УПРАВЛЕНИЕ ДОРОЖНОЙ ИНФРАСТРУКТУРЫ, ТРАНСПОРТА И СВЯЗИ АДМИНИСТРАЦИИ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОДСКОГО ОКРУГА «СЫКТЫВКАР»

ПРИКАЗ

«11» января 2021 г. № 3

По основной деятельности

Об утверждении локальных нормативных документов
в области защиты персональных данных
в Управлении дорожной инфраструктуры, транспорта и связи

С целью выполнения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Политику в отношении обработки персональных данных Управления дорожной инфраструктуры, транспорта и связи администрации МО ГО «Сыктывкар» (Приложение 1).
2. Утвердить инструкцию пользователя по работе с персональными данными в Управлении дорожной инфраструктуры, транспорта и связи администрации МО ГО «Сыктывкар» (Приложение 2).
3. Утвердить инструкцию пользователя государственной системы в Управлении дорожной инфраструктуры, транспорта и связи администрации МО ГО «Сыктывкар» (Приложение 3).
4. Утвердить инструкцию по организации учета, хранения и выдачи машинных носителей, содержащих персональные данные в информационных системах персональных данных в Управлении дорожной инфраструктуры, транспорта и связи администрации МО ГО «Сыктывкар» (Приложение 4).
5. Утвердить регламент установки обновлений программного обеспечения и средств защиты информации в Управлении дорожной инфраструктуры, транспорта и связи администрации МО ГО «Сыктывкар».
6. Руководителю группы кадровой работы и делопроизводства ознакомить сотрудников Управления под роспись.
7. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник Управления Е.Ю. Попов

Приложение №1

УТВЕРЖДЕНО
приказом Управления
дорожной инфраструктуры,
транспорта и связи администрации
МО ГО «Сыктывкар»
от 25.02.2021 №28/9

ПОЛОЖЕНИЕ О ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В УПРАВЛЕНИИ ДОРОЖНОЙ ИНФРАСТРУКТУРЫ, ТРАНСПОРТА И СВЯЗИ АДМИНИСТРАЦИИ МО ГО «СЫКТЫВКАР»

1. Общие положения

1.1. Настоящее Положение о защите конфиденциальной информации Управлении дорожной инфраструктуры, транспорта и связи администрации МО ГО «Сыктывкар» (далее – Управление ДИТИС АМО ГО «Сыктывкар») определяет комплекс организационных и технических мероприятий в части защиты конфиденциальной информации при ее обработке.

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 г. N 152-ФЗ "О персональных данных", Федеральным законом от 27.07.2006г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 29.07.2004 N 98-ФЗ "О коммерческой тайне", Положением об Управлении ДИТИС АМО ГО «Сыктывкар» и другими нормативно – правовыми актами Российской Федерации, регулирующими отношения в области информации.

1.3. Действие настоящего Положения распространяется на всех сотрудников Управления ДИТИС АМО ГО «Сыктывкар».

1.4. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

1.5. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

1.6. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

1.7. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

1.8. К информации, доступ к которой ограничен законодательством (информация ограниченного доступа), относятся: государственная тайна, коммерческая тайна, персональные данные, сведения, связанные с профессиональной деятельностью, служебная тайна.

1.9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

1.10. За разглашение информации с ограниченным доступом предусмотрена административная или уголовная ответственность.

1.11. Режим конфиденциальности снимается в случаях обезличивания или по истечении 25 лет срока хранения конфиденциальной информации, если иное не предусмотрено законодательством РФ.

1.12. В настоящем Положении используются следующие термины и определения:

Информация - сведения (сообщения, данные) независимо от формы их представления;

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

Конфиденциальная информация - любые сведения, составляющие служебную, коммерческую, врачебную, профессиональную тайну, включая персональные данные сотрудников и обучающихся.

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

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

Электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

Общедоступная информация - сведения и информация, доступ к которой не ограничен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги).

Обладатель конфиденциальной информации - лицо, которое владеет информацией, относящейся к конфиденциальной на законном основании, ограничило доступ к этой информации и установило в отношении ее режим конфиденциальной информации.

