Российская Федерация
БЕЛГОРОДСКАЯ ОБЛАСТЬ

УПРАВЛЕНИЕ АВТОМОБИЛЬНЫХ ДОРОГ ОБЩЕГО ПОЛЬЗОВАНИЯ И ТРАНСПОРТА БЕЛГОРОДСКОЙ ОБЛАСТИ
(УПРДОРиТ Белгородской области)

П Р И К А З

«25» июня 20 14 г. № 278

О политике в отношении обработки персональных данных

В соответствии с федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных», 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», распоряжением Губернатора Белгородской области от 7 июля 2011 года №459-р «Об утверждении Положения о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных органов исполнительной власти, государственных органов области» и в целях создания системы организационно-распорядительных документов в сфере безопасности персональных данных

ПРИКАЗЫВАЮ:

1. Утвердить Положение об обработке и защите персональных данных сотрудников Управления (далее – Положение, прилагается).

2. Работникам Управления, имеющим доступ к персональным данным руководствоваться утвержденным Положением.

3. Отделу кадровой работы и делопроизводства (Тютюнова О.А.), отделу информационного обеспечения (Головин К.В.) и консультанту по мобилизационной работе (Косищев С.Н.):

- обеспечить защиту персональных данных работников Управления от неправомерного использования или утраты в порядке, установленном федеральными законами;

- уточнить ответственных за обеспечение безопасности информации при использовании средств автоматизации, хранении и передаче персональных данных;

- уточнить соответствующие распорядительные документы в целях защиты персональных данных при их обработке в информационных системах.

4. Считать утратившим силу приказ начальника Управления от 6 апреля 2010 года №03-н/с «Об утверждении Положения об обработке и защите персональных данных сотрудников».

5. Контроль за исполнением данного приказа возложить на заместителя начальника управления – начальника отдела организации междугородних перевозок Куропова А.Ю.

Начальник
управления автодорог общего
пользования и транспорта
Белгородской области **С.Евтушенко**

Исп. Косищев С.Н.
(4722) 271512

УТВЕРЖДЕНО
приказом начальника управления автомобильных
дорог общего пользования и транспорта
Белгородской области
«25» 04 2014 г. № 278

ПОЛОЖЕНИЕ
об обработке и защите персональных данных сотрудников управления автомобильных дорог общего пользования и транспорта Белгородской области

I. Общие положения

1.1. Настоящее Положение разработано на основании ст. 24 Конституции Российской Федерации (далее – РФ), главы 14 Трудового кодекса РФ, федерального закона «Об информации, информатизации и защите информации» №149-ФЗ от 27.07.2006 года, федерального закона «О персональных данных» №152-ФЗ от 27.07.2006 года, постановления Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» №1119 от 01.11.2012 года, постановления Правительства РФ «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» №211 от 21.03.2012 года, методических рекомендаций по организации защиты персональных данных при их обработке в органах власти Белгородской области, принятых рабочей группой по информатизации, телекоммуникациям и защите информации в Белгородской области от 16.03.2011 года №27-08/29 ДСП.

1.2. Настоящее Положение утверждается приказом начальника управления автомобильных дорог общего пользования и транспорта Белгородской области (далее – Управление).

1.3. Настоящее Положение определяет:

- порядок обработки (приема, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения, учета персональных данных работников Управления;
- права и свободы работников Управления при обработке их персональных данных с использованием средств автоматизации или без использования таких средств;
- ответственность лиц, имеющих доступ к персональным данным, за невыполнение требований, регулирующих обработку и защиту персональных данных.

II. Основные понятия и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

1) **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), а также аналогичная информация об иных третьих лицах, полученная управлением на законных основаниях от его контрагентов и иных третьих лиц в результате реализации полномочий. Персональные данные являются конфиденциальной информацией.

К персональным данным относятся (в том числе, но не ограничиваясь этим) следующие сведения и документы:

- паспортные данные;
- биографические сведения;
- сведения об образовании;
- сведения о специальности (профессии);
- сведения о занимаемой или ранее занимаемых должностях;
- место регистрации (пребывания);
- домашний телефон;
- состав семьи;
- подлинники и копии приказов по личному составу;
- другая информация, необходимая Управлению в связи с реализацией полномочий, а также реализацией договорных отношений;

2) **обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

3) **конфиденциальность персональных данных** – обязательное для соблюдения назначенным лицом Управления ответственным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия работника (субъекта) или наличия иного законного основания;

4) **распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (предоставление персональных данных) или на ознакомление с персональными данными неопределенного 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;

5) **блокировка персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

6) **уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

7) **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

8) **информационная система персональных данных** – совокупность содержащихся в базе данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

9) **трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

10) **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

11) **информация** – сведения (сообщения, данные) независимо от формы их представления;

12) **документированная информация** – зафиксированная на материальном носителе путем документирования информации с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

2.2. Носителями персональных данных являются документы, содержащие сведения, перечисленные в п.1 часть 2.1 настоящего Положения.

