ПРИЛОЖЕНИЕ 2 к Приказу № 117-П
от « 01 » декабря 2023 г.

УТВЕРЖДЕНО:

Генеральный директор
СРО Ассоциации «НАКС»

_____/А. И. Прилуцкий/

« 01 » декабря 2023 года

ПОЛОЖЕНИЕ
об обработке и обеспечении безопасности персональных данных в Саморегулируемой организации Ассоциации «Национальное Агентство Контроля и Сварки» (СРО Ассоциации «НАКС»)

город Москва

2023 год

СОДЕРЖАНИЕ

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об обработке и обеспечении безопасности персональных данных (далее – Положение) в Саморегулируемой организации Ассоциации «Национальное Агентство Контроля и Сварки» (Сокращенное наименование СРО Ассоциация «НАКС») (далее Оператор) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативно правовыми актами Российской Федерации.

1.2. Настоящее Положение определяет для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, определяет правовые, организационные и технические меры по обеспечению безопасности персональных данных Оператором.

1.3. Действие настоящего Положения распространяется на структурные подразделения Оператора, в которых осуществляется обработка персональных данных.

1.4. Утверждение настоящего Положения, внесение в него изменений и отмена производятся приказом Генерального директора СРО Ассоциации «НАКС».

1.5. Работники Оператора, осуществляющие обработку персональных данных, ответственное лицо за организацию обработки персональных данных, Администратор информационной безопасности и члены Комиссии по обеспечению безопасности персональных данных должны быть ознакомлены с настоящим Положением.

1.6. Ознакомление с настоящим Положением должно подтверждаться подписью работника в Листе ознакомления.

2.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Положении используются следующие термины и определения:

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

Персональные данные, разрешенные субъектом персональных данных для распространения - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном законодательством Российской Федерации;

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;

Обработка персональных данных - любое действие (операция) 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 персональных данных;

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;

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;

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;

Контролируемая зона - границы пространства (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

3.ОБРАБАТЫВАЕМЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРОМ

3.1. Цели обработки персональных данных Оператором, категории, перечень обрабатываемых Оператором персональных данных, категории субъектов, персональные данные которых обрабатываются Оператором, способы, сроки их обработки, правовое обоснование обработки персональных данных Оператором определены локальным актом «Перечень обрабатываемых персональных данных в СРО Ассоциации «НАКС»».

3.2. Форма Перечня обрабатываемых персональных данных в СРО Ассоциации «НАКС» представлена в Приложении №1 к настоящему Положению.

3.3. Перечень обрабатываемых персональных данных, указанный в п. 3.2. настоящего Положения, формируется в соответствии с потребностью реализации бизнес-процессов Оператора и утверждается Генеральным директором СРО Ассоциации «НАКС».

3.4. Перечень обрабатываемых персональных данных, указанный в п. 3.2. настоящего Положения, должен быть актуализирован и утвержден в новой редакции в случаях:

- изменение целей обработки персональных данных;
- изменение категорий и перечня персональных данных;
- изменение категорий субъектов персональных данных;
- изменение способов обработки персональных данных;
- изменение сроков обработки персональных данных;
- изменение правового обоснования обработки персональных данных.

3.5. В случае актуализации Перечня обрабатываемых персональных данных, указанный в п. 3.2. настоящего Положения, соответствующие изменения должны быть внесены в Политику

в отношении обработки персональных данных в СРО Ассоциации «НАКС», а также в Уведомление уполномоченного органа по защите прав субъектов персональных данных.

3.6. Требования к срокам хранения и порядок уничтожения персональных данных субъектов персональных данных, в соответствии с Приказом Роскомнадзора от 28.10.2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных», установлены локальным актом Оператора «Порядок хранения и уничтожения персональных данных в СРО Ассоциации «НАКС»».

4. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Оператор при обработке персональных данных придерживается следующих принципов:

- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей, не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки;
- обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- принимаются необходимые меры по удалению или уточнению неполных или неточных данных;
- хранение персональных данных осуществляется 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.

