РОССИЙСКАЯ ФЕДЕРАЦИЯ
УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ ГОРОДА ТУЛЫ

МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ – ЦЕНТРАЛИЗОВАННАЯ БУХГАЛТЕРИЯ ПО МУНИЦИПАЛЬНЫМ ОБРАЗОВАТЕЛЬНЫМ УЧРЕЖДЕНИЯМ ГОРОДА ТУЛЫ

ПРИКАЗ

01 сентября 2022 г. **№106-а**

г. Тула

О внесении изменений в приказ от 20.01.2022 № 5-а «О защите персональных данных в МКУ-ЦБ по МОУ г.Тулы»

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 №18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения», письмом Роскомнадзора от 19.08.2022 №08-75348

ПРИКАЗЫВАЮ:

1. Внести изменения в приказ от 20.01.2022 №5-а «О защите персональных данных в МКУ-ЦБ по МОУ г.Тулы».
2. Изложить Приложения №1,3,4,6 к указанному выше приказу в новой редакции.
3. Специалисту по кадрам отдела правовой, кадровой работы и делопроизводства Задонской В.А. ознакомить с документами, утвержденными настоящим приказом, работников, на которых распространяется их действие под подпись в течение 5 (пяти) рабочих дней.
4. Специалисту по кадрам отдела правовой, кадровой работы и делопроизводства Задонской В.А. организовать ознакомление с документами,

утвержденными настоящим приказом, вновь принимаемых работников, на которых распространяется их действие под подпись.

5. Приказ вступает в силу с 1 сентября 2022 года.

6. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник - главный бухгалтер
МКУ - ЦБ по МОУ г. Тулы Л.А. Скалина

Приложение №1

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 01.09.2022 №106-а

Инструкция
ответственного за обеспечение безопасности персональных данных в информационных системах МКУ-ЦБ по МОУ г.Тулы

1. Общие положения.

1.1. Ответственный за обеспечение безопасности персональных данных в информационных системах МКУ-ЦБ по МОУ г.Тулы (далее - Ответственный) – сотрудник МКУ-ЦБ по МОУ г.Тулы, обеспечивающий защиту информации, обрабатываемой в информационных системах МКУ-ЦБ по МОУ г.Тулы, отвечающий за защиту информационных систем и содержащейся в них информации от несанкционированного доступа, осуществляет функции контроля за соблюдением режима защиты конфиденциальной информации (в т. ч. персональных данных), за корректировку разрешительной системы доступа к информационным системам (ресурсам), ведение и поддержание в актуальном состоянии документации по вопросам защиты информации в информационных системах МКУ-ЦБ по МОУ г.Тулы.

1.2. Ответственный осуществляет взаимодействие по вопросам технической защиты конфиденциальной информации (в т. ч. персональных данных) с организацией - лицензиатом ФСТЭК России, осуществлявшей аттестацию объектов информатизации МКУ-ЦБ по МОУ г.Тулы (орган по аттестации) на соответствие этих объектов требованиям законодательства Российской Федерации.

1.3. Ответственный в своей работе руководствуется положениями настоящей Инструкции, требованиями других нормативных правовых и нормативно-методических документов, регламентирующих защиту информации, требованиями эксплуатационной документации средств защиты информации, используемых в МКУ-ЦБ по МОУ г.Тулы, технических и программных средств, имеющих встроенные механизмы защиты.

2. В обязанности Ответственного входит:

2.1. Ведение учета перечня категорий персональных данных, обрабатываемых в МКУ-ЦБ по МОУ г.Тулы.

2.1. Ведение учета лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.

2.2. Ведение учета лиц, допущенных к работе со средствами криптографической защиты информации.

2.3. Разработка и поддержание в актуальном состоянии разрешительной системы доступа к локальным и сетевым ресурсам информационных систем МКУ-ЦБ по МОУ г.Тулы.

