



БЕЛГОРОДСКАЯ ОБЛАСТЬ
УПРАВЛЕНИЕ ВЕТЕРИНАРИИ
БЕЛГОРОДСКОЙ ОБЛАСТИ

ПРИКАЗ

Белгород

«30» сентября 2010 г.

№ 369

**Об утверждении Политики
управления ветеринарии Белгородской
области в отношении обработки
персональных данных**

В соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона 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, осуществляемой без использования средств автоматизации», в целях соблюдения принципов законности, справедливости и конфиденциальности при работе с персональными данными, а также обеспечения безопасности процессов их обработки, **п р и к а з ы в а ю:**

1. Утвердить Политику управления ветеринарии Белгородской области в отношении обработки персональных данных (прилагается).

2. Отделу организационно-контрольной работы и делопроизводства (Грязева Т.А.) организовать размещение настоящего приказа на официальном сайте управления ветеринарии области в сети Интернет.

3. Контроль за исполнением приказа оставляю за собой.

Начальник управления

Д.В. Карайченцев

Утверждена
Приказом начальника
управления ветеринарии
Белгородской области
от «___» _____ года № ____

ПОЛИТИКА
управления ветеринарии Белгородской области в отношении обработки
персональных данных

1. Общие положения

1.1 Настоящая «Политика управления ветеринарии Белгородской области в отношении обработки персональных данных» (далее – Политика) разработана на основании статьи 24 Конституции Российской Федерации, главы 14 Трудового кодекса Российской Федерации, Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информатизации и защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Гражданского кодекса Российской Федерации в целях соблюдения принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечения безопасности процессов их обработки.

1.2. Настоящая Политика утверждается приказом начальника управления ветеринарии Белгородской области либо лица, его замещающего.

1.3. Управление ветеринарии Белгородской области (далее – Управление) является юридическим лицом, организующим и (или) осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных (оператором).

Полное наименование: управление ветеринарии Белгородской области.

Почтовый адрес Управления: 308014, г. Белгород, 1-й Мичуринский пер., 22а.

Местонахождение Управления: г. Белгород, 1-й Мичуринский пер., 22а.

Телефон/факс приемной начальника Управления: (4722) 31-27-60, факс (4722) 31-27-59.

Адрес официального сайта Управления в сети Интернет: <http://www.belvet.ru/>

Электронный адрес: belvetupr@yandex.ru.

1.4. Настоящая Политика:

1.4.1. определяет порядок обработки (приема, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения, учета) персональных

1.4.2. обеспечивает защиту прав и свобод субъектов при обработке их персональных данных с использованием средств автоматизации или без использования таких средств, а также устанавливает ответственность лиц, имеющих доступ к персональным данным, за невыполнение требований, регулирующих обработку и защиту персональных данных.

1.4.3. разработана в целях обеспечения реализации требований законодательства Российской Федерации в области обработки персональных данных субъектов персональных данных.

1.4.4. раскрывает основные категории персональных данных, обрабатываемых оператором, цели, способы и принципы обработки оператором персональных данных, права и обязанности оператора при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых оператором в целях обеспечения безопасности персональных данных при их обработке.

1.4.5. является общедоступным документом, декларирующим концептуальные основы деятельности оператора при обработке персональных данных.

2. Основные понятия и состав персональных данных субъектов

2.1. Для целей настоящей Политики 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:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о стаже работы;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате;
- сведения о социальных льготах;
- сведения о полученной специальности;
- сведения о занимаемой должности;
- сведения о наличии судимости;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание служебного контракта (трудового договора);
- содержание сведений о доходах, расходах, об имуществе и обязательствах имущественного характера;
- материалы служебных проверок;
- любая иная информация, относящаяся к прямо или косвенно определенному

или определяемому физическому лицу (субъекту персональных данных) и 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, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

3) конфиденциальность персональных данных - обязательное для соблюдения назначенным должностным лицом Управления и (или) ответственным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия 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) блокирование 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 базах 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 информация 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 ч. 1 п. 2.1. настоящей Политики.

3. Цели обработки персональных данных

3.1. Управление обрабатывает персональные данные исключительно в следующих целях:

3.1.1. Исполнения положений нормативных актов, указанных в п. 1.1 Политики.

3.1.2. Выполнение обязательств по заключенным служебным контрактам, трудовым договорам, договорам гражданско-правового характера и договорам со сторонними организациями.

3.1.3. Исполнение законов и других нормативно-правовых актов Российской Федерации в сфере защиты и обработки персональных данных.

4. Категории обрабатываемых персональных данных

4.1. В информационных системах персональных данных Управления обрабатываются следующие категории персональных данных:

4.1.1. Персональные данные государственных гражданских служащих (сотрудников) Управления.

4.1.2. Персональные данные иных физических лиц.