5. ОСНОВНЫЕ УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Обработка персональных данных Оператором допускается случаях, установленных пунктом 1 статьи 6 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных», том числе:

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

- обработка персональных данных 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 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;

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

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

5.2. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев установленных пунктом 2 статьи 10 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных, в том числе:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

- персональные данные сделаны общедоступными субъектом персональных данных;

- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно, и в связи с осуществлением правосудия;

- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

5.3. Письменное согласие субъекта персональных данных должно включать:

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

- 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);
- наименование или фамилию, имя, отчество и адрес Оператора;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных»;
- подпись субъекта персональных данных.

5.4. Форма письменного согласия на обработку персональных данных представлена в Приложении №3 к настоящему Положению.

5.5. Обработка биометрических персональных данных Оператором не осуществляется.

5.6. Оператор не создает общедоступные источники персональных данных.

5.7. Оператор не осуществляет трансграничную передачу персональных данных.

5.8. Условия распространения персональных данных и передачи персональных данных третьим лицам, в соответствии со статьей 6 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных», установлены локальным актом Оператора «Порядок распространения и передачи персональных данных третьим лицам в СРО Ассоциации «НАКС»».

5.9. Оператор осуществляет обработку персональных данных как с использованием средств автоматизации, так и без использования средств автоматизации.

6. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРОМ, ОСУЩЕСТВЛЯЕМАЯ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

6.1. Требования к обработке персональных данных, осуществляемой без использования средств автоматизации установлены пунктом 3 статьи 4 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных» и Постановлением Правительства РФ от 15.09.2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6.2. Требования нормативных актов, указанных в пункте 6.1. настоящего Положения, отражены Оператором во локальном акте «Положение об особенностях обработки персональных данных СРО Ассоциацией «НАКС», осуществляемой без использования средств автоматизации».

6.3. Локальный акт «Положение об особенностях обработки персональных данных СРО Ассоциацией «НАКС», осуществляемой без использования средств автоматизации» определяет

особенности организации Оператором обработки персональных данных субъектов персональных данных, осуществляемой без использования средств автоматизации и меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

7. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРОМ, ОСУЩЕСТВЛЯЕМАЯ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

7.1. Обработка персональных данных с использованием средств автоматизации осуществляется в рамках информационных систем персональных данных Оператора.

7.2. Состав информационных систем персональных данных Оператора определяется локальным актом «Перечень информационных систем персональных данных СРО Ассоциации «НАКС»», утверждаемым Генеральным директором СРО Ассоциации «НАКС». Форма Перечня информационных систем персональных данных представлена в Приложении №4 к настоящему Положению.

7.3. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется Оператором в соответствии с требованиями:

- Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 18.02.2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСБ России от 10.07.2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

8. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРА

8.1. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Оператора

8.1.1. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных осуществляется Оператором в соответствии с

методическим документом «Методика оценки угроз безопасности информации» (Утвержденным ФСТЭК России 5 февраля 2021 г.).

8.1.2. По результатам оценки, проведенной в соответствии с Методическим документом, указанным в пункте 8.1.1. настоящего Положения, Оператором выявлены актуальные угрозы безопасности информации, реализация (возникновение) которых может привести к нарушению безопасности обрабатываемой в системах и сетях информации (нарушению конфиденциальности, целостности, доступности, недоказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования систем и сетей.

8.1.3. По результатам оценки угроз безопасности информации Оператором разработаны и утверждены Модели угроз безопасности информации для каждой информационной системы персональных данных.

8.1.4. Оператором, в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», установлены уровни защищенности персональных данных при их обработке в информационных системах персональных данных Оператора в зависимости от угроз безопасности этих данных.

8.2. Организация режима обеспечения безопасности помещений Оператора, в которых размещены информационные системы персональных данных и ведется обработка персональных данных субъектов персональных данных

8.2.1. В рамках исполнения Оператором требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов Российской Федерации, Оператор определяет перечень помещений, в которых размещены информационные системы персональных данных и ведется обработка персональных данных субъектов персональных данных. Форма Перечня помещений представлена в Приложении №5 к настоящему Положению.

