Утверждёно
приказом заместителя начальника
управления по делам архивов
Белгородской области
от 12 июля 2012 года № 40-ГС

ПОЛОЖЕНИЕ
о порядке организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных управления по делам архивов Белгородской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение определяет порядок получения, обработки, хранения, передачи, цели обработки и любого другого использования персональных данных работников управления по делам архивов Белгородской области (далее - Управление).

1.2. Цель разработки настоящего Положения – определение порядка обработки персональных данных, защита персональных данных от несанкционированного доступа и разглашения.

1.3. Настоящее Положение разработано на основе и во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, Федеральных законов от 27.06.2006 года № 152-ФЗ «О персональных данных» и от 27.12.2009 года № 363 - ФЗ «О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных», Федерального закона от 27.07.04 № 79-ФЗ «О государственной гражданской службе Российской Федерации», положений главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работников», Указа Президента РФ «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997 г., Постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и других нормативных правовых актов.

1.4. Положение определяет права и обязанности руководителей и работников Управления, порядок использования указанных данных в служебных целях, а также порядок взаимодействия по поводу сбора, документирования, хранения и уничтожения персональных данных работников.

1.5. Порядок ввода в действие и изменения Положения:

1.5.1. Настоящее Положение вступает в силу с момента его утверждения начальником Управления и действует бессрочно, до замены его новым Положением.

1.5.2. Все изменения в Положение вносятся приказом начальника Управления.

1.5.3. Все сотрудники, осуществляющие обработку персональных данных, а также лицо, ответственное за обеспечение безопасности персональных данных Управления, должны быть ознакомлены с настоящим Положением под роспись по установленной форме **(Приложение № 1).**

1.6. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения.

1.7. В настоящем Положении используются следующие понятия:

- работник – физическое лицо, вступившее в трудовые отношения с работодателем;

- работодатель – Управление;

- персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;

- обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

- распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- использование персональных данных – действия (операции) с персональными данными, совершаемые работодателем в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

- информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

- конфиденциальность персональных данных – обязательное для соблюдения работодателем или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

- служебные сведения (служебная тайна) – информация (сведения), доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.

2. ЦЕЛИ И СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. В Управлении для каждой информационной системы персональных данных определены цели и сроки обработки персональных данных.

2.2. Информационная система персональных данных «1С-Предприятие: Бухгалтерия», обрабатывает персональные данные в целях учёта подотчётных и материально-ответственных лиц Управления, в срок **постоянно.**

2.3. Информационная система персональных данных «Камин - зарплата», обрабатывает персональные данные в целях учёта и расчёта заработной платы сотрудников Управления и налоговых отчислений с неё, в срок **постоянно.**

2.4. Информационная система персональных данных «TOPAZ: кадры», обрабатывает персональные данные в целях ведения кадрового учёта в Управлении, в срок **постоянно.**

3. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

3.1. Понятие персональных данных работника.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями.

Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

3.2. К персональным данным работника относятся:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения, а также иные данные, содержащиеся в удостоверении личности работника;
- данные о семейном, социальном и имущественном положении;
- данные об образовании работника, наличии специальных знаний или подготовки;
- данные о профессии, специальности работника;
- сведения о доходах работника
- данные медицинского характера, в случаях, предусмотренных законодательством;
- данные о членах семьи работника;

- данные о месте жительства, почтовый адрес, телефон работника, а также членов его семьи;

- данные, содержащиеся в трудовой книжке работника и его личном деле, страховом свидетельстве государственного пенсионного страхования, свидетельстве о постановке на налоговый учет;

- данные, содержащиеся в документах воинского учета (при их наличии);

- иные персональные данные, при определении объема и содержания которых работодатель руководствуется настоящим Положением и законодательством РФ.

3.3. Документами, содержащими персональные данные, являются:

а) паспорт или иной документ, удостоверяющий личность;

б) трудовая книжка;

в) страховое свидетельство государственного пенсионного страхования;

г) свидетельство о постановке на учёт в налоговый орган и присвоения ИНН;

д) документы воинского учёта;

е) документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;

ж) карточка Т-2;

з) автобиография;

и) личный листок по учёту кадров;

к) медицинское заключение о состоянии здоровья;

л) документы, содержащие сведения о заработной плате, доплатах и надбавках;

м) приказы о приеме лица на работу, об увольнении, а также о переводе лица на другую должность;

н) другие документы, содержащие сведения, предназначенные для использования в служебных целях.

3.4. Перечень персональных данных, обрабатываемых в Управлении и подлежащих защите от несанкционированного доступа, пересматривается по мере необходимости, не реже раза в 5 лет и утверждается начальников Управления.

