УТВЕРЖДЕНО:
Приказом Директора
№ 27 от «16» ноября 2017 г.

_____ /А.В. Покатилов/

ПОЛОЖЕНИЕ
Об обработке Ассоциацией «СРО «РусЭнергоАудит» персональных данных и обеспечении их безопасности при обработке

г. Ярославль, 2017 г.

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией РФ, ФЗ от 12.01.1996 № 7-ФЗ «О некоммерческих организациях» (далее также – Закон о НКО), Трудовым кодексом РФ (далее также – ТК РФ), ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» (далее также – Закон о персональных данных), ФЗ от 01.12.2007 № 315-ФЗ «О саморегулируемых организациях» (далее также – Закон о СРО), ФЗ от 23.11.2009 № 261-ФЗ «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты РФ» (далее также – Закон об энергосбережении), Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом ФСБ России от 10.07.2014 № 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», Уставом Ассоциации «Саморегулируемая организация в области энергетического обследования «РусЭнергоАудит» (далее также – Ассоциация) в целях защиты прав и свобод физических лиц при обработке Ассоциацией их персональных данных.

1.2. Настоящее Положение определяет категории субъектов, персональные данные которых обрабатываются Ассоциацией, цели, основания и порядок обработки Ассоциацией персональных данных, устанавливает меры, принимаемые Ассоциацией для обеспечения безопасности персональных данных при их обработке.

1.3. Термины, относящиеся к обработке персональных данных и используемые в настоящем Положении, употребляются в значении, придаваемом им Законом о персональных данных, иными нормативными правовыми актами.

1.4. Обработка персональных данных осуществляется Ассоциацией в соответствии с принципами, изложенными в ст. 5 Закона о персональных данных, в объеме, соответствующем установленным разделом 2 настоящего Положения целям обработки персональных данных, с учетом требований нормативных правовых актов, определяющих объем данных, подлежащих обработке. Ассоциацией не осуществляется обработка персональных данных, указанных в ст. 11 Закона о персональных данных.

1.5. Обрабатываемые в соответствии с настоящим Положением персональные данные являются конфиденциальными (не подлежащими раскрытию третьим лицам без согласия субъекта персональных данных), если иное не предусмотрено федеральным законом.

1.6. Ассоциация осуществляет обработку персональных данных, имеющихся у Ассоциации, полученных непосредственно от субъекта персональных данных (его представителя), от третьих лиц, а также содержащихся в общедоступных источниках.

1.7. Права субъекта персональных данных и обязанности Ассоциации как оператора определяются в соответствии с главами 3 и 4 Закона о персональных данных.

2. Категории субъектов, персональные данные которых обрабатываются Ассоциацией, цели обработки персональных данных

2.1. Ассоциацией осуществляется обработка персональных данных следующих физических лиц:

2.1.1. лиц, вступивших в трудовые отношения с Ассоциацией (прекративших трудовые отношения, претендующих на трудоустройство);

2.1.2. лиц, входящих (входивших) в состав органов управления и специализированных органов Ассоциации;

2.1.3. членов Ассоциации (лиц, прекративших членство в Ассоциации, кандидатов на вступление в Ассоциацию), их работников (бывших работников); лиц, вступающих (находившихся, находящихся) в гражданско-правовые (трудовые) отношения с членами Ассоциации, работников (бывших работников) таких лиц, а также лиц, вступающих (находившихся, находящихся) в гражданско-правовые отношения с лицами, вступающими (находившимися, находящимися) в гражданско-правовые (трудовые) отношения с членами Ассоциации;

2.1.4. лиц, обращающихся в Ассоциацию с жалобами (обращениями), их представителей;

2.1.5. лиц, вступающих (находившихся, находящихся) в гражданско-правовые отношения с Ассоциацией, их представителей.

2.2. Обработка персональных данных лиц, указанных в п. 2.1.1 настоящего Положения, осуществляется в целях, предусмотренных п. 1 ст. 86 ТК РФ.

2.3. Обработка персональных данных лиц, указанных в п. 2.1.2 настоящего Положения, осуществляется в следующих целях:

2.3.1. избрание кандидатов в коллегиальные органы Ассоциации;

2.3.2. исполнение требований ч. 2 ст. 17 Закона об энергосбережении, п. 3 ч. 2 ст. 7 Закона о СРО, п. 3, 3.2 ст. 32 Закона о НКО, иных нормативных правовых предписаний, предусматривающих обязанность Ассоциации осуществлять обработку персональных данных соответствующих лиц.