8.2.2. Помещения Оператора, в которых размещены информационные системы персональных данных и ведется обработка персональных данных субъектов персональных данных, соответствуют следующим требованиям:

- исключена возможность бесконтрольного проникновения в помещения, в которых размещены информационные системы персональных данных и ведется обработка персональных данных субъектов персональных данных, в том числе имеется стационарный пункт охраны, двери и окна имеют прочные и надежные петли, двери и окна имеют исправные замки, определен перечень лиц, имеющих доступ к информационным системам персональных данных;
- исключена возможность визуального просмотра обрабатываемых персональных данных субъектов персональных данных посторонними лицами, в том числе мониторы персональных компьютеров на которых осуществляется обработка персональных данных установлены таким образом, что исключают возможность визуального просмотра персональных данных субъектов персональных данных посторонними лицами.

8.2.3. Оператор определяет контролируемые зоны и утверждает приказом Генерального директора СРО Ассоциации «НАКС».

8.3. Обеспечение сохранности носителей персональных данных субъектов персональных данных

8.3.1. Требования к обеспечению сохранности бумажных носителей персональных данных субъектов персональных данных установлены Оператором в локальном акте «Положение об особенностях обработки персональных данных СРО Ассоциацией «НАКС», осуществляемой без использования средств автоматизации», разработанном в соответствии с Постановлением Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

8.3.2. В рамках исполнения Оператором требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов Российской Федерации, требования к обеспечению сохранности машинных носителей персональных данных субъектов персональных установлены Оператором в локальном акте «Регламент обращения с машинными носителями персональных данных субъектов персональных данных в СРО Ассоциации «НАКС»».

8.4. Доступ к персональным данным субъекта персональных данных, обрабатываемым в информационной системе персональных данных

8.4.1. В рамках исполнения Оператором требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов Российской Федерации, порядок предоставления, изменения и прекращения прав доступа работников Оператора (внутренних пользователей) и третьих лиц (внешних пользователей) к персональным данным, которые обрабатываются в информационных системах Оператора установлен Оператором в локальном акте «Регламент предоставления прав доступа к персональным данным субъектов персональных данных, содержащимся в информационных системах персональных данных в СРО Ассоциации «НАКС»».

8.4.2. Внутренние и внешние пользователи наделены минимально необходимыми правами доступа к информационным системам персональных данных Оператора.

8.4.3. Для доступа в информационные системы персональных данным Оператором организована идентификация и аутентификация внутренних и внешних пользователей.

8.4.4. Локальным актом Оператора «Инструкция по организации парольной защиты в СРО Ассоциации «НАКС»» установлены требования к генерации, смене, восстановлению и прекращению действия паролей, установлен порядок действий при компрометации пароля в информационных системах персональных данных.

8.5. Средства защиты информации в информационных системах персональных данных Оператора

8.5.1. В рамках исполнения Оператором требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов Российской Федерации, Оператор использует средства защиты информации, прошедшие

процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в том числе:

- Средства антивирусной защиты. (Требования к организации антивирусной защиты серверов и персональных компьютеров от воздействий компьютерных вирусов и другого вредоносного программного обеспечения и единый порядок оснащения средствами антивирусной защиты информационных систем персональных данных установлен локальным актом Оператора «Инструкция по антивирусной защите информации в информационных системах персональных данных СРО Ассоциации «НАКС»»);
- Средства защиты информации при ее передаче по каналам связи, в том числе по беспроводным каналам связи.

8.6. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных в информационных системах персональных данных

8.6.1. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится Оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

8.6.2. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится не реже одного раза в 3 года.

8.7. Обнаружение фактов несанкционированного доступа к персональным данным субъектов персональных данных и принятие мер по реагированию на несанкционированный доступ к персональным данным субъектов персональных

8.7.1. В рамках исполнения Оператором требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и Приказа ФСБ России от 13.02.2023 г. № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных», Оператором разработан локальный акт «Регламент по реагированию на инциденты информационной безопасности в СРО Ассоциации «НАКС»».

