

УТВЕРЖДЕНО

приказ директора Могилевского
областного центра
олимпийского резерва по легкой
атлетике и игровым видам
спорта от _____ № _____

ПОЛОЖЕНИЕ

об обработке
персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Настоящее Положение определяет порядок:
обработки персональных данных в Могилевском областном центре олимпийского резерва по легкой атлетике и игровым видам спорта (далее – Учреждение);
доступа к персональным данным, обрабатываемым в Учреждении;
осуществления внутреннего контроля за обработкой персональных данных;
реагирования на нарушения системы защиты персональных данных в Учреждении.

2. ПОРЯДОК ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

15. Доступ в Учреждении к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе), предоставляется:
работникам Учреждения для выполнения должностных обязанностей в объеме, необходимом для надлежащего выполнения этих обязанностей.

ПОРЯДОК ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

22. Для помещений, в которых хранятся и обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащих персональные данные, а также исключается возможность несанкционированного или случайного доступа посторонних лиц.

23. Режим обеспечения безопасности обеспечивается:
оснащением помещения пожарной сигнализацией;
обязательным запираением помещений на ключ, даже при выходе из него в рабочее время;
закрытием шкафов и сейфов, где хранятся носители информации, содержащие персональные данные, на ключ.

24. Доступ в помещения, в которых ведется обработка персональных данных, включая их хранение, предоставляется:

работникам, непосредственно осуществляющим обработку персональных данных;
лицу, ответственному за осуществление внутреннего контроля за обработкой персональных данных;
сотрудникам контролирующих и правоохранительных органов, пожарных и аварийных служб при наличии служебного удостоверения и с

разрешения директора Учреждения (лица, исполняющего обязанности) в сопровождении лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных;

25. Во время пребывания в помещениях иных лиц, не являющихся работниками, непосредственно обрабатывающими персональные данные в Учреждении, обработку персональных данных:

необходимо прекратить;

либо 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.

26. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании рабочего времени работники, имеющие право доступа в помещения, обязаны:

убрать бумажные носители персональных данных и иные материальные носители персональных данных (диски, флеш-карты) в шкафы, закрыть шкафы;

отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

закрыть окна.

27. Уборка помещений, в которых ведется обработка персональных данных, и хранятся документы, содержащие персональные данные, должна производиться в присутствии работников, непосредственно осуществляющих обработку персональных данных.

При невозможности присутствия работников, непосредственно обрабатывающих персональные, в период уборки, в помещениях в открытом доступе не должны находиться документы, содержащие персональные данные.

28. Установка программного обеспечения и (или) его обновление, нового оборудования осуществляется работниками электронно-информационного отдела и в присутствии работника, непосредственного осуществляющего обработку персональных данных.

ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРЕДСТАВИТЕЛЕЙ КОНТРАГЕНТОВ, ГРАЖДАН, ЯВЛЯЮЩИХСЯ СТОРОНОЙ ПО ГРАЖДАНСКО-ПРАВОВОМУ ДОГОВОРУ.

68. Правовыми основаниями обработки персональных данных представителей контрагентов, граждан, являющихся стороной по гражданско-правовому договору, является договор в соответствии с абзацем пятнадцатым статьи 6 Закона.

69. Обработка персональных данных представителей контрагентов, граждан, являющихся стороной по гражданско-правовому договору, осуществляется для целей:

подготовки договора;

заключения договора;

досрочного расторжения договора;

исполнения обязанностей и реализации прав, предусмотренных договором;

исполнения обязательств, предусмотренных законодательными актами; проведения контрольных и надзорных мероприятий.

72. Обработка персональных данных представителей контрагентов, граждан, являющихся стороной по гражданско-правовому договору, осуществляется автоматизированным и неавтоматизированным способом.

73. Неавтоматизированным способом обработка персональных данных представителей контрагентов, граждан, являющихся стороной по гражданско-правовому договору, осуществляется посредством работы с документами на бумажных носителях.

74. Автоматизированным способом обработка персональных данных представителей контрагентов, граждан, являющихся стороной по гражданско-правовому договору, осуществляется с использованием следующих информационных систем (ресурсов):

1С –Предприятие 7.7;

СМДО.

75. Обработка персональных данных в названных в пункте 74 информационных системах (ресурсах) осуществляется на основании разграничения прав доступа пользователей.

76. Доступ к персональным данным представителей контрагентов имеют:

руководители структурных подразделений;

специалист по организации закупок;

юрисконсульт;

работники бухгалтерии;

инструкторы-методисты учебно-спортивного отдела.