2.4. Разработка и поддержание в актуальном состоянии технических паспортов информационных систем МКУ-ЦБ по МОУ г.Тулы.

2.5. Согласование вносимых изменений в технический паспорт аттестованных информационных систем с органом по аттестации.

2.6. Участие в проведении мероприятий внутреннего контроля по вопросам обработки и защиты конфиденциальной информации, в том числе персональных данных.

2.7. Ведение учета средств защиты информации, эксплуатационной и технической документации к ним.

2.8. Ведение учета съемных носителей персональных данных (в т. ч. маркировка учтенных съемных носителей).

2.9. Сообщать в срок до 10 рабочих дней в территориальное управление Роскомнадзора о намерении обрабатывать персональные данные, в том числе, если персональные данные обрабатываются в соответствии с трудовым законодательством Российской Федерации.

2.10. Сообщать в срок не более 48 часов в территориальное управление Роскомнадзора о неправомерном доступе третьих лиц к персональным данным сотрудников.

2.11. В случае прекращения обработки персональных данных сообщать в срок до 10 рабочих дней в территориальное управление Роскомнадзора о намерении прекратить обрабатывать персональные данные.

3. Ответственный имеет право:

3.1. Требовать от пользователей информационных систем МКУ-ЦБ по МОУ г.Тулы выполнения установленной технологии обработки информации, локальных актов в сфере информационной безопасности МКУ-ЦБ по МОУ г.Тулы.

3.2. Останавливать обработку информации информационных системах МКУ-ЦБ по МОУ г.Тулы в случае подтверждения нарушений установленной технологии обработки данных, приводящих к нарушению функционирования средств защиты информации.

3.3. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам защиты информации.

4. Ответственный несет персональную ответственность за качество и полноту проводимых им работ по обеспечению согласия на защиту информации в соответствии с настоящей инструкцией.

5. Ответственный несет ответственность по законодательству РФ за нарушение требований нормативно-методических документов по защите информации и настоящей инструкции.

Приложение №3

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 01.09.2022 №106-а

Политика
МКУ-ЦБ по МОУ г.Тулы в отношении обработки персональных данных

1. Общие положения

1.1. Настоящая Политика МКУ-ЦБ по МОУ г.Тулы в отношении обработки персональных данных (далее - Политика) разработана в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

1.2. Политика определяет цели, принципы обработки и реализуемые требования к защите персональных данных в МКУ-ЦБ по МОУ г.Тулы.

1.3. Персональные данные являются информацией ограниченного доступа и подлежат защите в соответствии с законодательством Российской Федерации.

2. Основные понятия

2.1. В настоящей Политике используются следующие основные понятия:

2.1.1. Субъектами персональных данных МКУ-ЦБ по МОУ г.Тулы являются:

- работники МКУ-ЦБ по МОУ г.Тулы;
- претенденты на замещение вакантной должности;
- студенты, проходящие практику в МКУ-ЦБ по МОУ г.Тулы;
- контрагенты МКУ-ЦБ по МОУ г.Тулы;
- лица, передавшие персональные данные в МКУ-ЦБ по МОУ г.Тулы в своих обращениях и заявлениях, в том числе при оформлении пропуска на территорию или в помещения МКУ-ЦБ по МОУ г.Тулы;
- лица, состоящие в договорных или иных отношениях с МКУ-ЦБ по МОУ г.Тулы.

2.1.2. В соответствии со ст. 86 ТК РФ МКУ-ЦБ по МОУ г.Тулы предоставлено право обрабатывать персональные данные сотрудника Учреждения исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получения образования и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.1.3. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.1.4. 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.

2.1.5. Конфиденциальность персональных данных – обязанность оператора и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Защита персональных данных

3.1. Работодатель принимает следующие меры по защите персональных данных:

3.1.1. Назначение лица, ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите персональных данных.

3.1.2. Разработка политики в отношении обработки персональных данных.

3.1.3. Установление правил доступа к персональных данных, обеспечение регистрации и учета всех действий, совершаемых с персональных данных.