8.7.2. Локальный акт Оператора «Регламент по реагированию на инциденты информационной безопасности в СРО Ассоциации «НАКС»» определяет порядок реагирования на инциденты информационной безопасности, порядок проведения внутреннего расследования инцидента информационной безопасности, порядок взаимодействия с Национальным координационным центром по компьютерным инцидентам и порядок уведомления уполномоченного органа по защите прав субъектов персональных данных о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных.

8.8. Восстановление персональных данных субъектов персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним

8.8.1. В рамках исполнения Оператором требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов Российской Федерации, с целью восстановления персональных данных субъектов персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним Оператором осуществляется резервное копирование персональных данных субъектов персональных данных.

8.8.2. Правила и объемы резервного копирования, порядок восстановления персональных данных субъектов персональных данных субъектов персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним установлен локальным актом Оператора «Регламент резервного копирования и восстановления персональных данных субъектов персональных данных в СРО Ассоциации «НАКС»».

8.9. Осуществление внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации

8.9.1. В рамках исполнения Оператором требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов Российской Федерации, Оператор осуществляет внутренний контроль соответствия обработки персональных данных требованиям законодательства Российской Федерации.

8.9.2. Внутренний контроль соответствия обработки персональных данных Оператором требованиям законодательства Российской Федерации включает в себя:

- проверку соответствия локальных актов Оператора требованиям Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;
- проверку ознакомления работников Оператора с локальными актами Оператора по вопросам обработки и обеспечения безопасности персональных данных;
- проверку соблюдения работниками Оператора локальных актов Оператора по вопросам обработки и обеспечения безопасности персональных данных.

8.9.3. Периодичность и состав мероприятий по проведению внутреннего контроля обработки персональных данных определены Оператором локальным актом «Регламент внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации в СРО Ассоциации «НАКС»».

8.10. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

8.10.1. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» осуществляется Оператором в соответствии с Приказом Роскомнадзора от 27.10.2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных

данных».

8.10.2. Алгоритм оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» установлен Оператором локальным актом Оператора «Порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

8.11. Обучение работников Оператора, непосредственно осуществляющих обработку персональных данных субъектов персональных данных

8.11.1. Оператор, в соответствии с требованиями части 1 статьи 18.1. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», проводит обучение работников Оператора, непосредственно осуществляющих обработку персональных данных.

8.11.2. Обучение работников Оператора, непосредственно осуществляющих обработку персональных данных включает в себя:

- ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных;
- ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с политикой Оператора в отношении обработки персональных данных, локальными актами Оператора по вопросам обработки и защиты персональных данных.

8.11.3. Обучение работников Оператора, непосредственно осуществляющих обработку персональных данных, проводится в форме инструктажа:

- первичный инструктаж;
- внеплановый инструктаж.

8.11.4. Первичный инструктаж проводится при допуске работника Оператора к персональным данным.

8.11.5. Внеплановый инструктаж проводится в случаях:

- изменение локальных актов Оператора по вопросам обработки персональных данных;
- нарушение работником Оператора требований законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных;
- нарушение работником Оператора требований локальных актов Оператора по вопросам обработки и защиты персональных данных.

8.11.6. Программы инструктажей работников Оператора, непосредственно осуществляющих обработку персональных данных, утверждаются приказом Генерального директора СРО Ассоциации «НАКС».

8.11.7. Сведения о проведенном инструктаже заносятся в Журнал инструктажей работников СРО Ассоциации «НАКС», непосредственно осуществляющих обработку персональных данных.

8.11.8. Форма Журнала инструктажей работников СРО Ассоциации «НАКС», непосредственно осуществляющих обработку персональных данных приведена в Приложении №6 к настоящему Положению.

8.11.9. Работники, непосредственно осуществляющие обработку персональных данных у Оператора обязаны подписать обязательство о неразглашении персональных данных.

