

Приложение № 1
к приказу Фонда «Росконгресс»
от «29» января 2024 г. № СИНВ 2024/П/4

ПОЛОЖЕНИЕ

**определяющее политику обработки и защиты персональных данных в
информационной системе Форума «Сильные идеи для нового времени»**

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение определяет политику обработки и защиты персональных данных при проведении Форума «Сильные идеи для нового времени» (далее – Положение, Мероприятие), определяет принципы, цели, условия, сроки и способы обработки персональных данных (далее – ПДн), перечень категорий субъектов ПДн, перечень действий, осуществляемых с ПДн субъектов, права субъектов ПДн, мероприятия по контролю за соблюдением требований законодательства Российской Федерации в отношении обработки ПДн, а также меры по защите ПДн.

1.2. Настоящее Положение разработано с учетом требований следующих законодательных и нормативных правовых актов Российской Федерации, а также локальных нормативных актов Фонда «Росконгресс» (далее – Фонд) в области персональных данных:

- Конституции Российской Федерации;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

— Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

— Приказа 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»;

— Политики Фонда в области обработки персональных данных.

1.3. Настоящее Положение является методическим документом и может быть использовано для:

— организации процесса обработки ПДн в соответствии с требованиями действующего законодательства;

— выработки мер по своевременному обнаружению фактов несанкционированного доступа (далее – НСД) к ПДн и определения мероприятий по предотвращению НСД к ПДн;

— организации контроля за обеспечением установленного уровня защищенности ПДн.

1.4. Ответственность за соблюдение требований законодательства Российской Федерации и локальных нормативных актов Фонда в области ПДн несет Директор Фонда.

1.5. Настоящее Положение является обязательным для исполнения должностными лицами при решении задач обеспечения обработки и безопасности ПДн.

2 ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Положении используются следующие термины и определения:

— информация – сведения (сообщения, данные) независимо от формы их представления;

— документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими

определить такую информацию или ее материальный носитель;

— персональные данные – любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

— конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

— 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), 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), 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;

— 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;

— 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.

3 ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Принципы обработки персональных данных

3.1.1 Обработка ПДн осуществляется на законной и справедливой основе.

3.1.2 Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Обработка ПДн, несовместимая с целями сбора ПДн, не допускается.

3.1.3 Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

3.1.4 Обработке подлежат только ПДн, которые отвечают целям их обработки.

3.1.5 Содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки. Обрабатываемые ПДн не являются избыточными по отношению к заявленным целям их обработки.

3.1.6 При обработке ПДн обеспечивается точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Фонд принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

3.1.7 Хранение ПДн осуществляется в форме, позволяющей определить субъект ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом или договором, стороной которого, выгодоприобретателем или поручителем, по которому, является субъект ПДн.

3.1.8 Обрабатываемые ПДн уничтожаются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено

федеральным законом.

3.1.9 ПДн не раскрываются третьим лицам и не распространяются без согласия субъекта ПДн, если иное не предусмотрено федеральными законами.

3.2 Цели обработки персональных данных

Обработка ПДн при проведении Мероприятия осуществляется в целях:

- обеспечения соблюдения законодательных и нормативных правовых актов Российской Федерации;
- подготовки, заключения, исполнения и прекращения договоров с контрагентами;
- подготовки и проведения мероприятия;
- осуществления аккредитации, получения и активации аккредитационных документов участникам мероприятия;
- обеспечения требований безопасности, пропускного и внутриобъектового режимов на объектах проведения мероприятия;
- организации электронной записи на ПЦР-тестирование;
- формирования и ведения информационного ресурса;
- информационного и организационного сопровождения участников на этапе подготовки и проведения мероприятия;
- информирования о сроках и месте проведения мероприятия;
- организации гостиничного размещения, осуществления бронирования (резервирования) мест в объектах размещения, организации транспортного обслуживания участников мероприятия;
- выдачи товарно-материальных ценностей на площадках проведения мероприятия;
- предоставления статистической и персонифицированной отчетности по участникам мероприятия;
- получения визового сопровождения для въезда в страну.

3.3 Перечень субъектов персональных данных

В ходе проведения Мероприятия осуществляется обработка следующих категорий субъектов ПДн:

- сотрудники Фонда;
- сотрудники контрагентов;
- представители средств массовой информации (СМИ);
- организаторы;
- участники (посетители) мероприятия.