2.4. Обработка персональных данных лиц, указанных в п. 2.1.3 настоящего Положения, осуществляется в следующих целях:

2.4.1. прием лица в члены Ассоциации;

2.4.2. проведение Общего собрания членов Ассоциации;

2.4.3. исполнение требований ч. 5.3 ст. 15, ч. 2 ст. 17 Закона об энергосбережении, п. 2, 8, 9, 10 ч. 1 ст. 6 Закона о СРО, иных нормативных правовых предписаний, предусматривающих обязанность Ассоциации осуществлять обработку персональных данных соответствующих лиц.

2.5. Обработка персональных данных лиц, указанных в п. 2.1.4 настоящего Положения, осуществляется в следующих целях:

2.5.1. проверка полномочий представителей при решении вопроса о принятии жалобы (обращения) к рассмотрению;

2.5.2. исполнение требований п. 2, 9 ч. 1 ст. 6 Закона о СРО, иных нормативных правовых предписаний, предусматривающих обязанность Ассоциации осуществлять обработку персональных данных соответствующих лиц.

2.6. Обработка персональных данных лиц, указанных в п. 2.1.5 настоящего положения, осуществляется в следующих целях:

2.6.1. проверка полномочий представителей лиц, с которыми Ассоциация вступает в гражданско-правовые отношения;

2.6.2. исполнение нормативных правовых предписаний, предусматривающих обязанность Ассоциации осуществлять обработку персональных данных соответствующих лиц.

2.7. Обработка персональных данных лиц, указанных в п. 2.1настоящего Положения, осуществляется также для:

2.7.1. достижения предусмотренных Уставом целей деятельности Ассоциации;

2.7.2. предоставления сведений, необходимых государственным органам (органам местного самоуправления) для исполнения возложенных на них обязанностей.

3. Основания обработки персональных данных

3.1. Обработка персональных данных в отношении лиц, указанных в п. 2.1.1-2.1.5 настоящего Положения, осуществляется на основании предписаний Конституции РФ, Закона о персональных данных, настоящего Положения.

Согласие на обработку персональных данных является основанием для их обработки, кроме случаев, указанных в п. 2-11 ч. 1 ст. 6, п. 2-10 ч. 2 ст. 10 Закона о персональных данных. Согласие должно отвечать требованиям, предъявляемым к нему ст. 9 Закона о персональных данных. В случае если в соответствии с требованиями федерального закона обработка персональных данных осуществляется с письменного согласия субъекта персональных данных, документ, содержащий согласие субъекта персональных данных, может быть составлен в произвольной форме, но с обязательным включением в него указанных в ч. 4 ст. 9 Закона о персональных данных реквизитов.

3.2. Основаниями обработки персональных данных лиц, указанных в п. 2.1.1 настоящего Положения, являются также предписания ТК РФ, ФЗ от 06.12.2011 № 402-ФЗ «О бухгалтерском учете», принятых в соответствии с ними нормативных правовых актов, регламентирующих обработку персональных данных.

3.3. Основаниями обработки персональных данных лиц, указанных в п. 2.1.2 настоящего Положения, являются также предписания Закона о НКО, Закона об энергосбережении, Закона о СРО, принятых в соответствии с ними нормативных правовых актов, регламентирующих обработку персональных данных.

3.4. Основаниями обработки персональных данных лиц, указанных в п. 2.1.3 настоящего Положения, являются также предписания Закона об энергосбережении, Закона о СРО, принятых в соответствии с ними нормативных правовых актов, регламентирующих обработку персональных данных.

3.5. Основаниями обработки персональных данных лиц, указанных в п. 2.1.4 настоящего Положения, являются также предписания Гражданского кодекса

Российской Федерации (далее – ГК РФ), Закона о СРО, принятых в соответствии с ними нормативных правовых актов, регламентирующих обработку персональных данных.

3.6. Основаниями обработки персональных данных лиц, указанных в п. 2.1.5 настоящего Положения, являются также предписания ГК РФ.

4. Общие положения о порядке обработки персональных данных. Передача и хранение персональных данных

4.1. Обработка персональных данных осуществляется Ассоциацией как с использованием средств автоматизации, так и без использования таких средств (смешанная обработка).

