НАЦИОНАЛЬНЫЙ СОВЕТ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ПРОФЕССИОНАЛЬНЫМ КВАЛИФИКАЦИЯМ

СОВЕТ ПО ПРОФЕССИОНАЛЬНЫМ КВАЛИФИКАЦИЯМ
В ОБЛАСТИ УПРАВЛЕНИЯ ПЕРСОНАЛОМ

У Т В Е Р Ж Д Е Н О
решением Совета
по профессиональным квалификациям
в области управления персоналом

Протокол от 17 октября 2018 г. № 21

Политика
по защите персональных данных

г. Москва
2018 год

1. Общие положения.

1.1. Совет по профессиональным квалификациям в области управления персоналом при Национальном Совете по профессиональным квалификациям при Президенте РФ, далее «Совет», являясь оператором обработки персональных данных, осуществляет работу с персональными данными:

- членов Совета (Субъекта персональных данных),
- членов рабочих групп и комиссий,
- привлекаемых к работе Совета экспертов,
- представителей и экспертов кандидатов на аккредитацию в качестве центра оценки квалификации,
- соискателей, обратившихся за прохождением профессиональных экзаменов,
- лиц, сдавших профессиональные экзамены
- и иных лиц – далее «Субъект персональных данных», чьи данные Совет обрабатывает согласно норм действующего законодательства, регулирующих систему профессиональных квалификаций.

1.2. Совет в своей деятельности руководствуется соответствующими нормами Конституции РФ (Российской Федерации), Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», а также общепризнанными принципами и нормами международного права и международных договоров РФ, которые в соответствии с частью четвертой ст. 15 Конституции РФ являются составной частью российской правовой системы.

1.3. Целью данной Политики по защите персональных данных (далее - Положение) является защита персональных данных от несанкционированного доступа третьих лиц и организация приема, хранения, обработки и передачи персональных данных Субъекта персональных данных в соответствии с установленными законодательными требованиями.

1.4. Сбор, хранение, использование и распространение информации о частной жизни Субъекта персональных данных без его письменного согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законодательством РФ.

1.5. Порядок утверждения данных правил, ввода их в действие и внесения изменений утверждается Решением Совета.

2. Понятие и состав персональных данных.

2.1. Понятие персональных данных:

- Персональные данные — любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (Субъекту персональных данных), необходимая Совету в связи с выполнением порученных ему функций, или полученная им на основании письменного согласия Субъекта персональных данных. Это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (Субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Если по совокупности сведений определить их принадлежность конкретному Субъекту невозможно, то данные сведения не относятся к персональным данным.
- 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.

- Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении Субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы Субъекта персональных данных или других лиц.
- Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.
- Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.
- Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному Субъекту персональных данных.
- Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.
- Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия Субъекта персональных данных или наличия иного законного основания;
- Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;
- Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия Субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
- Представители Субъекта персональных данных - лица, выступающие в качестве законного представителя в соответствии с нормами гражданского и семейного законодательства.

3. Сбор, обработка и хранение персональных данных.

3.1. Порядок получения персональных данных.

3.1.1. Все персональные данные Субъекта персональных данных следует получить у него самого. Если персональные данные Субъекта персональных данных можно получить только у третьей стороны, то Субъектперсональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Совет должен сообщить такому Субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Субъекта персональных данных дать письменное согласие на их получение.

3.1.2. Совет не имеет права получать и обрабатывать персональные данные Субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ Совет вправе получать и обрабатывать данные о частной жизни Субъекта персональных данных

только с его письменного согласия.

3.1.3. Совет вправе обрабатывать персональные данные Субъекта персональных данных только с его письменного согласия.

Письменное согласие Субъекта персональных данных на обработку своих персональных данных должно включать в себя:

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) реквизиты Совета,

4) цель обработки персональных данных;

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

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

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

8) срок, в течение которого действует согласие Субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись Субъекта персональных данных.

3.1.4. Согласие Субъекта персональных данных не требуется в случаях если:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия Совета;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов Субъекта персональных данных, если получение его согласия невозможно.

3.2. Состав Членов Совета, допущенных к обработке, передаче и хранению персональной информации.

3.2.1. Полный доступ: к обработке персональных данных Субъекта персональных данных, исходя из функциональных обязанностей должностных лиц, имеют полный доступ следующие лица:

- Председатель Совета;
- руководители рабочих групп Совета;
- члены рабочих групп Совета.