4.1.3. Персональные данные кандидатов на замещение должностей государственной гражданской службы в Управлении, а также должностей обслуживающего и вспомогательного персонала, не относящихся к должностям государственной гражданской службы области.

5. Основные принципы обработки, передачи и хранения персональных данных

5.1. Управление в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в статье 5 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

5.2. Управление не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

5.3. Управление не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

Персональные данные, сообщаемые субъектом (фамилия, имя, отчество, дату рождения, адрес, абонентский номер и др.), обрабатываются только с письменного согласия субъекта персональных данных.

6. Меры по обеспечению безопасности персональных данных при их обработке

6.1. Управление при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

6.1.1. назначением ответственных за организацию обработки персональных данных.

6.1.2. осуществлением внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам.

6.1.3. ознакомлением работников Управления, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и (или) обучением указанных сотрудников.

6.1.4. определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

6.1.5. применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных.

6.1.6. оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

6.1.7. выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.

6.1.8. установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

6.1.9. контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

6.2. Обязанности должностных лиц, осуществляющих обработку и защиту персональных данных, а также их ответственность, определяются в приказе Управления об организации работы по защите конфиденциальной информации.

7. Права субъектов персональных данных

7.1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных Управлением.

7.2. Субъект персональных данных вправе требовать от Управления, которое их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с законодательством Российской Федерации.

8. Контактная информация

8.1. Ответственным за организацию обработки и обеспечения безопасности

персональных данных в Управлении является начальник отдела кадровой и организационной работы.

8.2. Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

9. Доступ к персональным данным субъекта

9.1. Персональные данные могут быть предоставлены органам государственной власти и (или) специально уполномоченным лицам в целях предупреждения угрозы жизни и здоровью работника, а также в иные случаях, предусмотренных Трудовым Кодексом Российской Федерации и федеральными законами в порядке, установленном законодательством Российской Федерации. При этом указанные органы и (или) лица вправе получать только те персональные данные, которые необходимы им для выполнения конкретных функций.

9.2. Перечень должностных лиц Управления, имеющих доступ к персональным данным, определяется приказом начальника Управления.

9.3. Передача персональных данных третьим лицам возможна только с согласия субъекта в письменной форме или без его согласия в случаях, предусмотренных законодательством Российской Федерации.

10. Сбор, обработка и хранение Персональных данных

10.1. Обработка персональных данных может осуществляться исключительно в целях соблюдения иных нормативных правовых актов Российской Федерации, содействия субъектам в трудоустройстве, обучении, продвижении по службе (работе), обеспечения личной безопасности субъектов, контроля качества выполняемой работы, очередности предоставления ежегодного отпуска, установления размера, расчета и выплаты заработной платы, а также в иных целях при получении письменного согласия субъекта.

Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции почтовой связью, оформление разовых пропусков, обработка персональных данных для исполнения трудовых договоров или без использования средств автоматизации и в иных случаях, предусмотренных законодательством Российской Федерации.

10.2. Персональные данные следует получать непосредственно у субъекта.

Если персональные данные возможно получить только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Управление должно сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

10.3. При изменении персональных данных субъект уведомляет Управление о таких изменениях в 10-дневный срок.

10.4. Персональные данные на бумажных носителях, обрабатываемые без использования средств автоматизации, хранятся в Управлении в запираемых

помещениях, оборудованных охранно-пожарной сигнализацией под круглосуточной охраной.

10.5. Персональные данные могут также храниться в электронном виде в информационных системах Управления. В таком случае доступ к персональным данным должен быть технически возможен только специально уполномоченным лицам, упомянутым в пункте 9.2. При этом указанные лица должны иметь право получать только те персональные данные, которые необходимы им для выполнения конкретных функций.

Доступ к информационным системам, содержащим персональные данные, должен быть защищен паролями, а также разграничением доступа к различным подсистемам в зависимости от выполняемых должностных обязанностей.

11. Передача персональных данных субъекта

11.1. При передаче персональных данных Управление должно соблюдать следующие требования:

11.1.1. не передавать персональные данные третьей стороне без письменного согласия субъекта, либо, также, иных оснований, предусмотренных действующим законодательством;

11.1.2. предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц соблюдения правил обработки и хранения персональных данных. Лица, получающие персональные данные, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными в порядке, установленном законодательством Российской Федерации;

11.1.3. разрешать доступ к персональным данным только специально уполномоченным лицам Управления. Список должностей, имеющих доступ к персональным данным, определяется приказом начальника Управления.

12. Общедоступные источники персональных данных

12.1. В целях информационного обеспечения деятельности структурных подразделений Управления могут быть созданы общедоступные источники персональных данных (в том числе справочники, адресные книги и др.). В общедоступные источники персональных данных с письменного согласия субъекта могут включаться его фамилия, имя, отчество, сведения о занимаемой должности, контактный номер телефона, адрес места жительства и иные персональные данные, предоставленные субъектом.