4. ОСНОВНЫЕ УСЛОВИЯ ПРОВЕДЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, составленного по форме согласно **приложению № 2** к настоящему Положению, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона от 27.06.2006 года № 152-ФЗ «О персональных данных»;

- после направления уведомления об обработке персональных данных, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.06.2006 года № 152-ФЗ «О персональных данных»;

- после принятия необходимых мер по защите персональных данных.

4.2. В Управлении приказом начальника назначается сотрудник, ответственный за обеспечение защиты персональных данных, и определяется перечень лиц, допущенных к обработке персональных данных.

4.3. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей персональные данные, по форме согласно **приложению № 4** к настоящему Положению.

4.4. Запрещается:

- обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;

- осуществлять ввод персональных данных под диктовку.

5. СБОР, ОБРАБОТКА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Сбор персональных данных работника.

Документы, содержащие персональные данные работника, создаются путем:

а) копирования оригиналов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и другие документы);

б) внесения сведений в учетные формы (на бумажных и электронных носителях);

в) получения оригиналов необходимых документов (трудовая книжка, личный листок по учету кадров, автобиография, медицинское заключение).

5.2. Обработка персональных данных работника осуществляется исключительно в целях:

а) обеспечения соблюдения законов и иных нормативных правовых актов;

б) содействия работникам в трудоустройстве;

в) обеспечения личной безопасности работников;

г) контроля количества и качества выполняемой работы;

д) обеспечения сохранности имущества работника и работодателя.

5.3. Персональные данные следует получать лично у работника, за исключением случаев, если их получение возможно только у третьей стороны. Получение персональных данных работника у третьих лиц, возможно только при уведомлении работника об этом заранее и с его письменного согласия. В уведомлении работника о получении его персональных данных у третьих лиц должна содержаться следующая информация:

а) цели получения персональных данных;

б) предполагаемые источники и способы получения персональных данных;

в) характер подлежащих получению персональных данных;

г) последствия отказа работника дать письменное согласие на их получение.

5.4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, а равно как персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

5.5. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5.6. Сведения, содержащие персональные данные работника, включаются в его личное дело, а также содержатся на электронных носителях информации, доступ к которым разрешен лицам, непосредственно использующих персональные данные работника в служебных целях. Перечень должностных лиц определен в пункте 6.1 настоящего положения.

5.7. Хранение персональных данных в Управлении:

а) персональные данные, содержащиеся на бумажных носителях, хранятся в запираемых шкафах, установленных на рабочем месте консультанта Управления, ответственного за финансовое обеспечение;

б) персональные данные, содержащиеся на электронных носителях, хранятся на персональном компьютере консультанта Управления, ответственного за финансовое обеспечение.

в) персональные данные, включенные в состав личных дел, трудовая книжка хранятся в запертом металлическом сейфе, установленном на рабочем месте консультанта Управления, ответственного за кадровое делопроизводство;

г) персональные данные, содержащиеся на электронных носителях, хранятся на жестком диске персонального компьютера консультанта Управления, ответственного за кадровое делопроизводство.

5.8. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения.

6. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКА

6.1. Доступ к персональным данным работника имеют следующие сотрудники Управления, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей:

- начальник Управления;

- заместитель начальника Управле- ния;
- консультант Управления, ответственный за финансовое обеспечение;
- консультант Управления, ответственный за кадровое делопроизводство.

6.2. В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией начальника Управления, доступ к персональным данным работника может быть предоставлен иному работнику, должность которого не включена в Список должностей работников Управления, уполномоченных на обработку персональных данных работников и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

6.3. Уполномоченные лица имеют право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций в соответствии с должностным регламентом указанных лиц.

6.4. Работник имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев предусмотренных федеральным законом), содержащей его персональные данные. Работник имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

6.5. Сотрудники, имеющие доступ к персональным данным работников в связи с исполнением трудовых обязанностей, обеспечивают хранение информации, содержащей персональные данные работника, исключающее доступ к ним третьих лиц.

6.6. В период отпуска, служебной командировки и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные работников лицу, на которое приказом начальника Управления будет возложено исполнение его трудовых обязанностей.

В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные работников, передаются другому сотруднику, имеющему доступ к персональным данным работников по указанию начальника Управления.

При увольнении сотрудника, имеющего доступ к персональным данным работников, документы и иные носители, содержащие персональные данные работников, передаются другому сотруднику, имеющему доступ к персональным данным работников по указанию начальника Управления.

6.7. В случае если работодателю оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным работников Управления, то соответствующие данные предоставляются работодателем только после подписания с ними соглашения о неразглашении конфиденциальной информации.

