.1.2. Требовать от Оператора 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 в соответствии с законодательством Российской Федерации меры по защите своих прав.

9. Комиссия оператора по обработке персональных данных

9.1. Обработку персональных данных организует комиссия по обработке персональных данных (далее - Комиссия).

9.2. Комиссия:

1) доводит до сведения работников Оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

2) организует обработку персональных данных сотрудниками Оператора;

3) организует прием и обработку обращений и запросов субъектов персональных данных или их представителей.

9.3. Контроль за исполнением сотрудниками Оператора требований законодательства Российской Федерации и положений локальных нормативных актов Оператора при обработке персональных данных возложен на Ответственного ОПД.

9.4. Ответственный ОПД:

1) осуществляет внутренний контроль за соблюдением Оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) контролирует прием и обработку обращений и запросов субъектов персональных данных или их представителей.

9.5. Комиссия ОПД обеспечивает:

своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до Ответственного ОПД;

недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

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

постоянный контроль за обеспечением уровня защищенности персональных данных;

соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;

разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

9.6. Комиссия ОПД принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

9.7. Обмен персональными данными при их обработке в информационных системах Оператора осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

9.8. Доступ сотрудников Оператора к персональным данным, находящимся в информационных системах Оператора, предусматривает обязательное прохождение процедуры идентификации и аутентификации.

9.9. В случае выявления нарушений порядка обработки персональных данных в информационных системах Оператора уполномоченными

должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

10. Заключительные положения

10.1. Политика является общедоступным документом.

10.2. Ответственность лиц, имеющих доступ к персональным данным, определяется действующим законодательством Российской Федерации.

Начальник отдела кадров



О.Ю. Матвиенко

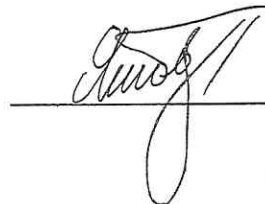
СОГЛАСОВАНО

Начальник отдела



Р.В. Пенерджи

Начальник юридического отдела



С.Ф. Яжборовский