III. Получение и обработка персональных данных работников

3.1. При заключении трудового договора лицо, поступающее на работу, предъявляет работодателю следующие документы:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случая, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета для военнообязанных и лиц, подлежащих воинскому учету;
- идентификационный номер налогоплательщика;
- документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки.

Приказ о приеме на работу, трудовой договор оформляет отдел кадровой работы и делопроизводства Управления. Копия приказа о приеме на работу передается в бухгалтерию Управления.

3.2. При заполнении личной карточки работника (унифицированная форма Т-2), работник дополнительно к представленным документам указывает следующие сведения о себе:

- знание иностранного языка;
- семейное положение и состав семьи;
- адрес места жительства (по паспорту и фактический) и домашний телефон;
- предыдущее (-ие) место (-а) работы;
- медицинское заключение о состоянии здоровья и возможности выполнения возлагаемой трудовой функции (по требованию);
- иные сведения, с которыми работник считает нужным ознакомить работодателя.

Ведение формы Т-2 как на бумажном носителе, так и в электронном виде, возложено на отдел кадровой работы и делопроизводства Управления.

3.3. При поступлении на работу инженерно-технический работник (руководитель, специалист, служащий) дополнительно к п.3.1 и 3.2 заполняет анкету, где указывает:

- фамилию, имя, отчество (при изменении ФИО, сведения об изменении);
- дату и место рождения;
- гражданство (при изменении, сведения об изменении);
- образование;
- знание иностранных языков;
- семейное положение и сведения о близких родственников;
- отношение к воинской обязанности;
- адрес места жительства (по паспорту и фактический), домашний телефон;
- предыдущее (-ие) место (-а) работы.

Анкета инженерно-технического работника хранится в личном деле работника. В личном деле также хранится вся информация, относящаяся к персональным данным работника в период его работы в Управлении. Первоначально, в личное дело группируются документы (копии документов), оформляющие процесс приема на работу, а в последствии – все основные документы (копии документов), характеризующие трудовую деятельность работника в Управлении. Все поступающие в личное дело документы группируются в папках и располагаются в хронологическом порядке с внутренней описью документов дела.

Личное дело работника состоит:

- опись документов дела;
- анкета;
- копии документов об образовании, квалификации;
- копия приказа о приеме на работу;
- копии приказов о назначении на должность;
- характеристики;
- протоколы аттестации, о присвоении категории, квалификации, аттестационные листы;
- копии приказов о поощрениях, взысканиях;
- заявление об увольнении, копия приказа об увольнении;
- другие документы.

Ведение личного дела возложено на отдел кадровой работы и делопроизводства Управления.

3.4. Работник представляет работодателю достоверные сведения о себе.

3.5. Работодатель не вправе требовать от работника предоставление информации о политических и религиозных убеждениях и о частной жизни работника.

3.6. При изменении персональных данных, работник письменно уведомляет работодателя о таких изменениях в срок, не превышающий 14 дней.

3.7. По мере необходимости работодатель требует у работника дополнительные сведения. Работник представляет необходимые сведения и в случае необходимости, предъявляет документы, подтверждающие достоверность этих сведений.

3.8. Персональные данные работника работодатель получает непосредственно от работника.

Работодатель вправе получать персональные данные работника от третьих лиц только при наличии письменного согласия работника.

IV. Хранение персональных данных работников

4.1. Книги приказов по личному составу, приказы по личному составу и основания к приказам, трудовые договоры хранятся в отделе кадровой работы и делопроизводства Управления и защищены от несанкционированного доступа.

4.2. Трудовые книжки работников хранятся в сейфе и защищены от несанкционированного доступа.

4.3. Личные карточки работников (форма Т-2) и личные дела хранятся в отделе кадровой работы и делопроизводства Управления, в отведенном месте, обеспечивающем защиту от несанкционированного доступа.

В конце рабочего дня все личные дела, карточки Т-2, трудовые книжки, затребованные для работы в течение рабочего дня, сдаются в отдел кадровой работы и делопроизводства Управления.

4.4. Информация о начислении и выплате заработной платы и других материальных и денежных выплатах хранится в отделе бухгалтерского учета и отчетности Управления и защищена от несанкционированного доступа.

4.5. Персональные данные работников Управления хранятся в электронном виде в локальной компьютерной сети и защищены от несанкционированного доступа паролем. Доступ к данным электронной базы, содержащей, персональные данные работников Управления обеспечивается трехступенчатой системой паролей на уровне локальной сети и уровне баз данных.

Пароль устанавливает отдел информационного обеспечения и сообщает индивидуально сотруднику Управления.