3.1.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

3.1.5. Применение прошедшей в установленном порядке процедуры оценки соответствия средств защиты информации.

3.1.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

3.1.7. Соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ.

3.1.8. Обнаружение фактов несанкционированного доступа к персональным данным.

3.1.9. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

3.1.10. Обучение работников, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Работодателя в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.

3.1.11. Осуществление внутреннего контроля и аудита.

3.1.12. Определение типа угроз безопасности и уровней защищенности персональных данных, которые хранятся в информационных системах.

3.2. Угрозы защищенности персональных данных:

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

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

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

3.3. Уровни защищенности персональных данных:

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

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

3.3.3. Третий уровень защищенности. Если при втором типе угрозы работодатель обрабатывает общие персональных данных работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории персональных данных работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает биометрические персональные данные, или при третьем типе угрозы работодатель обрабатывает общие персональные данные более чем 100 тыс. физических лиц.

3.3.4. Четвертый уровень защищенности. Если при третьем типе угрозы работодатель обрабатывает только общие персональные данные работников или менее чем 100 тыс. физических лиц.

3.4. При четвертом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещаете информационную систему;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных до ПД;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

3.5. При третьем уровне защищенности персональных данных дополнительно к мерам, перечисленным в пункте 2.4 настоящего Положения, работодатель назначает ответственного за обеспечение безопасности персональных данных в информационной системе.

3.6. При втором уровне защищенности персональных данных дополнительно к мерам, перечисленным в пунктах 3.4, 3.5 настоящего Положения, работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

3.7. При первом уровне защищенности персональных данных дополнительно к мерам, перечисленным в пунктах 3.4—3.6 настоящего Положения, работодатель:

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

3.8. В целях защиты персональных данных на бумажных носителях работодатель:

- приказом назначает ответственного за обработку персональных данных;
- ограничивает допуск в помещения, где хранятся документы, которые содержат персональных данных работников;
- хранит документы, содержащие персональные данные работников в шкафах, запирающихся на ключ;
- хранит трудовые книжки работников в сейфе в отделе кадров.

3.9. В целях обеспечения конфиденциальности документы, содержащие персональных данных работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии и службы охраны труда работодателя.

3.10. Работники отдела кадров, бухгалтерии и службы охраны труда работодателя, допущенные к персональных данных работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных работников не допускаются.

3.11. Допуск к документам, содержащим персональные данные работников, внутри организации осуществляется на основании Регламента допуска работников к обработке персональных данных.

3.12. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством РФ, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

3.13. Передача информации, содержащей сведения о персональных данных работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

4. Принципы и цели обработки персональных данных

4.1. МКУ-ЦБ по МОУ г.Тулы в своей деятельности по обработке персональных данных руководствуется следующими принципами:

4.1.1. Обработка персональных данных осуществляется на законной и справедливой основе.

4.1.2. Цели обработки персональных данных соответствуют полномочиям МКУ-ЦБ по МОУ г.Тулы.

4.1.3. Содержание и объем обрабатываемых персональных данных соответствуют целям обработки персональных данных.

4.1.4. Достоверность персональных данных, их актуальность и достаточность для целей обработки, недопустимость обработки избыточных по отношению к целям сбора персональных данных.

4.1.5. Ограничение обработки персональных данных при достижении конкретных и законных целей, запрет обработки персональных данных, несовместимых с целями сбора персональных данных.

4.1.6. Запрет объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.1.7. Осуществление хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем это требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством.

4.1.8. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

4.2. Обработка персональных данных работников МКУ-ЦБ по МОУ г.Тулы осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, заключения и исполнения трудовых договоров, ведения воинского учета, исполнения требований по охране труда.

