|  |
| --- |
| УТВЕРЖДАЮ |
| Директор ГКУ НСО ЦСПНКочковского района\_\_\_\_\_\_\_\_\_\_\_\_\_ Т.В.Гудова |
|  |
| «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2018 г. |

**Правила**

**осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в сегменте государственной информационной системы Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и Типизированное хранилище данных Новосибирской области» государственного казенного учреждения Новосибирской области «Центр социальной поддержки населения Кочковского района»**

**1. Общие положения**

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в сегменте государственной информационной системы Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и Типизированное хранилище данных Новосибирской области» государственного казенного учреждения Новосибирской области «Центр социальной поддержки населения Кочковского района» (далее – Правила) разработаны в соответствии с требованиями постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Целью проведения внутреннего контроля является проверка соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными нормативными актами оператора.

В Правилах определен порядок организации и осуществления внутреннего контроля обработки персональных данных (далее – ПДн) с целью своевременного выявления и предотвращения:

* хищения технических средств и носителей информации;
* утраты информации;
* преднамеренных программно-технических воздействий на информацию и (или) средства вычислительной техники, вызывающих нарушение конфиденциальности, целостности и доступности информации и нарушение работоспособности автоматизированной системы;
* несанкционированного доступа к ПДн с целью уничтожения, искажения, модификации (подделки), копирования и блокирования.

Внутренний контроль состояния защиты информации включает в себя:

* контроль организации защиты информации;
* контроль эффективности защиты информации.

**2. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности ПДн**

В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям организуется проведение периодических проверок условий обработки ПДн. Проверки осуществляются не реже одного раза в год в соответствии с утвержденным Планом проведения внутреннего контроля соответствия обработки информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну в сегменте государственной информационной системы Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и Типизированное хранилище данных Новосибирской области» государственного казенного учреждения Новосибирской области «Центр социальной поддержки населения Кочковского района» требованиям к защите такой информации (Приложение № 1 к настоящим Правилам).

При осуществлении внутреннего контроля соответствия обработки ПДн установленным требованиям производится проверка:

* соблюдения принципов обработки ПДн;
* соответствия локальных нормативных актов государственного казенного учреждения Новосибирской области «Центр социальной поддержки населения Кочковского района» в области ПДн действующему законодательству Российской Федерации;
* выполнения работниками ГКУ НСО ЦСПН Кочковского района требований и правил обработки ПДн в информационных системах персональных данных (далее – ИСПДн);
* актуальности информации о законности целей обработки ПДн и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн;
* правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой ИСПДн;
* актуальности перечня должностей должностных лиц, уполномоченных на обработку ПДн, имеющих доступ к ПДн;
* соблюдения прав субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн;
* соблюдения обязанностей оператора ПДн, предусмотренных действующим законодательством в области ПДн;
* порядка взаимодействия с субъектами персональных данных, ПДн которых обрабатываются в ИСПДн, в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПДн, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения (запросы) субъектов персональных данных, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами персональных данных;
* наличия необходимых согласий субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн;
* актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) персональных данных;
* актуальности перечня ИСПДн;
* знания и соблюдения работниками ГКУ НСО ЦСПН Кочковского района положений действующего законодательства Российской Федерации в области защиты ПДн, локальных нормативных актов ГКУ НСО ЦСПН Кочковского района;
* соблюдения работниками ГКУ НСО ЦСПН Кочковского района конфиденциальности ПДн;
* наличия и актуальности локальных нормативных актов, технической и эксплуатационной документации технических и программных средств ИСПДн.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за проведение проверки, докладывает начальнику ГКУ НСО ЦСПН Кочковского района или лицу, его замещающему.

При проведении внутреннего контроля соответствия обработки ПДн требованиям к защитесоставляется Отчет о результатах проведения внутренней проверки обеспечения защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, в сегменте государственной информационной системы Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и Типизированное хранилище данных Новосибирской области» государственного казенного учреждения Новосибирской области «Центр социальной поддержки населения Кочковского района» требованиям к защите такой информации по форме, приведенной в Приложении № 3 к настоящим Правилам.

**3. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн**

Во время осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям производится соответствие оценки соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн в информационных системах ГКУ НСО ЦСПН Кочковского района.

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн, для каждой ИСПДн производится экспертное сравнение заявленной оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области защиты ПДн и изложенных в настоящих Правилах осуществления внутреннего контроля соответствия обработки ПДн.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн, оформляется в виде отдельного документа, подписывается ответственным за обработку и защиту информации ГКУ НСО ЦСПН Кочковского района (либо лицом, его замещающим) и утверждается директором ГКУ НСО ЦСПН Кочковского района.