



**АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТВЕРСКОЙ ОБЛАСТИ «КАЛИНИНСКИЙ РАЙОН»**

РАСПОРЯЖЕНИЕ

«27 » января 2014

№ 17-р

Тверь

Об утверждении Порядка доступа сотрудников Администрации в помещения, предназначенные для обработки персональных данных

В целях обеспечения защиты информации и режима безопасности проводимых работ, в соответствии с требованиями руководящих документов ФСТЭК России по защите информации, обрабатываемой на объектах информатизации администрации муниципального образования Тверской области «Калининский район»,

1. Утвердить Порядок доступа сотрудников администрации муниципального образования Тверской области «Калининский район» в помещения, предназначенные для обработки персональных данных.

2. Отделу организационной и кадровой работы администрации (Беловцева А.Н.) довести настоящее распоряжение до заместителей главы администрации, управляющего делами администрации, руководителей отраслевых (функциональных) органов администрации под роспись.

3. Контроль за исполнением настоящего распоряжения возложить на управляющего делами администрации Грачеву Л.Г.

4. Отделу по обеспечению деятельности администрации (Модестова Н.В.) разместить настоящее распоряжение на официальном сайте администрации.

5. Распоряжение вступает в силу со дня его подписания.

Глава администрации

О.В. Гончаров

Порядок доступа сотрудников администрации муниципального образования Тверской области «Калининский район» в помещения, предназначенные для обработки персональных данных

1. Настоящая инструкция определяет порядок доступа сотрудников администрации муниципального образования Тверской области «Калининский район» (далее - Администрация) и других лиц в помещения, предназначенные для обработки персональных данных.

2. Ответственность за обеспечение исполнения требований настоящей инструкции несет ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных.

3. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

4. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только сотрудники и должностные лица, получившие доступ к персональным данным.

5. Нахождение в помещениях, в которых ведется обработка персональных данных лиц, не являющихся сотрудниками и должностными лицами, получившими доступ к персональным данным, возможно только в присутствии сотрудников и должностных лиц, получивших доступ к персональным данным на время, ограниченное необходимостью решения вопросов, связанных с исполнением должностных функций.

6. Присутствие других лиц в данных помещениях допускается в той мере, в какой этого требуют технологические процессы обработки персональных данных. Доступ в помещения Администрации осуществляется только в сопровождении сотрудника Администрации, который предварительно производит оценку целесообразности и требуемого времени нахождения лица в помещении, а также проверяет документы, удостоверяющие личность.

7. Сотрудники и должностные лица, получившие доступ к персональным данным не должны покидать помещение, в котором ведется обработка персональных данных, оставляя в нем без присмотра посторонних

лиц, включая сотрудников, не уполномоченных на обработку персональных данных.

8. Доступ в помещения, в которых осуществляется обработка персональных данных, разрешается только в рабочее время.

9. Доступ в помещения, в которых осуществляется обработка персональных данных, в нерабочее время возможен только по письменной заявке работника, согласованной с его непосредственным руководителем и имеющей разрешающую резолюцию Главы Администрации. Данные заявки хранятся у лица, ответственного за организацию обработки персональных данных в Администрации.

10. В помещениях, в которых происходит обработка и хранение персональных данных, запрещено использование не предусмотренных служебными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

11. Для предотвращения несанкционированного доступа к информации, содержащей ПДн, осуществляется контроль деятельности рабочих. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных Главой Администрации или его заместителями. Работы проводятся под контролем сотрудников Администрации.

12. Для исключения несанкционированного доступа к информации, содержащей ПДн, организована охрана помещений Администрации. Режим работы охраны устанавливается Регламентом работы Администрации.

13. Уборка помещения выполняется обслуживающим персоналом под контролем сотрудников, имеющих право доступа в данное помещение. Во время уборки в помещении должна быть приостановлена работа с ПДн, должны быть выключены все АРМ, на которых хранятся ПДн, носители, содержащие ПДн должны быть убраны в сейф.

14. После окончания рабочего дня дверь каждого помещения закрывается на ключ, при этом запрещается оставлять ключ в замке помещения.

15. В нерабочее время помещения, в которых ведется обработка персональных данных, хранятся документы, содержащиеся персональные данные, должны закрываться на ключ и сдаваться под охрану.

16. По окончании рабочего дня помещения, в которых ведется обработка ПДн, и установленные в них хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале ответственному за организацию обработки персональных данных или лицу, им уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

17. Ключи от помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ, в опечатанном виде должны быть

сданы под расписку в соответствующем журнале службе охраны. Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников Администрации, ответственных за эти хранилища.

18. При утрате ключа от хранилища или от входной двери в помещение, в котором ведется обработка ПДн, замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный за безопасность персональных данных.

19. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за безопасность персональных данных. Ответственный за безопасность персональных данных должен составить акт и принять, при необходимости, меры к локализации последствий несанкционированного доступа к ПДн.

20. Контроль соблюдения настоящего Порядка осуществляется лицом, ответственным за организацию обработки персональных данных Администрации.

21. Лицо, ответственное за организацию обработки персональных данных, в случае установления факта нарушения сотрудником Администрации настоящего Порядка проводит с ним разъяснительную работу, а в случае неоднократного нарушения – уведомляет Главу Администрации.