77. Работникам, имеющим доступ к персональным данным контрагентов, граждан, являющихся стороной по гражданско-правовому договору, а также работникам, непосредственно обрабатывающим персональные данные, запрещается:

использовать персональные данные в целях, не связанных с целями, указанными в пункте 69, а также в личных целях;

копировать персональные данные для целей, не связанных с целями, указанными в пункте 69, а также в личных целях;

изменять, удалять персональные данные из информационных систем (ресурсов), указанных в пункте 69, без предварительного уведомления ответственного за осуществление внутреннего контроля за обработкой персональных данных.

78. Персональные данные представителей контрагентов, граждан, являющихся стороной по гражданско-правовому договору, в том числе спортсменов-учащихся и их представителей, не распространяются.

80. Работники, непосредственно обрабатывающие персональные данные представителей контрагентов, граждан, являющихся стороной по гражданско-правовому договору, в том числе спортсмены-учащиеся и их представители, в случае предоставления персональных данных третьим лицам обязаны в течение 3 (трех) рабочих дней сообщать об этом

ответственному за осуществление внутреннего контроля за обработкой персональных данных.

81. Хранение персональных данных представителей контрагентов, граждан, являющихся стороной по гражданско-правовому договору, содержащихся в документах на бумажных носителях, осуществляется в:

- бухгалтерии;
- юрисконсульта;
- специалиста по организации закупок;
- учебно-спортивном отделе;

82. Хранение персональных данных представителей контрагентов, граждан, являющихся стороной по гражданско-правовому договору, содержащихся в документах на бумажных носителях осуществляется в закрываемых на ключ шкафах.

83. Срок хранения персональных данных граждан, являющихся стороной по гражданско-правовому договору, составляет 3 года (10 лет со дня проведения последней налоговой проверки).

Срок хранения персональных данных представителей контрагентов составляет 3 года (10 лет со дня проведения последней налоговой проверки).

ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ.

84. Правовые основания и цели обработки персональных данных работников определены в Политике обработки персональных данных работников.

85. Доступ к персональным данным работников имеют:

Директор Учреждения (лицо, исполняющее его обязанности) (к персональным данным всех работников);

Руководители структурных подразделений (к персональным данным своих подчиненных);

87. Предоставление персональных данных работников третьим лицам осуществляется с согласия указанных лиц, за исключением случаев, предусмотренных законодательством, в том числе:

87.1. Фонд социальной защиты населения – в рамках возложенной на Учреждение обязанности представлять в установленном Правилами порядке в органы, осуществляющие персонифицированный учет, достоверные сведения, необходимые для ведения персонифицированного учета согласно части второй статьи 10 Закона Республики Беларусь от 6 января 1999 г. № 230-З «Об индивидуальном (персонифицированном) учете в системе государственного социального страхования». Перечень персональных данных, передаваемых в Фонд социальной защиты населения установлен в статье 6 названного Закона;

87.2. ОАО «АСБ «Беларусбанк» - для зачисления заработной платы передаются следующие персональные данные работников: фамилия, имя, отчество (если таковое имеется), банковские реквизиты (расчетный счет, БИК), сумма заработной платы для зачисления;

87.3. в поликлинику, в зависимости от места жительства работников, – в рамках прохождения обязательных медицинских осмотров, вакцинации работников предоставляются следующие персональные данные работников:

фамилия, имя, отчество (если таковое имеется), сведения о месте работы, сведения о занимаемой должности, адрес регистрации (места жительства);

90. Работники, непосредственно обрабатывающие персональные данные работников, в случае предоставления персональных данных третьим лицам обязаны в течение 3 (трех) рабочих дней сообщать об этом ответственному за осуществление внутреннего контроля за обработкой персональных данных.

91. Сроки хранения персональных данных работников установлен Политикой обработки персональных данных работников.

ПОРЯДОК ВЕДЕНИЯ И ЗАПОЛНЕНИЯ РЕЕСТРА ОБРАБОТОК ПЕРСОНАЛЬНЫХ ДАННЫХ.

92. Для целей упорядочивания обработок персональных данных, контроля за сроками обработки персональных данных, соотношения целей обработки персональных данных и правовых оснований обработки персональных данных в Учреждении ведутся:

92.1. Реестр обработок персональных данных (далее – Реестр) по форме согласно приложению 1;

92.2. Реестр предоставления персональных данных третьим лицам (далее – Реестр предоставления) по форме согласно приложению 2.

93. В Реестр вносятся следующие сведения:

Наименование категории субъекта персональных данных;

Цель обработки персональных данных;

Правовое основание обработки персональных данных;

Категории обрабатываемых персональных данных;

Срок хранения персональных данных;

Лицо (подразделение), непосредственно осуществляющее обработку персональных данных.