В исключительных случаях, исходя из договорных отношений с контрагентом, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных работника.

6.8. Процедура оформления доступа к персональным данным уполномоченного сотрудника включает в себя:

- ознакомление сотрудника под роспись с настоящим Положением, иными нормативными актами (приказами, распоряжениями, инструкциями и т.п.), регулирующими обработку и защиту персональных данных работника;
- истребование с сотрудника (за исключением начальника Управления) письменного обязательства о соблюдении конфиденциальности персональных данных работника и соблюдении правил их обработки, подготовленного по установленной форме**.**

6.9. Консультант Управления, ответственный за финансовое обеспечение, и консультант Управления, ответственный за кадровое делопроизводство, вправе передавать персональные данные работника другим сотрудникам Управления, в случае если эти данные необходимы для исполнения уполномоченными сотрудниками Управления своих трудовых обязанностей.

При передаче персональных данных работника, консультант Управления, ответственный за финансовое обеспечение, и консультант Управления (ответственный за кадровое делопроизводство) предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и истребуют от этих лиц письменное обязательство в соответствии с п. 6.8. настоящего Положения.

6.10. Передача персональных данных работника третьим лицам осуществляется только с письменного согласия работника, которое оформляется по установленной форме и должно включать в себя:

- фамилию, имя, отчество, должность;
- наименование и юридический адрес работодателя, получающего согласие работника;
- цель передачи персональных данных;
- перечень персональных данных, на передачу которых дает согласие работник;
- срок, в течение которого действует согласие;
- порядок его отзыва **(приложение № 3).**

Согласия работника на передачу его персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника; когда третьи лица оказывают услуги Управления на основании заключенных договоров, а также в случаях, установленных федеральным законом и настоящим Положением.

6.11. Не допускается передача пер- сональных данных работника в коммерческих целях без его письменного согласия.

6.12. Сотрудники работодателя, передающие персональные данные работников третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные работников **(приложение № 5).**

Акт должен содержать следующие условия:

- уведомление лица, получающего данные документы об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена;

- предупреждение об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами.

Передача документов (иных материальных носителей), содержащих персональные данные работников, осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг Управлению;

- соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных работника;

- письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные работника, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных работника Управления несет сотрудник, осуществляющий передачу персональных данных работника третьим лицам, а также заместитель начальника Управления.

6.13. Представителю работника (в том числе адвокату) персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя работника;

- письменного заявления работника, написанного в присутствии сотрудника Управления (если заявление написано работником не в присутствии сотрудника Управления, то оно должно быть нотариально заверено).

Доверенности и заявления хранятся в личном деле работника.

6.14. Предоставление персональных данных работника государственным органам производится в соответствии с требованиями действующего законодательства и настоящим Положением.

6.15. Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника,

за исключением случаев, когда передача персональных данных работника без его согласия допускается действующим законодательством Российской Федерации.

6.16. Доступ к электронным базам данных, содержащим персональные данные работников, обеспечиваются системой паролей. Пароли устанавливаются сотрудником Управления, ответственным за обеспечение безопасности персональных данных и сообщаются индивидуально сотрудникам Управления, имеющим доступ к персональным данным работников.

7. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

7.1. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается работодателем за счёт средств работодателя в порядке, установленном федеральным законом.

7.2. Организацию защиты персональных данных работников осуществляет главный специалист Управления.

7.3. Главный специалист Управления обеспечивает:

- ознакомление сотрудника под роспись с настоящим Положением;
- при наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных работника, с данными актами также производится ознакомление сотрудника под роспись;
- истребование с сотрудников письменного обязательства о соблюдении конфиденциальности персональных данных работника и соблюдении правил их обработки;
- общий контроль за соблюдением сотрудниками работодателя мер по защите персональных данных работника.

7.4. При передаче персональных данных работников с соблюдением условий, предусмотренных разделом 4 настоящего Положения, должностные лица работодателя, обязаны предупредить лиц об ответственности в соответствии с законодательством Российской Федерации.

7.5. В целях обеспечения защиты персональных данных, хранящихся в личных делах, работники имеют право:

а) получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

б) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

в) требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением федерального закона. Работник при отказе работодателя исключить или исправить персональные данные работника имеет право заявлять в письменной форме работодателю о своем несогласии, обосновав соответствующим образом такое несогласие. Персо-

нальные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

г) требовать от работодателя уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведённых в них изменениях или исключениях из них;

д) обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите персональных данных работника.