4.6. Доступ к персональным данным работников Управления (к тем данным, которые необходимы для выполнения конкретных трудовых функций) имеют:

- начальник управления;
- заместитель начальника управления – начальник отдела организации междугородних перевозок;
- заместитель начальника управления – начальник отдела бухгалтерского учета и отчетности;
- заместитель начальника отдела бухгалтерского учета и отчетности;
- консультант отдела бухгалтерского учета и отчетности;
- начальник отдела кадровой работы и делопроизводства;
- консультант отдела кадровой работы и делопроизводства;
- начальник отдела правового обеспечения;
- начальник отдела информационного обеспечения;
- консультант по мобилизационной работе.

Доступ других работников Управления к персональным данным осуществляется на основании письменного разрешения начальника управления.

V. Использование персональных данных работников

5.1. Персональные данные работника используются для целей, связанных с выполнением работником трудовых функций.

5.2. Работодатель использует персональные данные, в частности, для решения вопросов продвижения работника по службе, очередности предоставления ежегодного отпуска, установления размера заработной платы, для обеспечения личной безопасности работника, а также для обеспечения сохранности имущества работодателя. Для предоставления дополнительных гарантий и компенсаций, условий труда по определенным основаниям, предусмотренным законодательством. На основании персональных данных работника решается вопрос о допуске работника к информации, составляющей государственную, служебную и коммерческую тайны.

5.3. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на фактах, событиях, обстоятельствах частной жизни работника.

VI. Передача персональных данных работников

6.1. Информация, относящаяся к персональным данным работника, может быть представлена государственным органам в порядке, установленным федеральными законами.

6.2. Работодатель не вправе представлять персональные данные работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также случаях, установленным федеральным законом.

В случае если, лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных работника, либо отсутствует письменное согласие работника на предоставление его персональных сведений, работодатель обязан отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении данных.

6.3. Персональные данные работника могут быть переданы представителям работников в порядке, установленном Трудовым кодексом, в том объеме, в каком это необходимо для выполнения указанными представителями их функций.

Работодатель обеспечивает учет выдачи персональных данных работников, а именно: регистрацию запросов, фиксирование сведений о лице, направившем запрос, регистрацию даты передачи персональных данных или даты уведомления об отказе в предоставлении персональных данных.

VII. Защита персональных данных работников

7.1. Общую организацию защиты персональных данных работников осуществляет начальник Управления.

7.2. Начальник отдела кадровой работы и делопроизводства организует:

- ознакомление с настоящим Положением под роспись работников Управления, имеющих доступ к персональным данным;

- в случае вступления иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных работников, также производится ознакомление под роспись;

- истребование с работников Управления письменного обязательства о соблюдении конфиденциальности персональных данных и соблюдения правил их обработки;

- общий контроль за соблюдением работниками Управления мер по защите персональных данных.

7.3. Организацию и контроль за защитой персональных данных осуществляют непосредственно работники Управления, которые имеют доступ к персональным данным.

Методическое руководство по защите персональных данных осуществляет начальник отдела информационного обеспечения.

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

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (матрица доступа), информационной системе и связанным с ее использованием работам, документам;

- ограничение доступа пользователей в помещение, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, постоянная проверка элементов системы на наличие следов взлома;

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

- учет и хранение съемных носителей информации, их обращение, исключающее хищение, подмену и уничтожение;

- использование средств защиты информации, прошедших процедуру оценки соответствия;

- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

- организация физической защиты помещения и собственно технических средств, позволяющих осуществлять обработку персональных данных;

- контроль доступа в помещение информационной системы посторонних лиц;

- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

7.5. Для защиты персональных данных в информационной системе персональных данных сотрудников Управления и выполнения пунктов раздела 7.4. настоящего Положения привлекаются для выполнения специальных, аналитических и экспертных работ по защите информации организация-лицензиат ФСТЭК и ФСБ России (ООО «Матрица»).

7.6. 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 помещения, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

7.7. При обработке персональных данных в информационной системе начальником Управления и лицом, ответственным за обеспечение безопасности, 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.

7.8. Каждый съемный носитель, с записанным на нем персональными данными, должен иметь маркировку, на которой указывается его универсальный номер. Учет и выдачу съемных носителей персональных данных осуществляет ответственный за обеспечение безопасности персональных данных.

7.9. В случае выхода из строя техники, на которой проводилась обработка персональных данных, вынос за пределы территории Управления с целью ремонта, замены и т.п. без согласования с начальником или ответственным за обеспечение безопасности персональных данных запрещается.

VIII. Гарантии конфиденциальности персональных данных и ответственность за разглашение

8.1. Информация, относящаяся к персональным данным работника, является служебной тайной и охраняется законом.

8.2. Работник имеет право на:

- полную информацию о своих персональных данных, их обработке, использования и хранения;

- свободный бесплатный доступ к своим персональным данным включая право на получение копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований трудового законодательства;

- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке или защите его персональных данных.

8.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника привлекаются к дисциплинарной и материальной ответственности, а также привлекаются к административной, гражданско-правовой и уголовной ответственности в соответствии с федеральными законами.

Начальник отдела кадровой работы и делопроизводства Управления О.Тютюнова

Консультант по мобработе Управления С.Косищев