94. Правовое основание обработки персональных данных обязательно должно содержать ссылку на положения статей 4, 6, 8 и 9 Закона.

95. В Реестр предоставления вносятся следующие сведения:

Наименование субъекта персональных данных;

Наименование категории субъекта персональных данных;

Категории предоставляемых персональных данных;

Носитель персональных данных (при наличии)

Лицо, которому персональные данные были предоставлены;

Контактные данные лица, которому персональные данные были предоставлены;

Цель предоставления персональных данных;

Правовое основание предоставления персональных данных;

Дата предоставления персональных данных.

96. Предоставление персональных данных между структурными подразделениями Учреждения не вносятся в Реестр предоставления.

97. Ведение Реестра и Реестра предоставления обеспечивается ответственным за осуществление внутреннего контроля за обработкой персональных данных в Учреждении.

98. При необходимости ответственным за осуществление внутреннего контроля за обработкой персональных данных в Учреждении могут вноситься изменения в формы Реестра и Реестра предоставления.

99. Сведения для Реестра и Реестра предоставления предоставляются руководителями структурных подразделений по требованию ответственного за осуществление внутреннего контроля за обработкой персональных данных в Учреждении в течение 5 (пяти) рабочих дней со дня требования о предоставлении информации для названных реестров.

100. Работники, непосредственно осуществляющие обработку персональных данных, обязаны в течение 3 (трех) рабочих дней со дня предоставления персональных данных третьим лицам сообщать о таком предоставлении ответственному за осуществление внутреннего контроля за обработкой персональных данных в Учреждении.

101. Пересмотр Реестр и Реестра предоставления с целью его актуализации производится ответственным за осуществление внутреннего контроля за обработкой персональных данных в Учреждении по мере необходимости, но не реже одного раза в год.

ПОРЯДОК ПРЕКРАЩЕНИЯ ОБРАБОТКИ.

102. Обработка персональных данных в Учреждении прекращается:

- по достижении цели обработки персональных данных, указанных в Политиках обработки персональных данных в Учреждении;
- при обнаружении неправомерной обработки персональных данных;
- по требованию Национального центра защиты персональных данных Республики Беларусь;
- по требованию субъекта персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку персональных данных;
- в случае истечения сроков хранения персональных данных;
- в случае прекращения деятельности Учреждения.

103. Прекращение обработки персональных данных осуществляется работником (лицом), непосредственно осуществляющим обработку персональных данных.

104. После прекращения обработки персональных данных в случае достижения целей обработки, отзыва субъекта персональных данных согласия на обработку персональных данных, по требованию субъекта или в случае прекращения деятельности Учреждения персональные данные подлежат удалению, уничтожению или блокированию (в случае невозможности удаления или уничтожения).

105. В случае прекращения обработки персональных данных при обнаружении неправомерной обработки персональных данных по требованию ответственного за осуществление внутреннего контроля за обработкой персональных данных в Учреждении обработка персональных данных приостанавливается работником, непосредственно осуществляющим обработку персональных данных, до проведения расследования при наличии нарушения системы защиты персональных данных.

106. В случае прекращения обработки персональных данных по требованию Национального центра защиты персональных данных Республики Беларусь обработка персональных данных приостанавливается до выполнения всех требований названного Центра и (или) устранения выявленных нарушений.

107. Если прекращение обработки персональных данных осуществлено на основании заявления субъекта персональных данных с требованием о прекращении обработки его персональных данных, об отзыве согласия на обработку персональных, то лицо, ответственное за осуществление внутреннего контроля за обработкой персональных данных в Учреждении, после рассмотрения такого заявления принимает решение о мерах по удалению, уничтожению или блокированию персональных данных в пятнадцатидневный срок после получения заявления субъекта персональных данных.

О своем решении и необходимых мерах по удалению, уничтожению или блокированию персональных данных ответственный за осуществление внутреннего контроля за обработкой персональных данных в Учреждении сообщает работнику, непосредственно осуществляющему обработку персональных данных.

108. Прекращение обработки персональных данных по достижении целей обработки осуществляется не позднее 3 (трех) календарных со дня достижения цели обработки или окончания срока хранения персональных данных. Персональные данные удаляются (уничтожаются), при невозможности – блокируются.

109. По результатам прекращения обработки персональных данных лицом, ответственным за осуществление внутреннего контроля за обработкой персональных данных, составляется акт по форме согласно приложению 3, который подписывается лицом, ответственным за осуществление внутреннего контроля за обработкой персональных данных, работником, непосредственно осуществляющим обработку персональных данных и директором Учреждения (лицом, исполняющим его обязанности). При необходимости акт может подписываться иными лицами.