Обладателем информации, составляющей конфиденциальную информацию, является Управление ДИТИС АМО ГО «Сыктывкар».

Служебная тайна - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании, и в отношении которой обладателем такой информации введен режим коммерческой тайны).

Информация может быть отнесена к служебной тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений и не влечет (не может повлечь) получения прибыли обладателем такой информации.

Служебную тайну Управления ДИТИС АМО ГО «Сыктывкар»составляют любые сведения, в том числе сведения, содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях и иных сообщениях, передаваемых по сетям электрической и почтовой связи, которые стали

известны работнику организации в связи с исполнением им возложенных на него трудовых обязанностей. К служебной тайне не относится информация, разглашенная Управлением ДИТИС АМО ГО «Сыктывкар» самостоятельно или с её согласия, а также иная информация, ограничения доступа к которой не допускаются в соответствии с законодательством РФ.

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

Научнотехническая, технологическая, производственная, финансово-экономическая или иная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

Информация может быть отнесена к коммерческой тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений, либо в результате гражданско-правовых отношений, влекущая или могущая повлечь получение прибыли обладателем такой информации.

Профессиональная тайна - информация, полученная гражданами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности.

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

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;

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Доступ к конфиденциальной информации - ознакомление определенных лиц с конфиденциальной информацией, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача конфиденциальной информации - передача конфиденциальной информации ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Предоставление конфиденциальной информации — передача конфиденциальной информации ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение (распространение) конфиденциальной информации - действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав

персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

Режим конфиденциальности - организационные, технические и иные меры по защите конфиденциальной информации, принимаемые ее обладателем на основании закона или договора.

1.13. В Управлении ДИТИС АМО ГО «Сыктывкар» обработка конфиденциальной информации может осуществляться исключительно в целях выполнения трудового договора, в иных, предусмотренных законодательством случаях.

1.15. Работу по организации и защите персональных данных Управления ДИТИС АМО ГО «Сыктывкар» координирует начальник Управления.

1.16. Ответственность за обеспечение безопасности персональных данных в информационной системе персональных данных Управления ДИТИС АМО ГО «Сыктывкар» возлагается на руководителя группы кадровой работы и делопроизводства.

1.17. Каждый работник, получающий доступ к конфиденциальной информации, в том числе к персональным данным, подписывает обязательство о неразглашении конфиденциальной информации, в том числе сведений о персональных данных, а также об ответственности в случае нарушения требований действующего законодательства в сфере защиты конфиденциальной информации.

2. Цели защиты конфиденциальной информации

Основными целями защиты конфиденциальной информации в Управлении ДИТИС АМО ГО «Сыктывкар» являются:

- предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения работниками;
- предотвращение несанкционированного уничтожения, искажения, подделки, копирования, распространения, блокирования информации в информационных системах, установленных в Управлении ДИТИС АМО ГО «Сыктывкар» и администрации МО ГО «Сыктывкар»;
- предотвращение утрат, уничтожения или сбоев функционирования носителей информации;
- предотвращение неправомерного или случайного доступа к защищаемой информации;
- обеспечение полноты, целостности, достоверности защищаемой информации;
- сохранение возможности управления процессом обработки и пользования защищаемой информацией.

3. Меры, принимаемые для защиты конфиденциальной информации

3.1. В целях установления режима ограниченного доступа и конфиденциальности сведений в Управлении ДИТИС АМО ГО «Сыктывкар» уполномоченное должностное лицо принимает следующие меры:
- осуществляет разработку локальных нормативных актов и инструкций по обеспечению защиты конфиденциальной информации и регламентации конфиденциального делопроизводства;
- заключает договоры (в том числе трудовые) с условием о сохранении и обеспечении конфиденциальности информации;
- обеспечивает ограничение доступа к защищаемой информации, оформляет допуск к такой информации, а также осуществляет учёт лиц, получающих доступ к такой информации;
- организует работу персонала с конфиденциальной информацией, в том числе с материальными носителями такой информации;

