

Ассоциация «Федерация профессиональных коучей и наставников»
ИНН: 7842203004, ОГРН: 1227800059068

Утверждено:
Председатель Президиума
Ассоциации «Федерация профессиональных
коучей и наставников»



О.В. Рыбина

г. Санкт-Петербург

«01» октября 2025 г.

ПОЛОЖЕНИЕ
о защите персональных данных

1. Общие положения

1.1. Положение о защите персональных данных Ассоциации «Федерация профессиональных коучей и наставников» ИНН: 7842203004, ОГРН: 1227800059068 (далее – Ассоциация, Оператор, Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами в области защиты персональных данных, действующими на территории РФ (далее – Закон 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. Положение действует в отношении всех персональных данных, которые обрабатывает Оператор.

1.3. Положение распространяется на отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящего Положения.

1.4. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных настоящее Положение публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на сайте Оператора.

1.5. Цель настоящего Положения – защита персональных данных сотрудников, клиентов, контрагентов, членов Ассоциации и пользователей сайта <https://procoach.ru/> от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

1.6. Настоящее Положение утверждается Президиумом Ассоциации во главе с Председателем Президиума, вводится в действие приказом Исполнительного директора Ассоциации и является обязательным для исполнения всеми членами Ассоциации, имеющими доступ к персональным данным членов Ассоциации.

2. Термины и принятые сокращения

Ассоциация – Ассоциация «Федерация профессиональных коучей и наставников» ИНН: 7842203004, ОГРН: 1227800059068.

Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных). Перечень персональных данных, обрабатываемых Оператором, указан в Положении о работе с персональными данными клиентов, контрагентов, пользователей сайта и членов

Ассоциации, Положении о работе с персональными данными работников, Политике обработки персональных данных

Персональные данные, разрешенные субъектом персональных данных для распространения – это 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.

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 (предоставление, доступ);
- распространение;
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

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

Неавтоматизированная обработка персональных данных – обработка персональных данных без помощи средств вычислительной техники (вручную).

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

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному 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.

Защита персональных данных – деятельность, направленная на предотвращение утечки защищаемых персональных данных, несанкционированных и непреднамеренных воздействий на защищаемые персональные данные.

Высший орган управления Ассоциации – общее собрание членов Ассоциации.

Президиум Ассоциации – постоянно действующий коллегиальный орган управления Ассоциации.

Исполнительный директор Ассоциации – единоличный исполнительный орган Ассоциации.

Член Ассоциации – полностью дееспособные физические лица.

Прочие термины и сокращения приводятся согласно действующему законодательству Российской Федерации.

3. Порядок и условия обработки и хранение персональных данных

3.1. Обработка персональных данных осуществляется Оператором в соответствии с Положением о работе с персональными данными клиентов, контрагентов, пользователей сайта и членов Ассоциации, Положением о работе с персональными данными работников, Политикой обработки персональных данных, а также требованиями законодательства Российской Федерации.

3.2. Хранение, использование, в том числе цели использования, порядок распространение персональных данных осуществляется в соответствии с Положением о работе с персональными данными клиентов, контрагентов, пользователей сайта и членов Ассоциации, Политикой обработки персональных данных и Положением о работе с персональными данными работников, утвержденными Оператором.

3.3. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Социальный фонд и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

3.4. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

3.5. Во всем ином, что не предусмотрено настоящим Положением, Оператор руководствуется Политикой обработки персональных данных, утвержденной Оператором и размещенной на сайте Оператора.

4. Защита персональных данных

4.1. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

- определяет угрозы безопасности персональных данных при их обработке;
- принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;
- назначает лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Оператора; осуществляющих организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением Оператором требований к защите персональных данных;
- создает необходимые условия для работы с персональными данными;
- организует учет документов, содержащих персональные данные;
- организует работу с информационными системами, в которых обрабатываются персональные данные;
- хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;
- организует обучение работников Оператора, осуществляющих обработку персональных данных;
- устанавливает индивидуальные пароли доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

- применяет прошедшие в установленном порядке процедуру оценки соответствия средств защиты информации;
- использует сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;
- обеспечивает соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;
- обеспечивает обнаружение фактов несанкционированного доступа к персональным данным;
- осуществляет восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обеспечивает изучение работниками, непосредственно осуществляющими обработку персональных данных, положений законодательства РФ о персональных данных, в том числе требований к защите персональных данных, документов, определяющих политику Оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных;
- осуществляет внутренний контроль и аудит.

4.2. Угрозы защищенности персональных данных:

4.2.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.

4.2.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах работников.

4.2.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

4.3. Уровни защищенности персональных данных (далее – ПД):

4.3.1. Первый уровень защищенности. Если Оператор отнес информационную систему к первому типу угрозы или если тип угрозы второй, но Оператор обрабатывает специальные категории ПД более 100 тыс. физических лиц без учета работников.