111. Документы на бумажных, иных материальных носителях, содержащие персональные данные, после прекращения обработки персональных данных уничтожаются с использованием shreddera.

112. В случае, если документы на бумажных, иных материальных носителях, содержащие персональные данные, содержат, в том числе, иную информацию, необходимую для осуществления деятельности Учреждения, лицом, ответственным за осуществление внутреннего контроля за обработкой персональных данных, производится удаление или обезличивание части персональных данных, если это допускается материальным носителем, способом, исключающим дальнейшую обработку этой части персональных данных, с сохранением возможности обработки иной части персональных данных.

ПОРЯДОК ВНУТРЕННЕГО КОНТРОЛЯ ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ.

113. Внутренний контроль за обработкой персональных данных в Учреждении (далее – внутренний контроль) осуществляется лицом, ответственным за осуществление внутреннего контроля, в форме:

плановых проверок соблюдения работниками законодательства о персональных данных, требований настоящего Положения и иных локальных правовых актов в сфере защиты персональных данных (далее – плановые проверки);

внеплановых проверок соблюдения работниками, непосредственно осуществляющими обработку персональных данных, законодательства о персональных данных, требований настоящего Положения и иных локальных правовых актов в сфере защиты персональных данных (далее – внеплановые проверки);

организации и проведения проверки знаний работников по вопросам обработки и защиты персональных данных.

114. План внутреннего контроля (далее – план) на очередной год формируется лицом, ответственным за осуществление внутреннего контроля, до 25 декабря текущего года, утверждается директором Учреждения (лицом, исполняющим его обязанности) и доводится до сведения работников.

115. В план включаются сведения:

о проведении плановых проверок;

о проведении проверки знаний работников по вопросам обработки и защиты персональных данных;

о проведении обучения работников по вопросам обеспечения защиты персональных данных;

117. При проведении проверки лицом, ответственным за осуществление внутреннего контроля за обработкой персональных данных, оцениваются:

соответствие обработки персональных данных заявленным целям;

избыточность персональных данных по отношению к заявленным целям обработки;

правовые основания обработки персональных данных;

своевременность удаления (уничтожения) персональных данных, срок хранения которых истек;

соблюдение порядка доступа к персональным компьютерам работников;

соблюдение порядка доступа в помещения, в которых осуществляется обработка персональных данных, в том числе их хранение;

соблюдение мер по хранению персональных данных, обрабатываемых в информационных системах (ресурсах);

соблюдение мер по хранению персональных данных, содержащихся в документах на бумажных носителях.

118. По результатам плановой или внеплановой проверки составляется акт в двух экземплярах, в котором должны быть отражены:

соответствие (несоответствие) принятых проверяемым работником мер по обеспечению им защиты персональных данных требованиям законодательства о персональных данных, настоящего Положения и иных локальных правовых актов;

экспертная оценка лица, ответственного за осуществление внутреннего контроля, о достаточности принятых проверяемым работником мер для защиты персональных данных;

выявленные нарушения законодательства о персональных данных либо вывод об отсутствии таких нарушений.

119. В случае выявления нарушений законодательства о персональных данных, требований настоящего Положения и иных локальных правовых актов, обработка персональных данных незамедлительно прекращается посредством ее приостановления по требованию лица, ответственного за осуществление внутреннего контроля, о чем сообщается директору Учреждения (лицу, исполняющему его обязанности) в день прекращения обработки персональных данных.

120. Акт плановой проверки составляется в течение пяти рабочих дней со дня ее окончания и подписывается лицом, ответственным за осуществление внутреннего контроля, и передается директору Учреждения (лицу, исполняющему его обязанности).

121. В случае выявления по результатам плановой проверки нарушений законодательства о персональных данных, требований настоящего Положения, иных локальных правовых актов, отраженных в акте плановой или внеплановой проверки, в течение трех рабочих дней со дня окончания проверки приказом директора Учреждения (лица, исполняющего его обязанности):

определяются конкретные меры об устранении выявленных нарушений и (или) приостановлении (прекращении) обработки персональных данных в информационном ресурсе (системе) с указанием действий, которые должны быть приостановлены (прекращены) и устанавливается срок такого устранения и (или) приостановления (прекращения), который не может превышать одного месяца;

решается вопрос о привлечении лиц, виновных в нарушении законодательства о защите персональных данных, к ответственности в соответствии с законодательными актами;

определяются лица, осуществляющие контроль за реализацией предусмотренных в приказе мер.