8.11.10. Форма Обязательства о неразглашении персональных данных. Представлена в Приложении №7 к настоящему Положению.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Во всем, что не урегулировано настоящим Положением, Оператор руководствуется действующим законодательством Российской Федерации.

9.2. Настоящее Положение должно быть пересмотрено в следующих случаях:

- при изменении законодательства Российской Федерации в области обработки и защиты персональных данных;
- в случаях получения предписаний от компетентных государственных органов на устранение несоответствий, затрагивающих область действия настоящего Регламента.

9.3. Все изменения в настоящее Положение утверждаются приказом Генерального директора СРО Ассоциации «НАКС».

10. ОТВЕТСТВЕННОСТЬ

Работники Оператора, независимо от занимаемых должностей, несут дисциплинарную ответственность и административную ответственность в соответствии с законодательством Российской Федерации за ненадлежащее исполнение или неисполнение требований настоящего Положения.

ПРИЛОЖЕНИЕ № 1 к Положению об обработке и обеспечении безопасности персональных данных в СРО Ассоциации «НАКС» от «___»_____ 20___года

УТВЕРЖДЕНО:

Генеральный директор
СРО Ассоциации «НАКС»

_____/_____/
подпись *расшифровка*

« _____ » _____ 20___ г.

ПЕРЕЧЕНЬ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ В СРО АССОЦИАЦИИ «НАКС»

1. Категория субъектов персональных данных – _____
(указать категорию субъектов персональных данных)

Состав персональных данных			**Общедоступные персональные данные**	**Цели обработки персональных данных**	**Правовое основание обработки персональных данных**	**Совершаемые действия (операции) с персональными данными**	**Срок обработки персональных данных**
Иные персональные данные, не являющиеся специальными или биометрическими	**Специальные персональные данные**	**Биометрические персональные данные**					

ПРИЛОЖЕНИЕ № 2 к Положению об обработке и обеспечении безопасности персональных данных в СРО Ассоциации «НАКС» от «___»_____ 20___года

СОГЛАСИЕ
на обработку персональных данных

Я, субъект персональных данных:

Фамилия Имя Отчество (при наличии)	
Адрес	
Наименование документа, удостоверяющего личность	
Номер документа, удостоверяющего личность	
Дата выдачи документа, удостоверяющего личность	
Орган, выдавший документ, удостоверяющего личность	

в соответствии с Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных», действуя по своей воле и в своих интересах, даю свое согласие на обработку моих персональных данных Саморегулируемой организации Ассоциации «Национальное Агентство Контроля и Сварки» (далее – СРО Ассоциация «НАКС»), (ИНН 7723367927, юридический адрес: 109341, г. Москва, ул. Братиславская, д. 6), с целью

_____.
(указать цель обработки персональных данных)

Перечень моих персональных данных, на обработку которых СРО Ассоциации «НАКС» дается согласие:

_____.
(указать перечень персональных данных)

Перечень действий с моими персональными данными, на совершение которых СРО Ассоциации «НАКС» дается согласие: _____.
(указать перечень действий с персональными данными)

Я предоставляю СРО Ассоциации «НАКС» право осуществлять обработку моих персональных данных _____.
(способ обработки)

Я даю право СРО Ассоциации «НАКС» передавать мои персональные данные _____.
(указать наименование третьего лица, ИНН, юр. адрес)

в соответствии с законодательством Российской Федерации, в рамках заключенного поручения, существенным условием которого является обеспечение безопасности персональных данных при их обработке и предотвращение разглашения моих персональных данных.

Настоящее согласие предоставляется мной с момента его подписания и действует до _____.

Настоящее согласие может быть отозвано мной при предоставлении в СРО Ассоциацию «НАКС» заявления в форме, установленной Политикой в отношении обработки персональных данных СРО Ассоциации «НАКС», размещенной на сайте СРО Ассоциации «НАКС» - https://naks.ru, либо в свободной форме, в соответствии с требованиями Законодательства Российской Федерации.

