

УТВЕРЖДЕНО

Решением учредителя

Автономной некоммерческой организации

«Центр непрерывного развития личности

и реализации человеческого потенциала»

от 31.01.2019 № 31/01/1

**ПОЛОЖЕНИЕ О РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ**  
**в Автономной некоммерческой организации**  
**«Центр непрерывного развития личности и реализации человеческого потенциала»**

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Положение о работе с персональными данными в Автономной некоммерческой организации «Центр непрерывного развития личности и реализации человеческого потенциала» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", Трудовым кодексом Российской Федерации и другими нормативными актами.

1.2. Положение регулирует отношения, связанные с обработкой персональных данных, осуществляемой Автономной некоммерческой организацией «Центр непрерывного развития личности и реализации человеческого потенциала» (далее – АНО).

1.3. Требования Положения обязательны к исполнению всеми работниками АНО.

1.4. За невыполнение требований Положения лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных, несут в установленном порядке дисциплинарную, материальную, гражданско-правовую, административную и уголовную ответственности в порядке, установленном федеральными законами.

**2. ОСНОВНЫЕ ПОНЯТИЯ**

2.1. В целях Положения используются следующие основные понятия:

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

2) 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;

3) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

4) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

5) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

6) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

7) 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;

8) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных (информационная система) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

### **3. ЛИЦО, ОТВЕТСТВЕННОЕ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

3.1. Директор АНО назначает лицо, ответственное за организацию обработки персональных данных.

3.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от Директора АНО и подотчетно ему.

3.3. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением АНО и работниками АНО законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников АНО положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

### **4. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

4.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

4.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

4.7. Хранение персональных данных должно осуществляться 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. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

### **5. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

5.1. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на АНО, как оператора персональных данных, функций, полномочий и обязанностей;

3) обработка персональных данных осуществляется в связи с участием в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

4) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

5) 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;

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

7) обработка персональных данных необходима для осуществления прав и законных интересов АНО или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом "О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон "О микрофинансовой деятельности и микрофинансовых организациях", либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона «О персональных данных», при условии обязательного обезличивания персональных данных;

9) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

10) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

11) в иных случаях, установленных законодательством.

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 следующих случаев:

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

2) персональные данные сделаны общедоступными субъектом персональных данных;

3) 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;

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

5) иных случаев, предусмотренных законодательством.

5.3. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются АНО для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, когда обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации.

5.4. АНО, как оператор персональных данных, вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение АНО). Лицо, осуществляющее обработку персональных данных по поручению АНО, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении АНО должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных». При этом лицо, осуществляющее обработку персональных данных по поручению АНО, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случае, если АНО поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет АНО. Лицо, осуществляющее обработку персональных данных по поручению АНО, несет ответственность перед АНО.

5.5. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

## **6. ПРАВО СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ДОСТУП К ЕГО ПЕРСОНАЛЬНЫМ ДАННЫМ. ОБЯЗАННОСТИ ОПЕРАТОРА ПО ОБЕСПЕЧЕНИЮ ДОСТУПА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ К ЕГО ПЕРСОНАЛЬНЫМ ДАННЫМ, ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПО УСТРАНЕНИЮ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА, ДОПУЩЕННЫХ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

6.1. Субъект персональных данных за исключением случаев, предусмотренных Федеральным законом «О персональных данных», имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных АНО, как оператором персональных данных;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые АНО, как оператором персональных данных, способы обработки персональных данных;
- 4) наименование и место нахождения АНО, как оператора персональных данных, сведения о лицах (за исключением работников АНО), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с АНО или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

10) иные сведения, предусмотренные законодательством.

6.2. Субъект персональных данных вправе требовать от АНО, как оператора персональных данных, уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.3. Сведения, указанные в п. 6.1. Положения, предоставляются АНО субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.4. Сведения, указанные в п. 6.1. Положения, предоставляются субъекту персональных данных или его представителю АНО, как оператором персональных данных, при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с АНО, как оператором персональных данных (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных АНО, как оператором персональных данных, подпись субъекта персональных данных или его представителя.