122. Организация и проведение проверки знаний работников по вопросам обработки и защиты персональных данных осуществляется лицом, ответственным за осуществление внутреннего контроля за обработкой персональных данных.

Проверка знаний работников по вопросам обработки и защиты персональных данных осуществляется один раз в три года.

123. Проверке знаний работников по вопросам обработки и защиты персональных данных должно предшествовать обучение работников по вопросам обработки и защиты персональных данных.

Обучение работников по вопросам обработки и защиты персональных данных может быть организовано в форме лекций, просмотра обучающих видео-программ и т.д.

124. Формы и методы проверки знаний работников по вопросам обработки и защиты персональных данных определяются лицом, ответственным за осуществление внутреннего контроля за обработкой персональных данных, самостоятельно.

125. По результатам проведения проверки знаний работников по вопросам обработки и защиты персональных данных составляется акт проведения проверки знаний, в котором отражаются сведения о:

дате проведения проверки знаний по вопросам обработки и защиты персональных данных;

форме проведения проверки знаний по вопросам обработки и защиты персональных данных;

работниках, прошедших проверку знаний по вопросам обработки и защиты персональных данных;

работниках, не прошедших проверку знаний по вопросам обработки и защиты персональных данных;

сроках повторной проверки знаний работников, не прошедших проверку знаний по вопросам обработки и защиты персональных данных.

126. Акт подписывается лицом, ответственным за осуществление внутреннего контроля за обработкой персональных данных, директором Учреждения (лицом, исполняющим его обязанности), работниками, участвовавшими в проверке знаний по вопросам обработки и защиты персональных данных.

РЕАГИРОВАНИЕ НА НАРУШЕНИЕ СИСТЕМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.

127. О нарушении системы защиты персональных данных в информационных системах (ресурсах) Учреждения может свидетельствовать следующее:

признаки наличия на компьютере вредоносной программы;

обнаружение попыток несанкционированного доступа к компьютеру, программному обеспечению, локальной сети, информационным системам (ресурсам), базам и банкам данных, содержащим персональные данные;

уведомление антивирусного средства о нарушении информационной безопасности на компьютере;

уведомление об отклонениях в работе установленных на компьютере системных или прикладных программ;

наличие файлов с нечитаемыми названиями;

неоднократные неудачные попытки авторизации на компьютере;

невозможность аутентификации в информационной системе (ресурсе).

128. О нарушении системы защиты персональных данных, содержащихся в документах на бумажных носителях и (или) иных материальных, может свидетельствовать следующее:

несоблюдение правил хранения персональных данных, содержащихся в документах на бумажном и (или) ином материальном носителе;

визуальные признаки повреждения места хранения персональных данных, содержащихся в документах на бумажных и (или) иных материальных носителях;

визуальные признаки нарушения доступа в помещения, где осуществляется обработка персональных данных, в том числе их хранение.

129. При возникновении нарушения системы защиты персональных данных работник незамедлительно информирует об этом директора Учреждения (лицо, исполняющее его обязанности), лицо, ответственное за осуществление внутреннего контроля за обработкой персональных данных, которыми в соответствии, в том числе с привлечением, при необходимости иных лиц:

проводится оценка риска и последствий нарушения системы защиты персональных данных;

вырабатывается стратегия реагирования на нарушение системы защиты персональных данных;

принимаются все возможные меры по устранению (при невозможности устранения – минимизации) последствий нарушений системы защиты персональных данных и исключению подобного в дальнейшем;

производится документирование нарушения системы защиты персональных данных с составлением заключения по факту его возникновения.

130. В течение трех рабочих дней после обнаружения нарушения системы защиты персональных данных Учреждения письменным уведомлением сообщает о нарушении системы защиты персональных данных в Национальный центр защиты персональных данных Республики Беларусь, за исключением если нарушение системы защиты персональных данных не привело к:

незаконному распространению, предоставлению персональных данных;

изменению, блокированию либо удалению персональных данных без возможности восстановления доступа к ним.

Приложение 3

к Положению об
обработке персональных
данных

АКТ ОБ УНИЧТОЖЕНИИ (УДАЛЕНИИ) ПЕРСОНАЛЬНЫХ ДАННЫХ

____. _____. 20__ г. г. _____

Наименование субъекта персональных данных

_____.

Виды персональных данных:

общедоступные, специальные, биометрические, генетические, иные.
(нужное подчеркнуть)

Категории персональных данных

_____.

Вид носителя персональных данных (название документа, раздела
информационного ресурса (системы))

_____.

Способ уничтожения (удаления) персональных данных

_____.

Состав комиссии:

_____ (подпись) _____ (ФИО)

_____ (подпись) _____ (ФИО)