3.4 Перечень обрабатываемых персональных данных

Перечень обрабатываемых ПДн определяется в соответствии с учетом целей обработки ПДн, указанных в настоящем Положении, и включает в себя следующие данные:

- фамилия, имя, отчество;
- пол;
- год, месяц, дата и место рождения;
- сведения о гражданстве;
- реквизиты документа, удостоверяющего личность (серия, номер, кем и когда выдан документ);
- электронная копия документа, удостоверяющего личность (серия, номер, кем и когда выдан документ);
- адрес фактического места проживания и адрес регистрации по месту жительства и (или) по месту пребывания;
- номер телефона;
- адрес электронной почты;
- фотография;
- сведения о месте работы/учебы и занимаемой должности.

3.5 Сроки обработки персональных данных

Обработка ПДн осуществляется до достижения поставленных целей обработки ПДн, если срок обработки ПДн не установлен федеральным законом или договором, стороной которого, выгодоприобретателем или поручителем, по которому, является субъект ПДн.

3.6 Условия обработки персональных данных

3.6.1 Обработка ПДн осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»).

3.6.2 Обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн.

3.6.3 Фонд вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (далее – поручение оператора). Лицо, осуществляющее обработку ПДн по поручению оператора, обязано соблюдать принципы и цели обработки ПДн, предусмотренные настоящим Положением и ФЗ «О персональных данных». В поручении оператора определяются перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, устанавливается обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также указываются требования к защите обрабатываемых ПДн в соответствии со статьей 19 ФЗ «О персональных данных».

3.7 Способы обработки персональных данных

3.7.1 Обработка ПДн осуществляется путем автоматизированной и неавтоматизированной (смешанной) обработки ПДн.

3.7.2 Трансграничная передача ПДн не осуществляется.

3.8 Перечень действий, осуществляемых с персональными данными субъектов

Обработка ПДн включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), блокирование, удаление, уничтожение ПДн.

3.9 Права субъекта персональных данных

3.9.1 Субъекты ПДн имеют право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн оператором;

- правовые основания и цели обработки ПДн;
- цели и применяемые оператором способы обработки ПДн;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных ФЗ «О персональных данных»;
- информацию о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами.

3.9.2 Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

3.10 Порядок обработки персональных данных

3.10.1 Источники получения ПДн:

- субъект ПДн;
- законный представитель субъекта ПДн.

3.10.2 Фонд не имеет права получать и обрабатывать ПДн субъекта ПДн о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

3.10.3 В случае использования для получения ПДн форм, расположенных на интернет-сайте Мероприятия:

— осуществляется возможность беспрепятственного ознакомления субъекта ПДн с Положением, определяющим политику обработки и защиты персональных данных в информационной системе Мероприятия;

— ПДн передаются на обработку только после получения согласия субъекта ПДн на обработку его ПДн, путем заполнения чек-бокса в форме регистрации на соответствующей странице интернет-сайта Мероприятия.

3.10.4 Фонд получает ПДн от самого субъекта или его представителя, после получения от такого субъекта или его представителя, согласия на обработку его ПДн, если иное не предусмотрено действующим законодательством Российской Федерации.

3.10.5 Обработка ПДн может осуществляться исключительно в целях, указанных в п. 3.2. настоящего Положения.

3.10.6 ПДн субъектов обрабатываются и хранятся в информационной системе персональных данных Мероприятия.

3.10.7 Пользователям информационной системы персональных данных Мероприятия запрещено записывать и хранить на внешних (отчуждаемых) носителях информацию, содержащую ПДн.

3.10.8 При принятии решений, затрагивающих интересы субъекта ПДн, Фонд не имеет права основываться на ПДн, полученных исключительно в результате их автоматизированной обработки.

3.10.9 При передаче ПДн Фонд обязуется соблюдать следующие требования:

— не сообщать ПДн субъекта ПДн третьей стороне без его согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, а также в случаях, установленных федеральными законами;

— предупредить лиц, получивших ПДн субъекта ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

3.10.10 В случае выявления неправомерных действий с ПДн Фонд обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений, Фонд в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерности действий с ПДн, обязан уничтожить такие ПДн.

3.10.11 Об устранении допущенных нарушений или об уничтожении ПДн Фонд обязан уведомить субъект ПДн, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

3.10.12 Персональные данные уничтожаются в случаях:

- достижения целей обработки ПДн;
- отзыва субъектом ПДн согласия на обработку своих ПДн.

4 ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ

4.1 Основные мероприятия по обеспечению безопасности персональных данных

4.1.1 Обеспечение безопасности ПДн при их обработке достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия с ПДн.

4.1.2 Мероприятия по обеспечению безопасности ПДн определяются в зависимости от уровня защищенности ПДн в ИСПДн с учетом возможного возникновения угроз жизненно важным интересам личности, общества и государства.