4.2. Право на обработку персональных данных предоставляется работникам Ассоциации при условии ознакомления лица, получающего право на обработку персональных данных, под роспись с настоящим Положением, включения такого лица в Перечень лиц, доступ которых к персональным данным, обрабатываемым Ассоциацией, необходим для выполнения ими трудовых обязанностей (Приложение № 1).

4.3. При передаче персональных данных должен соблюдаться режим конфиденциальности информации.

4.4. Передача персональных данных в пределах Ассоциации осуществляется с соблюдением требований, установленных настоящим Положением, и только лицам, управомоченным на обработку персональных данных, в объеме, необходимом для совершения определенного действия (операции).

4.5. Передача персональных данных представителю субъекта персональных данных осуществляется в объеме, соответствующем объему его полномочий и необходимом для их исполнения.

4.6. Трансграничная передача персональных данных Ассоциацией не осуществляется.

4.7. Хранение персональных данных, содержащихся как на бумажных, так и на электронных носителях, осуществляется в помещениях Ассоциации. Персональные данные, содержащиеся на бумажном (электронном) носителе, могут быть воспроизведены соответственно на электронном (бумажном) носителе.

5. Меры по обеспечению безопасности персональных данных при их обработке

5.1. В целях обеспечения безопасности персональных данных при их обработке Ассоциацией принимаются в том числе следующие меры:

5.1.1. утверждение Директором Ассоциации документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым Ассоциацией, необходим для выполнения ими трудовых обязанностей;

5.1.2. организация режима обеспечения безопасности помещений, в которых размещены носители персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

5.1.3. обеспечение сохранности носителей, содержащих персональные данные, организация их хранения и контроля за обращением;

5.1.4. назначение лица, ответственного за организацию обработки персональных данных;

5.1.5. обеспечение восстановления персональных данных, уничтоженных или измененных вследствие несанкционированного доступа к ним либо при отсутствии к тому основания;

5.1.6. определение мест, в которых осуществляется обработка персональных данных;

5.1.7. оценка эффективности принимаемых мер по обеспечению безопасности персональных данных при их обработке;

5.1.8. ознакомление работников, уполномоченных на обработку персональных данных, с положениями нормативных правовых актов, регламентирующих обработку персональных данных;

5.1.9. определение угроз безопасности персональных данных при их обработке;

5.1.10. обнаружение фактов несанкционированного доступа к персональным данным;

5.1.11. контроль за принимаемыми мерами безопасности персональных данных.

5.2. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных Ассоциации с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, помимо мер, перечисленных в п. 5.1.1-5.1.11 настоящего Положения, входят:

5.2.1. идентификация и аутентификация пользователей, являющихся работниками Ассоциации; управление идентификаторами, управление средствами аутентификации; защита обратной связи при вводе аутентификационной информации; идентификация и аутентификация внешних пользователей;

5.2.2. управление учетными записями пользователей; реализация необходимых методов, типов и правил разграничения доступа; управление информационными потоками между устройствами, сегментами информационной системы; разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы; назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы; ограничение неуспешных попыток доступа к информационной системе; реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети; регламентация и контроль использования в информационной системе технологий беспроводного доступа; регламентация и контроль использования в системе мобильных технических средств; управление взаимодействием с внешними информационными системами;

5.2.3. регистрация событий безопасности, в том числе определение событий безопасности, подлежащих регистрации, и сроков их хранения; определение состава и содержания информации о событиях безопасности, подлежащих регистрации; сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения; защита информации о событиях безопасности;

5.2.4. реализация антивирусной защиты; обновление базы данных признаков вредоносных компьютерных программ (вирусов);

5.2.5. контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

5.2.6. идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации; управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

5.2.7. размещение устройств вывода информации, исключающее ее несанкционированный просмотр;

5.2.8. обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;

5.2.9. обеспечение целостности информационной системы и персональных данных;

5.2.10. обеспечение доступности персональных данных;

5.2.11. управление конфигурацией информационной системы и системы защиты персональных данных.

5.3. Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения содержащих их носителей и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

6. Заключительные положения

6.1. Настоящее Положение вступает в силу с момента его утверждения и действует в течение неопределенного срока.

6.2. Изменение настоящего Положения, признание его утратившим силу осуществляется Директором Ассоциации.

В настоящем документе прошито,
пронумеровано, скреплено печатью
9 (девять) листа(ов)

«16» ноября 2017 г.

Директор Ассоциации «СРО «РусЭнергоАудит»

_____А.В. Покатилов