6.5. АНО, как оператор персональных данных, сообщает в порядке, предусмотренном настоящим разделом Положения, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

6.6. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя АНО, как оператором персональных данных, даёт в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

6.7. АНО, как оператор персональных данных, безвозмездно предоставляет субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными,

неточными или неактуальными, АНО, как оператор персональных данных, вносит в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, АНО, как оператор персональных данных, уничтожает такие персональные данные. АНО, как оператор персональных данных, уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

6.8. В случае, если сведения, указанные в п. 6.1. Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к АНО, как оператору персональных данных, или направить ему повторный запрос в целях получения сведений, указанных в п. 6.1. Положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.9. Субъект персональных данных вправе обратиться повторно к АНО, как оператору персональных данных, или направить ему повторный запрос в целях получения сведений, указанных в п. 6.1. Положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 6.8. Положения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 6.4. Положения, должен содержать обоснование направления повторного запроса.

6.10. АНО, как оператор персональных данных, вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 6.8. и 6.9. Положения. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на АНО, как операторе персональных данных.

6.11. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных АНО, как оператор персональных данных, осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению АНО) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных АНО, как оператор персональных данных, осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению АНО) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.12. В случае подтверждения факта неточности персональных данных АНО, как оператор персональных данных, на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные

либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению АНО) в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.13. В случае выявления неправомерной обработки персональных данных, осуществляемой АНО, как оператором персональных данных, или лицом, действующим по поручению АНО, АНО, как оператор персональных данных, в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению АНО. В случае, если обеспечить правомерность обработки персональных данных невозможно, АНО, как оператор персональных данных, в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных АНО, как оператор персональных данных, уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.14. В случае достижения цели обработки персональных данных АНО, как оператор персональных данных, прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению АНО) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению АНО) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между АНО и субъектом персональных данных либо если АНО не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

6.15. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных АНО, как оператор персональных данных, прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению АНО) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению АНО) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между АНО и субъектом персональных данных либо если АНО не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

6.16. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 6.13.-6.15. Положения, АНО, как оператор персональных данных, осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению АНО) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.17. Если субъект персональных данных посчитает, что АНО, как оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект

персональных данных вправе обжаловать действия или бездействие АНО, как оператора персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

## **7. ОБЯЗАННОСТИ ОПЕРАТОРА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

7.1. При сборе персональных данных АНО, как оператор персональных данных, обязана предоставить субъекту персональных данных по его просьбе информацию, предусмотренную п. 6.1. Положения.

7.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, АНО, как оператор персональных данных, разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

7.3. Если персональные данные получены не от субъекта персональных данных, АНО, как оператор персональных данных, за исключением случаев, предусмотренных п. 7.4. Положения, до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию:

- 1) наименование и адрес АНО или наименование либо фамилия, имя, отчество и адрес представителя АНО;
- 2) цель обработки персональных данных и ее правовое основание;
- 3) предполагаемые пользователи персональных данных;
- 4) установленные Федеральным законом «О персональных данных» права субъекта персональных данных;
- 5) источник получения персональных данных.

7.4. АНО, как оператор персональных данных, освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 7.3. Положения, в случаях, если:

- 1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- 2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- 3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- 4) АНО, как оператор персональных данных, осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- 5) предоставление субъекту персональных данных сведений, предусмотренных п. 7.3. Положения, нарушает права и законные интересы третьих лиц.

7.5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", АНО, как оператор персональных данных, 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, предусмотренных законодательством.

7.6. АНО, как оператор персональных данных, принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным



законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами:

1) Директор АНО назначает лицо, ответственное за организацию обработки персональных данных.

2) В АНО применяются правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

3) Проводится ознакомление работников АНО, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику АНО в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

4) АНО принимает иные предусмотренные законодательством меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

7.7. АНО, как оператор персональных данных, при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

7.8. Обеспечение безопасности персональных данных достигается, в частности:

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

2) Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3) Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

Необходимо для каждого из уровней защищенности персональных данных применение средств криптографической защиты информации (далее – СКЗИ) соответствующего класса, позволяющих обеспечивать безопасность персональных данных при реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых СКЗИ персональных данных или создания условий для этого (далее - атака), которое достигается путем:

а) получения исходных данных для формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

б) формирования и утверждения Директором АНО совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ;

в) использования для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше.

4) Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- Идентификация и аутентификация субъектов доступа и объектов доступа. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

- Управление доступом субъектов доступа к объектам доступа. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

- Ограничение программной среды. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

- Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

- Регистрация событий безопасности. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

- Антивирусная защита. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

- Обнаружение (предотвращение) вторжений. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

- Контроль (анализ) защищенности персональных данных. Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

- Обеспечение целостности информационной системы и персональных данных. Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

- Обеспечение доступности персональных данных. Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

- Защита среды виртуализации. Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

- Защита технических средств. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

- Защита информационной системы, ее средств, систем связи и передачи данных. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

- Выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них. Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

- Управление конфигурацией информационной системы и системы защиты персональных данных. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Технические меры защиты персональных данных реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных. В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится АНО самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

5) Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

6) Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

7) Обеспечением сохранности носителей персональных данных путем:

- осуществления хранения съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов);

- осуществления поэкземплярного учета машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров.

8) Утверждением Директором АНО и поддержанием в актуальном состоянии документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

9) Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

10) Контролем за соблюдением работниками АНО законодательства, в том числе в области персональных данных.

11) Совершенствованием внутренних документов АНО по вопросам обработки персональных данных, обеспечения технологической и информационной безопасности.

12) Оптимизацией кадровых ресурсов АНО путем:

- изучения современного состояния менеджмента, применения организационных моделей, испытанных на практике; адаптации мирового опыта в области построения функционирующих организационных схем к конкретным условиям деятельности АНО;

- подбора квалифицированных кадров и эффективной расстановки кадров на всех функциональных направлениях деятельности АНО;

- разработки системы критериев при приеме работников на работу в АНО (определенный уровень образования, стаж, личностные характеристики потенциального работника применительно к содержанию работы и объему ответственности);

- обучения, переподготовки и повышения квалификации кадров;

- разработки подробных и ясных должностных инструкций, создания процедур контроля за соблюдением работниками АНО своих должностных обязанностей;

- организации взаимозаменяемости работников АНО;

- распределения прав и обязанностей между работниками АНО таким образом, который исключает возникновение конфликта интересов;

- четкое разграничение полномочий и ответственности для каждого работника АНО и механизма принятия коллегиальных решений в случае пересечения функций работников АНО;

- разработки системы поощрений и взысканий работников.

15) Организацией режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, обеспечиваемой следующими мероприятиями:

- размещением помещения АНО и оборудования способом, исключающим возможность бесконтрольного проникновения в это помещение и к этому оборудованию посторонних лиц;

- оборудованием помещения АНО охранной сигнализацией;

- обеспечением контроля за входом в помещение АНО;

- оснащением помещений входными дверьми с замками, обеспечением постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывания помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений;

- утверждением правил доступа в помещения в рабочее и нерабочее время, а также в нестандартных ситуациях;

- утверждением перечня лиц, имеющих право доступа в помещения.

16) Разграничением прав доступа при вводе и обработке данных, имеющее своей целью предохранение от несанкционированных действий работников АНО, обеспечиваемым следующими мероприятиями:

- доступ к данным только ограниченного круга лиц, являющихся непосредственными исполнителями;

- доступ к данным только с определенных автоматизированных рабочих мест;

- доступ к данным только в пределах полномочий, предоставленных непосредственно исполнителям.

17) Защитой рабочих мест работников АНО и мест хранения документов от беспрепятственного доступа и наблюдения, обеспечиваемой следующими мероприятиями:

- размещением рабочих мест работников таким образом, чтобы исключить возможность несанкционированного просмотра документов и информации, отраженной на экранах мониторов;

- хранением документов в запираемых шкафах или сейфах.

18) Ограничением доступа работников АНО к служебной информации и иной конфиденциальной информации, обеспечиваемым следующими мероприятиями:

- наличие доступа работников АНО только к сведениям, необходимым им для выполнения своих прямых служебных обязанностей;

- установлением паролей доступа к данным, содержащимся в автоматизированной системе.

19) Наличием системы разграничения доступа к разным уровням баз данных и операционной среды используемого программного обеспечения, состоящей из системы разграничения доступа на уровне локальной сети.

7.9. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

7.10. АНО, как оператор персональных данных, сообщает в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

7.11. АНО, как оператор персональных данных, до начала обработки персональных данных уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных пунктом 7.12. Положения.

