**Брянская городская администрация**
**Муниципальное бюджетное дошкольное образовательное учреждение**
**детский сад № 129 «Подсолнушек» г. Брянска**

1-й проезд Станке Димитрова, дом 3а, г. Брянск, 241037
Телефон 8(4832) 64-56-58, 64-99-31; E-mail: podsolnushekl29@rambler.ru
ИНН/КПП 3234037957/325701001, ОГРН 1023202748458

УТВЕРЖДАЮ
Заведующий
МБДОУ детский сад №129
«Подсолнушек» г. Брянска
_____В.С.Мильшина
02.02.2026 г. приказ № 11/1

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №129 "ПОДСОЛНУШЕК" Г. БРЯНСКА

Подписано цифровой печатью: МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №129 "ПОДСОЛНУШЕК" Г. БРЯНСКА
Дата:2026.02.02 10:18:16 +03'00'

# ПОРЯДОК ДОСТУПА
## сотрудников муниципального бюджетного дошкольного образовательного учреждения детский сад № 129 «Подсолнушек» г. Брянска в помещения, в которых ведется обработка персональных данных

1. Настоящий Порядок доступа сотрудников муниципального бюджетного дошкольного образовательного учреждения детский сад № 129 «Подсолнушек» г. Брянска (далее - ДОУ) в помещения, в которых ведется обработка персональных данных, разработан в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 года № 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 в области защиты персональных данных.

2. Целью настоящего Порядка является исключение несанкционированного доступа к персональным данным (далее - ПДн) субъектов ПДн в ДОУ

3. Персональные данные относятся к конфиденциальной информации.

Сотрудники ДОУ, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без письменного согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

4. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе,

установлением правил доступа в помещения, где обрабатываются персональные данные в информационной системе персональных данных и без использования средств автоматизации.

5. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется только в охраняемых помещениях. 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.

6. Входные двери помещений должны быть оборудованы замками, гарантирующими надежную защиту помещений в нерабочее время.

7. На каждый механический замок входной двери помещения должно быть не менее 2 -х экземпляров ключей. Один ключ должен находиться у ответственного за помещение, а резервный комплект ключей сдаётся на пост охраны в опечатанном пенале.

8. Окна помещений должны быть оборудованы сигнализацией на вскрытие, разбитие стекла и шторами.

9. Обращается особое внимание, что при работе с информацией персональных данных двери помещений должны быть всегда закрыты.

10. При отсутствии в помещениях сотрудников они должны быть закрыты.

11. В помещении устанавливаются сейфы (металлические шкафы), оборудованные опечатывающими устройствами, предназначенные для хранения носителей информации, в т.ч. ключевой информации и документов по персональным данным и других рабочих материалов.

12. По окончании рабочего дня помещения закрываются и опечатываются.

13. В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения, помещение вскрывается комиссией, не менее 2-х человек, из числа первого прибывшего сотрудника ДОУ и дежурного охранника.

14. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Сотрудникам ДОУ, находящимся на работе, производить постоянный контроль за помещениями, в которых находятся автоматизированные рабочие места, хранятся материальные хранители информации.

15. Доступ сотрудников ДОУ 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.

16. 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 ДОУ или лицом, ответственным за обработку персональных данных, в котором происходит обработка персональных данных.

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

18. Во время пребывания лиц в помещениях ДОУ ,не являющихся уполномоченными 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 персональных данных (различные списки и реестры сотрудников ДОУ, личные дела, приказы и др. материальных носителей информации).

19. Уборка помещений, в которых ведется обработка персональных данных, и хранятся документы, содержащие персональные данные, должна производиться в присутствии сотрудников, проводящих обработку персональных данных.

20. 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 сотрудником, в котором происходит обработка персональных данных и только в присутствии руководства ДОУ.

21. В помещения ДОУ, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только сотрудники ДОУ, уполномоченные на обработку персональных данных.

22. Доступ в помещение кадрового подразделения производится только сотрудниками кадрового подразделения и доступ третьих лиц и сотрудников ДОУ должен быть ограничен.

Документы, содержащие персональные данные сотрудника (работника), воспитанника ДОУ (Личное дело: содержащее копии личных документов (паспорт, диплом, военный билет и т.п.), заявления, трудовая книжка, экземпляр трудового договора, приказ о приеме на работу и т.д.) хранятся на бумажных носителях в специально оборудованных и запирающихся шкафах и сейфах, обеспечивающих защиту от несанкционированного доступа.

Хранение персональных данных на автоматизированном рабочем месте (далее - 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 министерства, а так же действующим законодательством.

23. Вскрытие и закрытие (опечатывание) помещения производится работниками ДОУ, работающими в данном помещении.

24. Перед закрытием помещения по окончании рабочего дня сотрудники обязаны:

- навести порядок на рабочем месте, закрыть на замки и опечатать сейфы и шкафы; закрыть окна, форточки;
- отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;
- закрыть помещение на замок, опечатать;
- сдать ключ от помещения на пост охраны.

25. Перед вскрытием помещения работник ДОУ, имеющий право вскрытия помещения, обязан:

- получить ключи от помещения на посту охраны под роспись;
- внешним осмотром убедиться в целостности двери и замка;
- открыть дверь и осмотреть помещение, наличие и целостность печатей на сейфах и шкафах.

26. При обнаружении неисправности двери и запирающих устройств сотрудник ДОУ обязан:

- не вскрывая помещение доложить заведующему (заместителю заведующего, ответственному лицу за защиту ПДн);
- вызвать дежурного, охраняющего объект;
- в присутствии вышеуказанных лиц вскрыть помещение и осмотреть его;
- составить акт о выявленных нарушениях и передать его заведующему ДОУ для проведения служебной проверки.

27. Ответственными за организацию доступа в помещения ДОУ, в которых ведется обработка персональных данных, являются лицо ответственное за организацию обработки ПДн,

28. Внутренний контроль за соблюдением порядка доступа в помещения ДОУ, в которых ведется обработка персональные данные (далее - ПДн), проводится лицом ответственным за организацию обработки ПДн, а так же заведующим.