7.6. Запрещается передавать информацию о состоянии здоровья работника, за исключением сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

7.7. В целях обеспечения защиты сведений, хранящихся в электронных базах данных Управления, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, применяются следующие основные методы и способы защиты информации:

а) контроль доступа в помещение, в котором расположена ИСПДн, постоянная проверка элементов системы на наличие следов взлома;

б) идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

в) регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;

г) учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета съемных носителей информации **(приложение № 6);**

д) обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;

е) физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

ж) периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной си-

стемы с помощью тест-программ, ими- тирующих попытки несанкционированного доступа;

з) наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

7.8. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов), носителей информации, встроенных в технические средства, или съемных маркированных носителей;

б) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

7.9. При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

а) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

б) учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

д) описание системы защиты персональных данных.

7.10. Каждый съемный носитель с записанными на нем персональными данными должен иметь маркировку, на которой указывается его уникальный учетный номер. Учет и выдачу съемных носителей персональных данных осуществляют сотрудники, ответственные за обеспечение безопасности персональных данных, в журнале учета.

7.12. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией, утвержденной приказом по Учреждению. По результатам уничтожения носителей составляется акт **(Приложение № 7)**, при необходимости

уничтожения информации с носителей персональных данных также составляется акт **(Приложение № 8).**

8. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ РАБОТНИКА

8.1. Иные права, обязанности, действия сотрудников, в должностные обязанности которых входит обработка персональных данных работника, определяются также должностными регламентами.

8.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

8.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной ответственности. К данным лицам могут быть применены следующие дисциплинарные взыскания:

а) замечание;

б) выговор;

в) предупреждение о неполном должностном соответствии;

г) освобождение от занимаемой должности;

д) увольнение.

8.4. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

8.5. Копия приказа о применении к работнику дисциплинарного взыскания с указанием оснований его применения вручается работнику под расписку в течение пяти дней со дня издания приказа.

8.6. Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Работодатель до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с работника по собственной инициативе, по письменному заявлению работника или по ходатайству его непосредственного руководителя.

8.7. Сотрудники, имеющие доступ к персональным данным работника и совершившие указанный дисциплинарный проступок, несут полную материальную

ответственность в случае причинения его действиями ущерба работодателю (п.7 ст. 243 Трудового кодекса РФ).

8.8. Сотрудники, имеющие доступ к персональным данным работника, виновные в незаконном разглашении или использовании персональных данных работников работодателя без согласия работников из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со ст. 183 Уголовного кодекса РФ.

Приложение № 1
к Положению о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных управления по делам архивов Белгородской области

ЛИСТ ОЗНАКОМЛЕНИЯ

с Положением о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных управления по делам архивов Белгородской области

№ п/п	Ф.И.О.	Должность	Дата	Подпись

Приложение № 2
к Положению о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных управления по делам архивов Белгородской области

Согласие
на обработку персональных данных

Я,_____
(фамилия, имя отчество)

даю согласие_____
(наименование и адрес места нахождения органа государственной власти области)

_____

на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, включающих: фамилию, имя, отчество, дату и место рождения, номер основного документа, удостоверяющего личность и заграничного паспорта, сведения о дате выдачи указанных документов и выдавшем их органе, адрес регистрации, адрес проживания, семейное положение, сведения о профессиональном образовании, в том числе о документах подтверждающих его, сведения о выполняемой работе с начала трудовой деятельности, близких родственниках, номере страхового свидетельства обязательного пенсионного страхования, идентификационном номере налогоплательщика, и совершение действий, предусмотренных п. 3 ч. 1 ст. 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», в целях обеспечения соблюдения законодательства о государственной гражданской службе, трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, обеспечения личной безопасности, формирования кадровых документов.

Я согласен на передачу своих персональных данных в правоохранительные органы, территориальные федеральные органы исполнительной власти, органы государственной власти области.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

Дата____**_____** **Подпись** / _____ / _____
(расшифровка подписи)

Приложение № 3
к Положению о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных управления по делам архивов Белгородской области

Отзыв согласия на обработку персональных данных

Наименование (Ф.И.О.) оператора

_____
Адрес оператора

_____
Ф.И.О. субъекта персональных данных

_____
Адрес, где зарегистрирован субъект персональных данных

_____
Номер основного документа, удостоверяющего его личность

_____
Дата выдачи указанного документа

_____
Наименование органа, выдавшего документ

Заявление

Прошу Вас прекратить обработку моих персональных данных в связи с _____
(указать причину)

«__» _____ 20__ г. _____ _____
(подпись) (расшифровка подписи)

Приложение № 4
к Положению о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных управления по делам архивов Белгородской области

ОБЯЗАТЕЛЬСТВО
о неразглашении информации, содержащей персональные данные

Я, _____,
(Ф.И.О. государственного гражданского служащего органа власти области)

исполняющий (ая) должностные обязанности по замещаемой должности

_____
(должность, наименование структурного подразделения)

_____,

предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. В течение года, после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к ответственности в соответствии с законодательством Российской Федерации.