«_____»_____20_____г._____ /_____/
Дата *Личная подпись* *Расшифровка личной подписи*

ПРИЛОЖЕНИЕ № 3 к Положению об обработке и обеспечении безопасности персональных данных в СРО Ассоциации «НАКС» от «___»_____ 20___года

УТВЕРЖДЕНО:

Генеральный директор
СРО Ассоциации «НАКС»

_____/_____/
подпись *расшифровка*

« _____ » _____ 20___ г.

ПЕРЕЧЕНЬ

ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ в СРО АССОЦИАЦИИ «НАКС»

Наименование информационной системы персональных данных	**Категории обрабатываемых субъектов персональных данных**	**Категории обрабатываемых персональных данных**	**Объем обрабатываемых персональных данных**	**Наличие подключения к сетям международного обмена**	**Наличие подключения к внутренней сети**
1	**2**	**3**	**4**	**5**	**6**

ПРИЛОЖЕНИЕ № 4 к Положению об обработке и обеспечении безопасности персональных данных в СРО Ассоциации «НАКС» от «___»_____ 20___года

УТВЕРЖДЕНО:

Генеральный директор
СРО Ассоциации «НАКС»

_____/_____/
подпись *расшифровка*

« _____ » _____ 20___ г.

ПЕРЕЧЕНЬ

помещений, в которых размещены информационные системы персональных данных и ведется обработка персональных данных субъектов персональных данных

Наименование помещения, адрес местонахождения	**Категории обрабатываемых субъектов персональных данных**	**Категории обрабатываемых персональных данных**	**Лица, имеющие доступ в помещение**	**Перечень средств защиты помещения**
1	**2**	**3**	**4**	**5**

ПРИЛОЖЕНИЕ № 5 к Положению об обработке и обеспечении безопасности персональных данных в СРО Ассоциации «НАКС» от «___»_____ 20___года

ТИТУЛЬНАЯ СТРАНИЦА

ЖУРНАЛ

инструктажей работников СРО Ассоциации «НАКС», непосредственно осуществляющих обработку персональных данных

Начат _____
Окончен _____
Срок хранения_____

Ответственный за журнал:

_____
(должность, подпись, расшифровка)

Контактный телефон:
Место хранения журнала:
Журнал содержит ____ (_____) листа (-ов).

СОДЕРЖАНИЕ ЖУРНАЛА

№ п/п	Наименование инструктажа (первичный, внеплановый), номер программы инструктажа	Дата проведения инструктажа	Должность, ФИО работника, проводившего инструктаж	Подпись работника, проводившего инструктаж	Должность, ФИО работника, прошедшего инструктаж	Подпись работника, прошедшего инструктаж
1	2	3	4	5	6	7

ПРИЛОЖЕНИЕ № 6 к Положению об обработке и обеспечении безопасности персональных данных в СРО Ассоциации «НАКС» от «___»_____ 20___года

ОБЯЗАТЕЛЬСТВО О НЕРАЗГЛАШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,_____,
(Фамилия Имя Отчество (при наличии)

являясь работником СРО Ассоциации «НАКС» в соответствии с трудовым договором и локальными нормативными актами СРО Ассоциации «НАКС» понимаю, что во время исполнения своих обязанностей я осуществляю обработку персональных данных субъектов персональных данных, и добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам персональные данные субъектов персональных данных, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. Не передавать и не раскрывать третьим лицам персональные данные субъектов персональных данных, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

3. В случае попытки третьих лиц получить от меня персональные данные субъектов персональных данных, сообщать непосредственному руководителю.

4. Не использовать персональные данные субъектов персональных данных с целью получения выгоды.

5. Выполнять требования локальных нормативных актов СРО Ассоциации «НАКС», регламентирующих вопросы обработки персональных данных субъектов персональных данных.

6. В течение года после прекращения права на доступ к персональным данным субъектов персональных данных не разглашать и не передавать третьим лицам известные мне персональные данные субъектов персональных данных.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

«____»_____20___ года _____ /_____/
(дата) *(подпись)* *(расшифровка)*