- организует обучение и проверку знаний по обеспечению режима конфиденциальности информации;
- принимает необходимые технические меры, направленные на ограничение доступа посторонних лиц к защищаемой информации;
- организует уничтожение конфиденциальной информации;
- принимает в установленном порядке меры по приостановлению или прекращению обработки конфиденциальной информации, осуществляемой с нарушением требований законодательства;
- проводит служебные проверки в целях установления виновных лиц, допустивших нарушение законодательства о защите конфиденциальной информации, и последующего привлечения их к дисциплинарной ответственности;
- обеспечивает невозможность несанкционированного доступа к документам, содержащим конфиденциальную информацию;
- обеспечивает хранение конфиденциальной информации в порядке, исключающем их утрату или их неправомерное использование.

3.2. Допуск к информации ограниченного доступа включает в себя:
- ознакомление работника с законодательством о защите конфиденциальной информации, об ответственности за его нарушение и с локальными нормативными актами о защите конфиденциальной информации в Управлении ДИТИС АМО ГО «Сыктывкар»;
- принятие работником на себя обязанности по обеспечению конфиденциальности информации, полученной при осуществлении своей трудовой функции в Управлении ДИТИС АМО ГО «Сыктывкар», а также после прекращения трудовых отношений на период действия режима конфиденциальности данной информации;
- прохождение обучения и проверки знаний требований по обеспечению конфиденциальности защищаемой информации.

4. Обязанности работников по защите конфиденциальной информации

4.1. Работники Управления ДИТИС АМО ГО «Сыктывкар», получившие доступ к конфиденциальной информации, обязуются обеспечивать защиту такой информации.

4.2. В целях обеспечения конфиденциальной информации, работник обязан:

- знать и соблюдать требования по получению, обработке, передаче, хранению, конфиденциальной информации, предусмотренные нормативными правовыми актами, соглашениями, должностной инструкцией, локальными нормативными актами о защите конфиденциальной информации в Управлении ДИТИС АМО ГО «Сыктывкар» и трудовым договором;
- знать какие конкретно сведения подлежат защите, а также строго соблюдать правила пользования ими;
- принимать меры по установлению и сохранению режима конфиденциальности, предусмотренные нормативными правовыми актами о защите конфиденциальной информации в Управлении ДИТИС АМО ГО «Сыктывкар»;
- не использовать конфиденциальную информацию ограниченного доступа в целях, не связанных с осуществлением трудовой функции;
- не разглашать конфиденциальную информацию, а также не совершать иных деяний, влекущих уничтожение или утрату такой информации;
- не допускать передачу конфиденциальной информации по телефону или факсу;
- незамедлительно сообщать об утрате или несанкционированном уничтожении конфиденциальной информации своему непосредственному руководителю, а также об иных обстоятельствах, создающих угрозу сохранения конфиденциальности такой информации.

4.3. При прекращении трудовых отношений с Управлением ДИТИС АМО ГО «Сыктывкар» работник обязан сдать все материальные носители защищаемой информации, а также ключи от помещений и шкафов, в которых они хранятся.

4.4. Непосредственный руководитель структурного подразделения, в котором

уволился работник, обязан в письменном виде сообщить об увольнении специалисту по информационной безопасности и защите персональных данных.

5. Требования по получению, обработке, хранению и использованию конфиденциальной информации.

5.1. Обработка и хранение конфиденциальной информации осуществляется в таком порядке и таким способом, которые исключают возможность доступа к ней неуполномоченных лиц.

5.2. Не допускается передача и выдача документов, содержащих сведения конфиденциального характера неуполномоченным лицам без законных на то оснований.

5.3. Использование конфиденциальной информации допускается только в служебных целях.

5.4. Хранение конфиденциальной информации осуществляется в порядке, исключающем ее утрату, неправомерное использование или получение доступа неуполномоченными лицами.

5.5. Все документы, содержащие сведения конфиденциального характера должны храниться в сейфах, шкафах, оборудованных замками либо закрытых и опечатанных помещениях.

5.6. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

6) подпись субъекта персональных данных.