4.1.3 Реализуются меры, направленные на выполнение требований, установленных ФЗ «О персональных данных»:

- получение согласия субъектов ПДн на обработку их ПДн, за исключением случаев, предусмотренных законодательством Российской Федерации;
- назначение ответственного за организацию обработки ПДн;
- назначение ответственного за обеспечение безопасности ПДн;
- принятие локальных нормативных актов в области обработки и защиты ПДн;
- применение правовых, организационных и технических мер по защите ПДн в соответствии с требованиями к защите ПДн;
- осуществление внутреннего контроля соответствия обработки ПДн ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым

актам, требованиям к защите ПДн, политике Фонда в отношении обработки ПДн, а также локальным нормативным актам Фонда в области обработки и защиты ПДн;

— осуществление оценки вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ «О персональных данных»;

— ознакомление лиц, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику в отношении обработки ПДн, локальными нормативными актами по вопросам обработки ПДн;

— учет машинных носителей ПДн;

— применение мер для восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

— хранение материальных носителей ПДн с соблюдением условий, обеспечивающих сохранность ПДн и исключающих несанкционированный доступ к ним;

— установление запрета на передачу ПДн по открытым каналам связи за пределы контролируемой зоны без применения установленных мер по обеспечению безопасности ПДн.

4.2 Меры защиты персональных данных

4.2.1 Разграничение полномочий доступа к ПДн, обрабатываемым в информационной системе персональных данных Мероприятия.

4.2.2 Для защиты входа на автоматизированное рабочее место применяются логин и пароль, индивидуальные для каждого пользователя. Защита от несанкционированного доступа осуществляется с использованием средства защиты информации.

4.2.3 Для защиты информационной системы персональных данных Мероприятия от вредоносных программ применяется средство антивирусной защиты.

4.2.4 Для защиты сетевой инфраструктуры Фонда при межсетевом взаимодействии применяются многофункциональные устройства, включающие в себя межсетевой экран, средство обнаружения вторжений, а также средство построения VPN-каналов.

4.2.5 Для защиты ПДн при передаче по открытым сетям связи используется шифрование по протоколам.

5 ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ПДн

5.1 Работы по защите ПДн в Фонде организуются с учетом следующих основных принципов:

- учет требований руководящих документов по обеспечению безопасности ПДн;
- комплексный подход к построению системы защиты ПДн;
- обеспечение защиты на всех этапах обработки ПДн и во всех режимах функционирования ИСПДн, в том числе при проведении ремонтных и регламентных работ;
- обеспечение необходимого уровня защиты ПДн при минимальных затратах;
- использование средств защиты, не ухудшающих существенно основные характеристики информационной системы персональных данных;
- обеспечение контроля эффективности средств защиты ПДн.

5.2 Непосредственное руководство работами по созданию, эксплуатации и совершенствованию системы защиты ПДн на Мероприятии осуществляет ответственный за обеспечение безопасности ПДн.

5.3 При организации и выполнении работ по защите ПДн необходимо руководствоваться действующими законами, постановлениями, руководящими документами по защите ПДн, а также требованиями настоящего Положения.

5.4 Организация выполнения работ по установке, настройке и вводу в эксплуатацию программных и программно-аппаратных средств защиты ПДн, разработке организационных мер по защите ПДн и контролю за состоянием системы защиты ПДн в информационной системе персональных данных Мероприятия возлагается на ответственного за обеспечение безопасности ПДн.

6 КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОТНОШЕНИИ ОБРАБОТКИ ПДН

Контроль за соблюдением требований законодательства Российской Федерации в области ПДн производится с целью:

- проверки соответствия обработки ПДн данным требованиям;
- проверки соответствия применяемых мер по защите ПДн данным требованиям;
- принятия мер, направленных на выявление и предотвращение нарушений данных требований;
- выявления возможных каналов утечки ПДн;
- устранения последствий возможных нарушений.

Контроль за соблюдением требований законодательства Российской Федерации в области обработки ПДн возлагается на ответственного за организацию обработки ПДн.

7 КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ПДН

7.1 Контроль состояния защищенности ПДн осуществляется с целью своевременного выявления и предотвращения несанкционированного доступа к ПДн, преднамеренных программно-технических воздействий на ПДн и оценки эффективности защиты ПДн.

7.2 Контроль заключается в проверке выполнения правовых законодательных и нормативных актов по вопросам защиты ПДн, а также в оценке обоснованности и эффективности принятых мер защиты ПДн.

7.3 По результатам контроля дается оценка эффективности принятых мер защиты ПДн. Защита ПДн считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам. Несоответствие мер установленным требованиям и нормам по защите ПДн является нарушением. Результаты анализа периодического контроля, установленные причины нарушений, рекомендации по их устранению отражаются в актах или справках, которые докладываются Директору Фонда для принятия соответствующих решений.