3.2.2. Ограниченный доступ имеют иные лица, допущенные к персональным данным Субъекта персональных данных, если такой допуск требуется для выполнения функций Совета данным лицом. При этом ответственность за организацию допуска, ознакомление с установленными в Совете требованиями по защите персональных данных и контроль за соблюдением указанных требований и норм действующего законодательства лежит на руководителе рабочей группы Совета в рамках работы которой которых совершается допуск к персональным данным Субъекта персональных данных.

3.3. Порядок обработки, передачи и хранения персональной информации.

3.3.1. В соответствии с требованиями действующего законодательства в целях обеспечения прав и свобод человека и гражданина Совет и его Члены при обработке персональных данных Субъекта персональных данных должны соблюдать требования законодательства в части того, что обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, а также нормативных актов Совета.

3.3.2. В целях обеспечения защиты персональных данных, хранящихся у Совета, Субъекты персональных данных имеют право:

- на полную информацию об их персональных данных и обработке этих данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Субъекта персональных данных, за исключением случаев, предусмотренных федеральным законом;
- на определение своих представителей для защиты своих персональных данных;
- на доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;
- на требование об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства. При отказе Совета исключить или исправить персональные данные Субъекта персональных данных он имеет право заявить в письменной форме Совету о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера Субъект персональных данных имеет право дополнить заявлением, выражающим его собственную точку зрения;
- на требование об извещении Советом всех лиц, которым ранее были сообщены неверные или неполные персональные данные Субъекта персональных данных, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- на обжалование в суде любых неправомерных действий или бездействия Совета при обработке и защите его персональных данных.

3.4. Ответственность за разглашение.

3.4.1. Все лица, непосредственно имеющие отношение к персональной базе данных, должны подписывать обязательство о неразглашении персональных данных информации Субъекта персональных данных, в виде ознакомления с данным Положением под роспись.

3.4.2. Персональная ответственность — одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

3.4.3. Руководитель рабочей группы, Председатель Совета, разрешающий доступ Субъекта персональных данных к конфиденциальному документу, несет персональную ответственность за данное разрешение.

3.4.4. Каждый Субъект персональных данных, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

3.4.5. Ответственность лиц, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных Субъекта персональных данных, согласно действующему законодательству, может быть дисциплинарной, административной, гражданско-правовой или уголовной в соответствии с федеральными законами.

4. Доступ к персональным данным Субъектов.

4.1. Внутренний доступ.

4.1.1. Право доступа к персональным данным Субъекта персональных данных, имеют лица, указанные в п.3.2. данного положения. Другие Члены Совета имеют доступ к персональным данным Субъекта только с письменного согласия самого Субъекта персональных данных.

4.1.2. По письменному заявлению Субъекта персональных данных Совет обязан не позднее трех рабочих дней со дня подачи этого заявления выдать Субъекту персональных данных копии документов, связанных с его деятельностью, содержащие сведения о его Персональных данных. Указанные документы, должны быть заверены надлежащим образом и предоставляться Субъекта персональных данных безвозмездно.

4.2. Внешний доступ.

4.2.1. К числу лиц, допущенных к персональным данным Субъекта персональных данных, относятся организации (и соответственно должностные лица, данных организаций), осуществляющие контрольные и надзорные функции, а также вышестоящие органы управления и сопровождения системы профессиональных квалификаций, в соответствии с федеральными законами, в частности:

- Национальный Совет при Президенте РФ по профессиональным квалификациям;
- Национальное Агентство развития квалификаций;
- Министерство труда и занятости населения;
- Министерство образования;
- И др.

4.2.3. Органы и должностные лица, указанные в п.4.2.1, имеют доступ к информации только в сфере своей компетенции, в порядке, установленном законодательством РФ.

4.2.4. Организации, в которые Субъект персональных данных может осуществлять перечисления денежных средств, могут получить доступ к персональным данным Субъекта персональных данных только в случае письменного разрешения Субъекта персональных данных.

4.2.5. Сведения о Субъекте персональных данных могут быть предоставлены третьему лицу только на основании письменного запроса, оформленного на бланке организации, с приложением копии нотариально заверенного заявления Субъекта персональных данных, содержащего согласие на передачу указанным лицам таких сведений, с полным указанием того, какие сведения могут быть переданы на основании данного согласия.

5. Мероприятия по защите персональных данных.

5.1. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

5.2. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Общества.

5.3. Источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения, являются

субъекты, действия которых нарушают регламентируемые в информационной системе персональных данных правила разграничения доступа к информации.

5.4. Этими Субъектами могут быть:

- нарушитель;
- носитель вредоносной программы;
- аппаратная закладка.

Под нарушителем понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах.

5.5. Внутренняя защита.

5.5.1. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации.