4.3. Обработка персональных данных граждан, не являющихся работниками МКУ-ЦБ по МОУ г.Тулы, осуществляется с целью реализации полномочий МКУ-ЦБ по МОУ г.Тулы в соответствии с Уставом, а также с целью отбора претендентов на замещение вакантных должностей МКУ-ЦБ по МОУ г.Тулы.

5. Гарантии конфиденциальности персональных данных

5.1. Все работники организации, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональных данных, в соответствии с Положением, требованиями законодательства РФ.

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

5.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.

6. Перечень мер по обеспечению безопасности персональных данных при их обработке

6.1. МКУ-ЦБ по МОУ г.Тулы при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

6.1.1. Назначением ответственного за организацию обработки персональных данных.

6.1.2. Утверждением локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

6.1.3. Осуществлением внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных.

6.1.4. Ознакомлением работников МКУ-ЦБ по МОУ г.Тулы, непосредственно осуществляющих обработку персональных данных, с требованиями законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, локальными актами в отношении обработки персональных данных, и обучением указанных работников.

6.1.5. Выполнением требований, установленных постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» при обработке персональных данных, осуществляемой без использования средств автоматизации.

6.1.6. Применением прошедшей в установленном порядке процедуры оценки соответствия средств защиты информации.

6.1.7. Учетом машинных носителей персональных данных.

6.1.8. Выявлением фактов несанкционированного доступа к персональным данным и принятием мер.

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

6.1.10. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых в информационной системе персональных данных.

6.2. Работники МКУ-ЦБ по МОУ г.Тулы, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение №4

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 01.09.2022 №106-а

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите конфиденциальной информации в МКУ-ЦБ по МОУ г.Тулы

I. Общие положения

1. Настоящее Положение устанавливает порядок организации и проведения работ по защите конфиденциальной информации в МКУ-ЦБ по МОУ г.Тулы (далее – Учреждение).

2. Действие настоящего Положения не распространяется на правоотношения, связанные с обращением со сведениями, составляющими государственную тайну.

3. В настоящем Положении под конфиденциальной информацией (информацией конфиденциального характера, сведениями конфиденциального характера) понимается информация ограниченного доступа, свободный доступ к которой ограничен в соответствии с федеральным законодательством, а также служебная информация, доступ к которой ограничен обладателем информации.

4. В настоящем Положении используются основные понятия в значении, определенном Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», а также следующие понятия:

автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

допуск к конфиденциальной информации – процедура оформления права граждан на доступ к сведениям конфиденциального характера;

защищаемые помещения (ЗП) – помещения (кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, конференций, переговоров и т.п.), связанных с обсуждением и (или) оглашением информации конфиденциального характера;

контролируемая зона (КЗ) – пространство (территория, здание, помещение или их часть), в котором исключено неконтролируемое пребывание лиц, не имеющих допуска, а также транспортных, технических и иных материальных средств;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по функциональному предназначению и техническим

характеристикам;

носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информационных сигналов;

ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы;

служебная информация ограниченного распространения – информация, касающаяся деятельности Учреждения, ограничение на распространение которой диктуются служебной необходимостью;

средство защиты информации (СЗИ) – техническое, программное, программно-техническое средство, предназначенное (используемое) для защиты информации;

утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

5. Защита конфиденциальной информации осуществляется на основании действующего законодательства Российской Федерации.

6. Доступ к сведениям конфиденциального характера Учреждение, в том числе содержащимся в информационных системах, может быть предоставлен с согласия обладателя информации и (или) в случаях, установленных законодательством.

7. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.

8. Согласие на обработку персональных данных в обязательном порядке должно содержать следующие позиции:

- ФИО;
- контактная информация (номер телефона, адрес электронной почты или почтовый адрес);
- сведения об операторе-организации;
- сведения об операторе-физическом лице;
- сведения об операторе-гражданине, являющимся ИП;
- сведения об информационных ресурсах оператора, через которые неограниченному кругу лиц предоставляется доступ к данным и производятся иные действия с персональными данными;
- цель обработки персональных данных;
- категории и перечень персональных данных, на обработку которых

дается согласие субъекта: персональные данные (ФИО, год, месяц, дата рождения, место рождения, адрес, семейное положение и др.), специальные категории персональных данных и биометрические данные;

- срок действия согласия.

9. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате.

10. Обработка биометрических персональных данных несовершеннолетних лиц с письменного согласия законного представителя субъекта персональных данных на обработку его биометрических персональных данных не допускается, за исключением случаем, обусловленных п.9 настоящего Положения.

11. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В таком случае оператор обязан прекратить обработку персональных данных в течение 30 календарных дней.

В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, предусмотренных действующим законодательством Российской Федерации Федерального закона.

12. В случае обращения сотрудника Учреждения по вопросу обработки его персональных данных ответ предоставляется не позднее 10 рабочих дней с момента поступления обращения.

13. В Учреждении осуществляется разрешение или ограничение доступа к информации, определяется порядок и условия такого доступа.

14. Сведения конфиденциального характера, в том числе служебная информация, ставшие известными работнику вследствие выполнения должностных обязанностей, запрещается использовать в личных целях и в целях причинения имущественного ущерба, морального вреда.

II. Принципы ограничения доступа к сведениям

1. Основными принципами ограничения доступа являются законность, обоснованность и своевременность.

2. Законность ограничения доступа заключается в выполнении требований законодательства при отнесении сведений к категории конфиденциальной информации. При этом учитываются как нормы, предписывающие налагать

ограничения на доступ к этим сведениям, так и запрещающие такие ограничения.

3. Обоснованность ограничения доступа заключается в установлении путем экспертной оценки целесообразности ограничения доступа, вероятных последствий этого акта, исходя из законных интересов Учреждения.

4. Своевременность ограничения доступа заключается в установлении ограничений на разглашение и (или) распространение сведений с момента их получения (разработки) или заблаговременно.

III. Порядок отнесения сведений к категории конфиденциальной информации

1. Решение об отнесении сведений к категории конфиденциальной информации принимает руководитель Учреждения путем утверждения перечня сведений конфиденциального характера (далее – Перечень сведений).

2. Для включения в Перечень сведений осуществляется анализ информации, содержащейся в утверждаемых руководителем документах, документах текущей деятельности (информационных потоках), обрабатываемых как в интересах обладателя информации, так и в интересах других лиц.

3. С целью обеспечения принципа обоснованности рассматривается возможный ущерб, который может быть нанесен государству, Учреждению, иным лицам в результате разглашения или распространения конфиденциальной информации, с затратами, необходимыми на ограничение доступа к ней.

4. Возможный ущерб оценивается исходя из наличия материальных, финансовых, репутационных и иных рисков или морального вреда в результате несанкционированного разглашения или распространения конфиденциальной информации.

5. При определении размера (степени) ущерба прогнозируются возможные потери и риски, возникающие не только в настоящее время, но и те, которые могут возникнуть в будущем.

6. При рассмотрении вопросов отнесения сведений к категории конфиденциальной информации учитываются следующие отрицательные факторы разглашения конфиденциальной информации:

- нарушение федеральных законов и иных нормативных правовых актов по ограничению доступа к информации;
- разрыв отношений (или их осложнение) с деловыми партнерами, юридическими и физическими лицами по причине разглашения сведений;
- срыв или невыполнение договорных обязательств, контрактов;
- создание трудностей при взаимодействии;
- экономические, судебные и иные санкции со стороны юридических и физических лиц за незаконное разглашение сведений о них;
- потеря, блокирование или искажение информации в базах данных;
- несанкционированная передача баз данных или их части;
- раскрытие действующей системы защиты информации.

7. Информация, полученная в результате взаимодействия Учреждения с контрагентами в процессе хозяйственной деятельности, может быть отнесена к

категории конфиденциальной положениями заключаемых договоров, соглашений, в которых также отражаются взаимные обязательства и ответственность сторон за сохранность этой информации.

