Министерство образования Московской области
Государственное бюджетное профессиональное образовательное учреждение
Московской области «Серпуховский колледж»

УТВЕРЖДАЮ
Директор ГБПОУ МО
«Серпуховский колледж»
_____ Т.В. Федорова
«01» июня 2021 г.

Рег. № 3.39
Приказ от «01» 06 2021 г. № 91-о

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных в ГБПОУ «Серпуховский колледж» требованиям к защите персональных данных

Рассмотрено на заседании Совета колледжа
Протокол № 12 от 31. 05 2021 г.

г. Серпухов

1. Общие положения

1.1. Настоящие «Правила осуществления внутреннего контроля соответствия обработки персональных данных в ГБПОУ «Серпуховский колледж», требованиям к защите персональных данных» (далее – Правила) разработаны на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ ОТ 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных», 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».

1.2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБПОУ «Серпуховский колледж» (далее – колледж) и действуют постоянно.

1.3. Целью осуществления внутреннего контроля соответствия обработки персональных данных в колледже требованиям к защите персональных данных (далее – внутренний контроль) является соблюдение в колледже законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных.

1.4. Внутренний контроль включает в себя: контроль организации защиты информации и контроль эффективности защиты информации.

1.5. Исполнение данных Правил обязательно для всех работников колледжа, осуществляющих обработку персональных, как без использования средств автоматизации, так и в информационных системах обработки персональных данных.

2. Порядок осуществления внутреннего контроля

2.1. Внутренний контроль подразделяется на плановый и внеплановый.

2.2. Внутренний контроль осуществляется комиссией по персональным данным, лицом, ответственным за организацию обработки персональных данных, и администратором ИСПДн.

2.3. Плановый внутренний контроль проводится на основании плана, утвержденного директором колледжа. Периодичность планового контроля – не реже одного раза в год.

2.4. Срок проведения планового внутреннего контроля составляет 10 рабочих дней.

2.5. Внеплановый внутренний контроль проводится по решению комиссии по персональным данным лица, ответственного за организацию обработки персональных данных или администратора ИСПДн:

- на основании поступившего устного обращения либо документа в письменной или электронной форме содержащего заявления субъекта персональных данных о нарушении законодательства в области персональных данных;
- в связи с проведением государственного контроля за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных;
- при вводе ИСПДн в эксплуатацию;
- после ремонта технических средств, входящих в состав ИСПДн и средств защиты информации;
- при изменении условий эксплуатации ИСПДн и размещения технических средств;
- по итогам расследования случаев нарушения информационной безопасности или компрометации персональных данных.

2.6. Внеплановый внутренний контроль может проводиться на основании решения директора колледжа.

2.7. Внеплановый внутренний контроль должен быть завершен не позднее чем через месяц со дня принятия решения о его проведении.

2.8. Результаты внутреннего контроля оформляются в виде справки или протокола.

2.9. При выявлении в ходе внутреннего контроля нарушений в протоколе указываются:

- перечень мероприятий по устранению выявленных нарушений и сроки их устранения;
- целесообразность приостановления или прекращения обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- необходимость привлечения к дисциплинарной ответственности лиц виновных в нарушении законодательства Российской Федерации о персональных данных.

2.10. По результатам внутреннего контроля могут быть выработаны предложения о совершенствовании правового, технического и организационного обеспечения безопасности персональных данных при их обработке.

2.11. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, сообщать директору колледжа.

2.12. В отношении персональных данных, ставших известными лицу, ответственному за организацию обработки персональных данных, или членам комиссии в ходе проведения внутреннего контроля, соблюдается конфиденциальность и обеспечивается безопасность при их обработке.

3. Объекты и тематика внутреннего контроля

3.1. В число основных объектов внутреннего контроля входят:

- структурные и обособленные подразделения колледжа, в которых осуществляется обработка ПДн;
- работники, допущенные в установленном порядке к обработке ПДн, и их носителям, и выполняющие работы с их использованием;
- служебные помещения, в которых проводятся работы с носителями ПДн;
- места непосредственного хранения носителей ПДн (хранилища, сейфы, шкафы);
- непосредственно носители ПДн (документы, материалы, изделия, магнитные носители);
- компоненты ИСПДн, в которых осуществляется обработка ПДн;
- локальная сеть передачи данных.

3.2. Особенности контроля безопасности ПДн в отдельных ИСПДн могут регулироваться дополнительными локальными актами.

3.3. Тематика проверок обработки персональных данных с использованием средств автоматизации:

- соответствие локальных актов колледжа в области обработки персональных данных с использованием средств автоматизации действующему законодательству Российской Федерации;
- выполнение работниками требований и правил обработки ПДн в ИСПДн;
- актуальность информации о законности целей обработки ПДн и оценке вреда, который может быть причинен субъектам персональных данных в случаях нарушения требований по обработке и обеспечению безопасности ПДн;
- правильность осуществления сбора, систематизации, записи, накопления, хранения ,уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой из ИСПДн;
- актуальность перечня должностных лиц, уполномоченных на обработку ПДн, имеющих доступ к ПДн;
- актуальность перечня должностных лиц, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;

- соблюдение прав субъектов персональных данных, ПДн которых обрабатываются в ИСПДн;
- соблюдение обязанностей оператора ПДн, предусмотренных действующим законодательством в области ПДн;
- порядок взаимодействия с субъектами персональных данных, ПДн которых обрабатываются в ИСПДн, в том числе соблюдение сроков, предусмотренных действующим законодательством в области ПДн, соблюдение 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;
- актуальность сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) персональных данных;
- актуальность перечня ИСПДн и обрабатываемых ПДн;
- знание и соблюдение работниками положений действующего законодательства Российской Федерации в области ПДн и локальных актов Общества;
- соблюдения работниками конфиденциальности ПДн и требований по обеспечению безопасности ПДн;
- наличие и актуальность локальных актов, технической и эксплуатационной документации технических и программных средств ИСПДн;
- соответствие полномочий пользователя ИСПДн правам, предоставленным ему Положением о разграничении прав доступа к персональным данным, обрабатываемым в колледже;
- соблюдение пользователями ИСПДн парольной политики;
- соблюдение пользователями ИСПДн антивирусной политики;
- соблюдение пользователями ИСПДн правил работы со съемными носителями персональных данных;
- соблюдение порядка доступа в помещения колледжа, где расположены элементы ИСПДн;
- соблюдение порядка резервирования баз данных и хранения резервных копий;
- своевременность проведения мероприятий по уничтожению информации, размещенной на электронных носителях и содержащей ПДн;
- соблюдение порядка работы со средствами защиты информации;

- знание пользователей ИСПДн о своих действиях во внештатных ситуациях.

3.4. Тематика проверок обработки персональных данных без использования средств автоматизации:

- соответствие локальных актов колледжа в области обработки персональных данных без использования средств автоматизации действующему законодательству Российской Федерации;
- условия хранения бумажных носителей с персональными данными;
- доступ к бумажным носителям с персональными данными;
- доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

Ответственный за организацию
обработки персональных данных _____ С.Л. Булгаков