Для защиты персональных данных Субъектов персональных данных Совет принимает следующие меры:

- ограничение и регламентация состава Члена Советов, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между рабочими группами, комиссиями, экспертами, Членами Совета;
- знание Субъектом персональных данных требований нормативно - методических документов по защите информации и сохранении тайны. Для этого со всеми Членами Совета, и иными лицами, допущенными к персональным данным, проводится при допуске и периодически соответствующий инструктаж и обучение;
- наличие необходимых условий, исключающих несанкционированный доступ в помещения для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава лиц, имеющих право доступа (входа) в помещение, в котором находятся персональные данные на бумажных носителях и вычислительной технике.
- организация порядка уничтожения информации. Способ уничтожения определяется специальной комиссией, создаваемой по решению Совета.
- воспитательная и разъяснительная работа с лицами, допущенными к обработке персональных данных по предупреждению утраты ценных сведений при работе с конфиденциальными документами. Данная обязанность возложена на руководителей рабочих групп Совета, в подчинении которых находятся лица, допущенные к персональным данным.

5.5.2. Защита персональных данных Субъекта персональных данных на электронных носителях: все папки, содержащие персональные данные Субъекта персональных данных, защищены паролем.

5.5.3. Защита персональных данных на бумажных носителях: все документы, содержащие персональные данные Субъекта персональных данных, хранятся либо у Председателя Совета, его заместителя, либо у Ответственного секретаря, либо у руководителя соответствующей рабочей группы Совета, в специально отведенном для этого месте, с применением специального оборудования (металлические несгораемые шкафы, сейфы, запираемые шкафы, к которым исключен несанкционированный доступ).

5.5.4. Ключи от специального оборудования в рабочее время хранятся у ответственных за сохранность указанных данных лиц без права передачи третьим лицам.

5.5. Внешняя защита.

5.5.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности.

5.5.2. Для защиты персональных данных Субъекта персональных данных Совет предпринимает следующие меры:

- порядок приема, учета и контроля документов, содержащих персональные данные Субъекта;
- в случае необходимости прохождения третьих лиц, в помещения, в которых хранятся персональные данные Субъекта, должен соблюдаться пропускной режим.
- использование технических средств охраны, сигнализации.
- обеспечение охраны территории, зданий, помещений, транспортных средств.

6. Информационные системы.

6.1. Совет использует следующие информационные системы (каждые отдельно или в совокупности):

- Информационная система, обрабатывающая биометрические персональные данные (в которой обрабатываются сведения, которые характеризуют физиологические и биологические особенности Субъекта персональных данных, на основании которых можно установить его личность и которые используются Советом для установления личности Субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных).
- Информационная система, обрабатывающая общедоступные персональные данные (в которой обрабатываются персональные данные Субъектов персональных данных, полученные только из общедоступных источников персональных данных).
- Информационная система, обрабатывающая персональные данные Субъекта персональных данных. (в которой обрабатываются персональные данные только Субъекта персональных данных).

6.2. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

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

6.4. Для обеспечения безопасности информационных систем Советом предпринимается следующая система защиты:

- Обеспечение безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- Назначение ответственного лица за обеспечение безопасности;
- Обеспечение сохранностей носителей персональных данных, при помощи установления паролей и блокировок;
- Обеспечение средствами антивирусной защиты;

- Тестирование информационной системы на проникновения.

7. Заключительные положения.

7.1. Настоящее Положение по защите персональных данных Субъектов персональных данных вступает в силу с момента его утверждения Советом и действует до введения нового Положения по защите персональных данных.

7.2. Ознакомление Субъектов персональных данных с условиями настоящего Положения производится путем публичного размещения данного Положения в общедоступном месте на сайте Совета.

7.3. Ознакомление Членов Совета и лиц, допущенных к персональным данных Субъектов персональных данных осуществляется под расписку в листе ознакомления, являющемся неотъемлемой частью настоящего Положения по защите персональных данных.

7.4. Подпись Члена Совета и лиц, допущенных к персональным данным Субъектов в листе ознакомления с Положением по защите персональных данных означает его согласие на выполнение требований данного Положения и соблюдение требований законодательства о защите персональных данных, и обязательство исполнения данного Положения в рамках тех задач и функций, которые лицо, допущенное к персональным данным осуществляет.

7.5. Персональную ответственность за соблюдение законодательства по защите персональных данных членами Совета и иными лицами, допущенными к персональным данным Субъектов несет Председатель Совета и руководители рабочих групп в рамках их полномочий по обработке персональных данных субъектов.

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Положение по защите персональных данных состоит из 10л., включая 2 пронумерованных листа ознакомления.