7.12. АНО, как оператор персональных данных, вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

- 1) обрабатываемых в соответствии с трудовым законодательством;
- 2) полученных АНО в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются АНО исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- 3) сделанных субъектом персональных данных общедоступными;
- 4) включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- 5) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится АНО, или в иных аналогичных целях;
- 6) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;
- 10) в иных случаях, установленных законодательством.

7.13. В случае изменения сведений, указанных в уведомлении, предусмотренном п. 7.11. Положения, а также в случае прекращения обработки персональных данных АНО, как оператор персональных данных, уведомляет об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

7.14. АНО, как оператор персональных данных, имеет другие обязанности, установленные Положением, Федеральным законом «О персональных данных», иными нормативными актами.

## **8. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ**

8.1. Обработка персональных данных работника АНО осуществляется АНО в объеме и содержании, установленных законодательством, и в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в получении образования, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, а также в иных целях, предусмотренных законодательством.

8.2. АНО получает персональные данные работника АНО у самого работника. Если персональные данные работника АНО возможно получить только у третьей стороны, то работник АНО уведомляется АНО об этом заранее и от работника получается письменное согласие. АНО сообщает работнику АНО о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника АНО дать письменное согласие на их получение.

8.3. АНО не имеет права получать и обрабатывать сведения о работнике АНО, относящиеся в соответствии с законодательством Российской Федерации в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных Трудовым кодексом РФ и другими федеральными законами.

8.4. При принятии решений, затрагивающих интересы работника АНО, АНО не имеет права основываться на персональных данных работника АНО, полученных исключительно в результате их автоматизированной обработки или электронного получения;

8.5. АНО обеспечивает защиту персональных данных работника АНО от неправомерного их использования или утраты в порядке, установленном Трудовым кодексом РФ и иными федеральными законами.

8.6. Порядок хранения и использования персональных данных работников АНО устанавливается АНО с соблюдением требований Трудового кодекса и иных федеральных законов.

8.7. При передаче персональных данных своего работника АНО соблюдает следующие требования:

- Не сообщает персональные данные работника АНО третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом или иными федеральными законами.

- Не сообщает персональные данные работника АНО в коммерческих целях без его письменного согласия.

- Предупреждает лиц, получающих персональные данные работника АНО, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требует от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника АНО, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Трудовым кодексом РФ и иными федеральными законами.

- Осуществляет передачу персональных данных работника АНО в пределах АНО в соответствии с Положением.

- Разрешает доступ к персональным данным работников АНО только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника АНО, которые необходимы для выполнения конкретных функций. Перечень уполномоченных лиц, имеющих доступ к персональным данным работников АНО, утверждается Приказом Директора АНО.

- Не запрашивает информацию о состоянии здоровья работника АНО, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником АНО трудовой функции;

- Соблюдает иные требования, установленные законодательством.

8.8. В целях обеспечения защиты персональных данных, хранящихся в АНО, работники АНО имеют право на:

- полную информацию об их персональных данных и обработке этих данных;

- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника АНО, за исключением случаев, предусмотренных федеральным законом;

- определение своих представителей для защиты своих персональных данных;

- доступ к медицинской документации, отражающей состояние их здоровья;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса РФ или иного федерального закона. При отказе АНО исключить или исправить персональные данные работника АНО последний имеет право заявить в письменной форме в адрес АНО о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник АНО имеет право дополнить заявлением, выражающим его собственную точку зрения;

- требование об извещении АНО всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника АНО, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия АНО при обработке и защите персональных данных работника АНО.

## 9. УТВЕРЖДЕНИЕ И ИЗМЕНЕНИЕ ПОЛОЖЕНИЯ

9.1. Положение вступает в силу после его утверждения решением учредителя АНО и может быть изменено в любое время по решению учредителя АНО.

## 10. ОЗНАКОМЛЕНИЕ РАБОТНИКОВ С ПОЛОЖЕНИЕМ

10.1. Работники АНО знакомятся под роспись с Положением, с иными документами АНО, устанавливающими порядок обработки персональных данных работников АНО, а также права и обязанности работников АНО в этой области.

Учредитель  
Автономной некоммерческой организации  
«Центр непрерывного развития личности  
и реализации человеческого потенциала»



С.Т.Патрикеева