Такая информация в Перечень сведений не включается.

IV. Обязанности по защите конфиденциальной информации и ответственность

1. В Учреждении назначается лица, ответственные:

– за организацию обработки персональных данных;

– за обеспечение безопасности конфиденциальной информации (в том числе персональных данных).

2. Указанные в пункте 20 ответственные лица в пределах своей компетенции организуют:

– контролируемый допуск работников Учреждения к информации конфиденциального характера;

– учет, хранение и уничтожение документов и машинных носителей с конфиденциальной информации;

– обработку конфиденциальной информации с помощью средств вычислительной техники;

– выполнение мероприятий по защите конфиденциальной информации;

– контроль соблюдения порядка работы с конфиденциальной информацией.

3. Не допускается хранение и обработка конфиденциальной информации на территории иностранных государств, если иное не предусмотрено действующими международными соглашениями Российской Федерации.

4. Доступ к конфиденциальной информации осуществляется в соответствии с разрешительной системой доступа (матрицей доступа), утверждаемой руководителем Учреждения.

5. За разглашение конфиденциальной информации, а также нарушение порядка обращения с ней, работник Учреждения может быть привлечен к дисциплинарной и (или) иной ответственности, предусмотренной действующим законодательством.

6. Не реже одного раза в год в Учреждении осуществляется контроль (аудит) соблюдения порядка работы с конфиденциальной информацией.

V. Порядок обмена конфиденциальной информации

1. Предоставление (передача) конфиденциальной информации может производиться только на основании решения руководителя Учреждения при условии соблюдения требований по защите информации.

2. Информация конфиденциального характера предоставляется органам государственной власти, государственным учреждениям и органам местного самоуправления Тульской области на безвозмездной основе.

3. Предоставление конфиденциальной информации иным лицам, если иное не установлено законодательством, регулируется заключаемыми договорами, устанавливающими права, обязанности и ответственность сторон,

перечень предоставляемых конфиденциальных сведений и компенсацию за разглашение и иное распространение указанных сведений.

4. При направлении сторонним организациям (учреждениям, предприятиям) сведений и документов, содержащих конфиденциальную информацию, в сопроводительном письме необходимо уведомлять (информировать) получателя о законном требовании соблюдения конфиденциальности полученной им информации и ответственности за ее разглашение или распространение. При обмене конфиденциальной информацией между органами власти, учреждениями делать указанное уведомление не обязательно.

5. Передача конфиденциальной информации в электронном виде разрешается только по защищенным каналам связи, оборудованным сертифицированными средствами защиты.

6. Не допускается речевая передача конфиденциальной информации по открытым проводным каналам связи, выходящим за пределы КЗ, и радиоканалам. При необходимости передачи конфиденциальной информации следует использовать защищенные линии связи.

7. Проведение конфиденциальных мероприятий (в том числе совещаний, комиссий, собраний, обсуждений и т.п.) разрешается только в ЗП, исключающих возможность перехвата речевой информации конфиденциального характера.

8. При необходимости ЗП оборудуются сертифицированными средствами защиты информации. ЗП должны быть аттестованы по требованиям безопасности информации и размещаться в пределах контролируемой зоны органа власти.

9. В Учреждении в соответствии с установленными требованиями по защите информации определяется перечень ЗП и лиц, ответственных за их эксплуатацию.

10. Во время проведения конфиденциальных мероприятий запрещается использование в ЗП радиотелефонов, устройств сотовой, пейджинговой и транкинговой связи.

VI. Организация и проведение работ по защите конфиденциальной информации

1. Проведение работ по защите конфиденциальной информации осуществляется путем:

– выполнения комплекса мероприятий (правовых, организационных, технических), направленных на предотвращение утечки информации (в том числе по техническим каналам), несанкционированного доступа к ней, преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения;

– проведения специальных работ, порядок организации и выполнения которых определяется Правительством Российской Федерации и федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, противодействия техническим разведкам и

технической защиты информации, в пределах их полномочий.

