

Государственное казенное учреждение социального обслуживания
Владимирской области
«Владимирский социально-реабилитационный центр
для несовершеннолетних»

П Р И К А З

17.11.2017.

№ 98

*Об утверждении Порядка
доступа сотрудников учреждения в
помещения, в которых ведется
обработка персональных данных*

В соответствии с постановлением Правительства Российской Федерации от 21.03.2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» **п р и к а з ы в а ю:**

1. Утвердить с 20.11.2017 г. Порядок доступа сотрудников государственного казенного учреждения социального обслуживания Владимирской области «Владимирский социально-реабилитационный центр для несовершеннолетних» в помещения, в которых ведется обработка персональных данных (Приложение № 1).

2. Заведующему отделением организационно-методической работы Фоминой М.М. опубликовать настоящий приказ на сайте учреждения не позднее 10 дней со дня его подписания.

3. Специалисту по кадрам Смирновой Л.Н. ознакомить сотрудников учреждения с настоящим приказом под роспись (Приложение № 2).

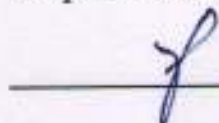
4. Контроль за соблюдением приказа оставляю за собой.

И.о. директора

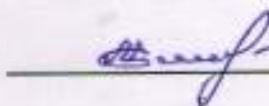


Т.А. Мачинскене

С приказом ознакомлены:



М.М. Фомина



Л.Н. Смирнова

Порядок доступа сотрудников учреждения в помещения, в которых ведется обработка персональных данных

1. Настоящий Порядок доступа сотрудников государственного казенного учреждения социального обслуживания Владимирской области «Владимирский социально-реабилитационный центр для несовершеннолетних» (далее - Учреждение) в помещения, в которых ведется обработка персональных данных, разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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» и другими нормативными правовыми актами.

2. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется только в защищенных помещениях. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

3. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

4. Доступ сотрудников Департамента и иных лиц в помещения, в которых ведется обработка персональных данных, осуществляется с учетом обеспечения безопасности информации и исключения доступа к персональным данным третьих лиц.

Доступ в помещения, в которых ведется обработка персональных данных, предоставляется:

- лицу, ответственному за организацию обработки персональных данных;
- сотрудникам, осуществляющим обработку персональных данных;
- иным лицам в случае необходимости по согласованию с заведующим отделением, в котором происходит обработка персональных данных.

6. Нахождение лиц в помещениях Учреждения, не являющихся уполномоченными лицами на обработку персональных данных, возможно только в сопровождении ответственных сотрудников Учреждения на время, ограниченное необходимостью решения вопросов, связанных с выполнением трудовых функций и (или) осуществлением полномочий в рамках договоров, заключенных с другими организациями.

7. Во время пребывания лиц в помещениях Учреждения, не являющихся полномочными лицами на обработку персональных данных необходимо прекратить обработку персональных данных, предотвратить либо прекратить вывод на экран мониторов информации с персональными данными, если данные лица находятся в непосредственной близости от монитора, либо от материальных носителей информации персональных данных.

8. В нерабочее время помещения Учреждения, в которых ведется обработка персональных данных, хранятся документы, содержащие персональные данные, должны закрываться на ключ и должны быть опечатаны, ставиться на сигнализацию (при наличии).

9. Опечатывание помещений производится должностными лицами, определяемыми приказом директора Учреждения (в период отсутствия лица его замещающее), при отсутствии должностного лица опечатывание проводит лицо его замещающее.

10. Уборка помещений, в которых ведется обработка персональных данных, хранятся документы и носители информации, содержащие персональные данные, должна производиться в присутствии сотрудников, производящих обработку персональных данных ознакомленных с нормативными документами Учреждения по информационной безопасности персональных данных.

11. Установка нового оборудования, его замена или ремонт в помещениях, в которых ведется обработка персональных данных, хранятся документы и носители информации, содержащие персональные данные, должны проводиться по согласованию с администратором безопасности информационных систем и только в присутствии администратора безопасности информационных систем или сотрудника, осуществляющего обработку персональных данных в помещении.

12. В помещения Учреждения, где размещены технические средства, позволяющие осуществить обработку персональных данных, а также хранятся носители информации, допускаются только сотрудники Учреждения, уполномоченные на обработку персональных данных.

13. Доступ в кабинет специалиста по кадрам разрешается только специалисту по кадрам (в период отсутствия лицу его замещающему), ответственному за организацию обработки персональных данных.

14. Документы, содержащие персональные данные сотрудника (работника) хранятся на бумажных носителях в специально оборудованных и запирающихся шкафах или сейфах, обеспечивающих защиту от несанкционированного доступа. Хранение персональных данных на АРМ осуществляется только на защищенных паролями доступа АРМ, информационная безопасность которых обеспечивается комплексом мер защиты информации, утвержденных требованиями к настройкам АРМ по минимизации угроз утечки, несанкционированного доступа, изменения, удаления, блокирования персональных данных в информационных системах Учреждения, а также федеральным законодательством.

15. Ответственность за организацию доступа в помещения Учреждения, в которых ведется обработка персональных данных, являются заведующие отделениями, начальники отделов, ответственные специалисты, осуществляющими обработку ПДн, Учреждения.

16. Внутренний контроль за соблюдением порядка доступа в помещения Учреждения, в которых ведется обработка ПДн, проводится лицом, ответственным за обработку ПДн, заведующими отделениями, администратором безопасности информационных систем, ответственными специалистами, осуществляющими обработку ПДн.