4.3.2. Второй уровень защищенности. Если тип угрозы второй и Оператор обрабатывает специальные категории ПД субъектов персональных данных, вне зависимости от их количества, или специальные категории ПД менее чем 100 тыс. физических лиц, или любые другие категории ПД более чем 100 тыс. физических лиц, или при третьем типе угрозы Оператор обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

4.3.3. Третий уровень защищенности. Если при втором типе угрозы Оператор обрабатывает общие ПД субъектов персональных данных или менее чем 100 тыс. физических лиц, или при третьем типе угрозы Оператор обрабатывает специальные категории ПД субъектов или менее чем 100 тыс. физических лиц, или при третьем типе угрозы Оператор обрабатывает биометрические ПД, или при третьем типе угрозы Оператор обрабатывает общие ПД более чем 100 тыс. физических лиц.

4.3.4. Четвертый уровень защищенности. Если при третьем типе угрозы Оператор обрабатывает только общие ПД субъектов персональных данных или менее чем 100 тыс. физических лиц.

4.4. При четвертом уровне защищенности персональных данных Оператор:

- обеспечивает режим безопасности помещений, в которых размещается информационная система;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных до ПД субъектов персональных данных;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

4.5. При третьем уровне защищенности ПД дополнительно к мерам, перечисленным в пункте 4.4 настоящего Положения, Оператор назначает ответственного за обеспечение безопасности ПД в информационной системе.

4.6. При втором уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 4.4, 4.5 настоящего Положения, Оператор ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

4.7. При первом уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 4.4 - 4.6 настоящего Положения, Оператор:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к ПД в системе;
- создает отдел, ответственный за безопасность ПД в системе, либо возлагает такую обязанность на один из существующих отделов.

4.8. В целях защиты ПД на бумажных носителях Оператор:

- приказом назначает ответственного за обработку ПД;
- ограничивает допуск в помещения, где хранятся документы, которые содержат ПД субъектов персональных данных;
- хранит документы, содержащие ПД субъектов персональных данных в шкафах, запирающихся на ключ.

4.9. В целях обеспечения конфиденциальности документы, содержащие ПД субъектов персональных данных, оформляются, ведутся и хранятся только работниками Оператора, утвержденными приказом исполнительного директора.

4.10. Работники, указанные в п.4.9 настоящего Положения, допущенные к ПД субъектов ПД, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки ПД не допускаются.

4.11. В соответствии с требованиями нормативных документов Оператором создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

4.12. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

4.13. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами.

4.14. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПД.

5. Защита персональных данных члена Ассоциации

5.1. Защита персональных данных члена Ассоциации от неправомерного их использования или утраты обеспечивается Ассоциацией за счет собственных средств и в порядке, установленном законодательством РФ.

5.2. Внутренняя защита.

5.2.1. Для обеспечения внутренней защиты персональных данных членов Ассоциации, Ассоциация обязуется соблюдать следующие меры:

- ограничить и регламентировать состав членов Ассоциации, функциональные обязанности которых требуют конфиденциальных знаний;
- избирательно и обоснованно распределить доступ к документам и информации между членами Ассоциации и членами иных созданных или учрежденных органов Ассоциации;
- контролировать знание членами Ассоциации требований нормативно – методических документов по защите информации и сохранению тайны;
- организовать порядок уничтожения персональных данных;
- своевременно выявлять нарушения требований разрешительной системы доступа членам Ассоциации и членами иных созданных или учрежденных органов Ассоциации.

5.2.2. Защита персональных данных членов Ассоциации на электронных носителях. Информационные базы и иные вычислительные комплексы, используемые Ассоциацией и содержащие персональные данные членов Ассоциации, должны быть защищены паролем.

5.3. Внешняя защита.

5.3.1. Для обеспечения внешней защиты персональных данных применяются меры, препятствующие несанкционированному доступу к информации. 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.

5.3.2. Под посторонним понимается лицо, не имеющее непосредственного отношения к деятельности Ассоциации, посетители, члены других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в Ассоциации.

5.4. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных членов Ассоциации.

5.5. По возможности персональные данные обезличиваются.

6. Заключительные положения

6.1. Ответственность за нарушение требований законодательства Российской Федерации и нормативных документов Оператора в области персональных данных определяется в соответствии с законодательством Российской Федерации.

6.2. Все работники и члены Ассоциации, осуществляющие обработку ПД, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Положением, требованиями законодательства РФ.

6.3. Субъект персональных данных вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

6.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

6.5. Порядок актуализации, исправления, удаления и уничтожения персональных данных, выдачи ответов на запросы субъектов на доступ к персональным данным указаны в локальных нормативных правовых актах о персональных данных Оператора, а также в Политике обработки персональных данных, размещенной на сайте.

6.6. Настоящее Положение вступает в силу с момента утверждения и действует бессрочно до принятия новой редакции Положения.