2. Организация мероприятий по защите конфиденциальной информации возлагается на ответственных лиц, указанных в пункте 20 настоящего Положения.

3. Обработка конфиденциальной информации допускается только на АС Учреждения, оснащенных сертифицированными по требованию законодательства программными, техническими и программно-техническими средствами защиты информации.

4. АС обработки такой информации должны быть аттестованы по требованиям безопасности информации, а применяемое в них программное обеспечение должно быть лицензионным.

5. При обработке конфиденциальной информации с использованием АС необходимо неукоснительно выполнять требования утвержденных руководителем Учреждения локальных актов, регламентирующих:

- антивирусную защиту информации;
- использование программного обеспечения;
- применение машинных носителей информации;
- организацию сетевой защиты информации;
- авторизацию пользователей;
- иные аспекты защиты информации.

Приложение №6

УТВЕРЖДЕНО
приказом МКУ-ЦБ по МОУ г. Тулы
от 01.09.2022 №106-а

ИНСТРУКЦИЯ
по обработке персональных данных, осуществляемой без использования средств автоматизации, МКУ-ЦБ по МОУ г.Тулы

I. Общие положения

1. Настоящая инструкция по обработке персональных данных, осуществляемой без использования средств автоматизации, в МКУ-ЦБ по МОУ г.Тулы (далее - Инструкция) устанавливают порядок обработки персональных данных, осуществляемой без использования средств автоматизации, а также порядок заполнения типовых форм документов МКУ-ЦБ по МОУ г.Тулы (далее – Учреждение), характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма).

2. Основные понятия, используемые в настоящих Правилах, соответствуют основным понятиям, установленным Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных».

II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

1. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

2. Работники Учреждения, осуществляющие обработку персональных данных без использования средств автоматизации, а также лица, осуществляющие такую обработку по договору с Учреждением, информируются о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти Тульской области, а также локальными правовыми актами Учреждения. По факту информирования указанные лица подписывают обязательства о неразглашении персональных данных.

3. При хранении материальных носителей персональных данных, обрабатываемых без использования средств автоматизации, с целью соблюдения условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ, применяются следующие меры:

3.1. Хранение материальных носителей персональных данных, обрабатываемых без использования средств автоматизации, осуществляется в

местах, установленных локальными актами Учреждения.

3.2. Обеспечивается раздельное хранение персональных данных, обработка которых осуществляется в несовместимых целях.

3.3. Руководитель Учреждения устанавливает перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

4. Работник Учреждения, ответственный за организацию обработки персональных данных, совместно с администратором безопасности контролирует реализацию мер, указанных в п.п. 3.1.-3.3. Инструкции, а также порядок их принятия.

5. При оформлении трудового договора с сотрудником Работодатель не имеет права делать копии и хранить документы с биометрическими данными. Документы, предъявляемые при приеме на работу, проверяются кадровым сотрудником, заносятся в личную карту и возвращаются кандидату на должность.

III. Порядок заполнения типовых форм

1. Учреждение является оператором, осуществляющим обработку персональных данных, адрес: г. Тула, ул. Гоголевская, д. 92.

2. Целями обработки персональных данных является осуществление деятельности, реализация полномочий Учреждения, в том числе кадровый учет, исполнение трудовых договоров, рассмотрение кандидатур на замещение вакантных должностей, антикоррупционная деятельность, воинский учет, ведением бухгалтерского, налогового и иных видов учета и пр.

3. Источником получения персональных данных, обрабатываемых без использования средств автоматизации, является непосредственно субъект персональных данных, либо его официальный представитель.

4. Сроки обработки персональных данных устанавливаются локальными актами Учреждения.

5. Персональные данные в администрации обрабатываются смешанным образом. Перечень действий с персональными данными, обрабатываемыми без использования средств автоматизации: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, удаление, уничтожение персональных данных.