_____ _____
(фамилия, инициалы) (подпись)

«____» _____ 20__ г.

Приложение № 5
к Положению о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных управления по делам архивов Белгородской области

АКТ
приёма-передачи документов (иных материальных ценностей), содержащих персональные данные работника

_____лице _____,
(наименование учреждения)

_____
(ФИО, должность сотрудника, имеющего допуск к персональным данным)

передаёт, а _____
(наименование учреждения)

лице _____,
(ФИО, должность сотрудника, имеющего допуск к персональным данным)

получает документы, содержащие персональные данные работников _____
(наименование учреждения)

для включения в Информационную систему _____.
(название информационной системы)

Перечень документов, содержащих персональные данные работника:

№ п/п	Наименование документа	Количество листов документа

Полученные персональные данные работника могут быть использованы лишь в целях, для которых они сообщены. Незаконное использование предоставленных персональных данных путём их разглашения, уничтожения и другими способами, установленными федеральными законами, может повлечь соответствующую гражданско-правовую, материальную, дисциплинарную, административно-правовую и уголовную ответственность.

Передал _____
(ФИО, должность сотрудника, имеющего допуск к персональным данным, подпись)

Принял _____
(ФИО, должность сотрудника, имеющего допуск к персональным данным, подпись)

(дата)

Приложение № 6
к Положению о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных управления по делам архивов Белгородской области

_____
(наименование Учреждения)

ЖУРНАЛ
учета и хранения съёмных носителей персональных данных
Управления по делам архивов Белгородской области

Ответственный за ведение и хранение: _____

Начат «___» _____ г.

Окончен «__» _____ г.

На _____листах

№ п/п	Учет-ный номер	Дата регистра-ции	Вид носителя	Тип носителя	Наименова-ние наносимой информации	Местонахож-дение носителя	Дата записи информа-ции	Ф.И.О. (сотрудник , которому выдает-ся носитель) получил, вернул, передал, подпись	Ф.И.О. подпись исполнителя	Отметка о переносе информации на другой носитель	Отметка об уничтожении (стирании) информации	Отметка об уничто-жении носителя
1	2	3	4	5	6	7	8	9	10	11	12	13

Приложение № 7
к Положению о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных управления по делам архивов Белгородской области

_____
(по заполнению для служебного пользования)

АКТ
уничтожения носителей персональных данных

«___» _____ 20__ г. № _____

Комиссия в составе председателя комиссии _____
_____ членов комиссии _____
_____
действуя на основании приказа от _____
(приказ о создании комиссии)
произвела отбор следующих носителей информации для уничтожения:

№ п/п	Тип машинного носителя информации	Учетный номер	Количество экземпляров	Номера экземпляров	Всего уничтожается	Примечание
1	2	3	4	5	6	7

Всего подлежит уничтожению _____
(прописью)
наименований. Записи акта с учетными данными сверены.

Перечисленные носители информации сверены с записями в акте и полностью уничтожены путем _____.

(указывается способ уничтожения носителей)

«___»_____ 20__г.

Председатель комиссии: _____
(должность, фамилия, подпись)
Члены комиссии: _____
(должность, фамилия, подпись)
Уничтоженные машинные носители информации в журнале учета и хранения съёмных носителей персональных данных списаны.
Ответственный за учет _____
(должность, подпись, фамилия, дата)

Приложение № 8
к Положению о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных управления по делам архивов Белгородской области

_____
(по заполнению для служебного пользования)

АКТ
уничтожения информации находящейся на электронных носителей

«___» _____ 20__ г. № _____

Комиссия в составе председателя комиссии _____
_____ членов комиссии _____
_____
действуя на основании приказа от _____
(приказ о создании комиссии)
произвели отбор следующей информации находящейся на электронных носителей для уничтожения:

№ п/п	Вид информации	Тип носителя	Учетный номер носителя	Примечание
1	2	3	4	6

После получения разрешения на уничтожение перечисленная информация и документы перед уничтожением сверили с записями в акте и полностью уничтожили путем _____.
(указывается способ уничтожения информации с электронных носителей)

«___»_____ 20__г.

Председатель комиссии:_____
(должность, фамилия, подпись)
Члены комиссии:_____
(должность, фамилия, подпись)