6. Организация конфиденциального делопроизводства

6.1. Сведения, составляющие конфиденциальную информацию могут быть выражены в письменной, устной и электронной формах. Конфиденциальная информация, ставшая известной работнику из письменных, устных и электронных источников, охраняется равным образом.

6.2. Все документы, содержащие конфиденциальную информацию должны сохраняться в режиме конфиденциальности и быть доступными только тем лицам, которые имеют допуск к такой информации в силу исполнения ими своих должностных обязанностей.

6.3. Организация конфиденциального делопроизводства должна исключать ознакомление с информацией иных лиц, не имеющих такого доступа.

6.4. Приказом директора по каждому структурному подразделению назначается лицо, ответственное за учет, хранение и использование конфиденциальной информации.

6.5. Контроль за порядком допуска и работы с конфиденциальной информацией осуществляет руководитель структурного подразделения, в котором осуществляется работа и хранение информации, относящейся к конфиденциальной.

6.6. В случае необходимости оперативного доведения до заинтересованных лиц сведений конфиденциального характера руководителем структурного подразделения ставится резолюция, которая должна содержать:

- перечень фамилий работников, обязанных ознакомиться с документами или их исполнить, срок исполнения, другие указания, подпись руководителя и дату. Руководитель может при необходимости предусмотреть ограничения в доступе конкретных работников к определенным сведениям.

6.7. При работе с документами, содержащими сведения конфиденциального характера, запрещено:

- делать выписки в целях, не связанных с осуществлением трудовой функции;
- знакомить с такими документами, в том числе в электронном виде, других лиц, не имеющих соответствующего доступа;
- использовать информацию из таких документов в открытых сообщениях, докладах, переписке, рекламных изданиях (такое использование допускается только при условии обезличивания информации);
- оставлять на рабочем месте документы и иные носители конфиденциальной информации;
- не допускать к компьютерам, содержащим конфиденциальную информацию, посторонних лиц;
- не оставлять включенными компьютеры, содержащие конфиденциальную информацию.

6.8. Передача документов, содержащих конфиденциальную информацию, неуполномоченным лицам допускается, если обработка необходима:

- для исполнения гражданско-правового договора и в соответствии с условиями договора;

- для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица;

- для защиты жизни или жизненно важных интересов гражданина;

- для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы граждан;

- в интересах гражданина и с его письменного согласия;

- для иных целей, предусмотренных законодательством РФ.

6.11. Уничтожение документов, содержащих конфиденциальную информацию осуществляется в следующими способами: сжигание, плавление, шредирование, химическая обработка. В каждом случае уничтожения составляется акт.

6.12. Проверка соблюдения требований настоящего Положения осуществляется в соответствии с Правилами осуществления внутреннего контроля.

7. Ответственность за нарушение режима конфиденциальности

7.1. К способам нарушения режима конфиденциальности относятся:

- разглашение конфиденциальной информации, обладание которыми входит в круг служебных обязанностей сотрудника, другим сотрудникам, у которых в силу своего служебного положения нет к ним доступа, а также третьим лицам, не являющимся сотрудниками Управления ДИТИС АМО ГО «Сыктывкар»;

- разглашение сведений, которые были получены случайным образом, сотрудникам, не имеющим доступа к данной информации, а также третьим лицам, не являющимся сотрудниками Управления ДИТИС АМО ГО «Сыктывкар»;

- неправомерное использование конфиденциальной информации;

- утрата документов и иных материальных носителей, содержащих сведения конфиденциального характера;

- неправомерное уничтожение документов, содержащих сведения конфиденциального характера;

- нарушение требований хранения документов, содержащих сведения конфиденциального характера;

- получение информации, составляющей коммерческую тайну, с использованием специальных средств или путем противоправных действий;

- другие нарушения требований законодательства и настоящего Положения.

7.2. За разглашение конфиденциальной информации, а также за нарушение порядка обращения с документами, содержащими сведения конфиденциального характера, работник организации несут предусмотренную законодательством Российской Федерации ответственность и может быть привлечен к дисциплинарной, административной или уголовной ответственности.