12.2. Сведения о субъекте могут быть в любое время исключены из общедоступных источников персональных данных по его требованию либо по решению уполномоченных должностных лиц Управления, а также в случаях, предусмотренных законодательством Российской Федерации.

13. Безопасность персональных данных

13.1. При обработке персональных данных, ответственное лицо Управления обязано принимать необходимые организационные и технические меры, в том числе

использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

13.2. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии хранения, которая обеспечивает защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

13.3. В целях предупреждения нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечения безопасности информации в процессе управленческой и хозяйственной деятельности Управления устанавливается комплекс мер по защите персональных данных. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе деятельности Управления.

Комплекс мер включает в себя:

13.3.1. Внутреннюю защиту - регламентацию доступа к конфиденциальным сведениям Управления, документам и базам данных, входящую в число основных направлений организационной защиты информации и предназначенную для разграничения полномочий. Для защиты персональных данных субъекта должностные лица Управления обязаны соблюдать следующие меры безопасности:

- ограничивать и регламентировать состав государственных гражданских служащих и работников Управления, функциональные обязанности которых требуют доступа к персональным данным;

- избирательно и обоснованно распределять документы и информацию между государственными служащими и работниками;

- рационально размещать рабочие места, при котором исключается бесконтрольное использование конфиденциальной информации;

- организовать необходимые условия в помещении для работы с конфиденциальными документами и базами данных;

- регламентировать порядок уничтожения информации;

- выявлять нарушения доступа к персональным данным;

- проводить работы по предупреждению утраты сведений при работе с персональными данными;

- защищать персональные компьютеры паролями доступа.

13.3.2. Внешнюю защиту - созданные для защиты персональных данных целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др. Под посторонним лицом понимается любое лицо, не имеющее санкционированного доступа к персональным данным, в том числе непосредственного отношения к деятельности Управления, посетители, работники других организаций и иные лица.

Лица, не являющиеся работниками Управления, не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в Управлении. В отдельных случаях возможно предоставление доступа к данной информации для третьих лиц, осуществляющих внедрение, сопровождение и аудит процессов в Управлении, при условии, что от них получено обязательство о неразглашении в письменной форме. Доступ к вышеуказанной информации возможен только после согласования с председателем (первым заместителем, заместителем председателя) Управления.

Для защиты персональных данных субъектов необходимо соблюдать:

- порядок приема, учета и контроля деятельности посетителей;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и беседах.

14. Обязанности Управления

14.1. Обязанности Управления при сборе персональных данных.

14.1.1. При сборе персональных данных сотрудники Управления обязаны предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных, в том числе содержащую:

- подтверждение факта обработки персональных данных Управлением;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Управлением способы обработки персональных данных;
- наименование и место нахождения Управления, сведения об Управлении и должностных лицах Управления, которым могут быть раскрыты персональные данные на основании договора с Управлением;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных настоящей Политикой;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных;
- иные сведения, предусмотренные настоящей Политикой;

14.1.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, сотрудники Управления обязаны разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

14.1.3. Если персональные данные получены не от субъекта персональных данных, Управление, за исключением случаев, предусмотренных п. 14.1.4., до начала обработки таких персональных данных обязано предоставить субъекту персональных данных следующую информацию:

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные настоящей Политикой права субъекта персональных данных;
- источник получения персональных данных.

14.1.4. Управление освобождается от обязанности предоставить субъекту

персональных данных сведения, предусмотренные п. 14.1.3. в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных Управлением;

2) персональные данные получены Управлением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

4) Управление осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) предоставление субъекту персональных данных сведений, предусмотренных п. 14.1.3. настоящей главы, нарушает права и законные интересы третьих лиц.

14.2. Меры, направленные на обеспечение выполнения Управлением обязанностей

14.2.1. Управление обязано принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящей Политикой. Управление самостоятельно определяет состав, и перечень мер, необходимых и достаточных для обеспечения выполнения обязанности. К таким мерам могут, в частности, относиться:

1) издание Управлением, являющимся юридическим лицом, документов, определяющих Политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

2) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящей политике, требованиям к защите персональных данных, политике в отношении обработки персональных данных, локальным актам оператора;

3) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящей Политики, соотношение указанного вреда и принимаемых Управлением мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящей Политикой;

4) ознакомление государственных гражданских служащих (работников) Управления, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

14.2.2. Управление обязано опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

14.2.3. Управление обязано представить документы и локальные акты, и (или) иным образом подтвердить принятие мер, указанных в разделе 15 настоящей Политики, по запросу уполномоченного органа по защите прав субъектов персональных данных.

14.3. При обработке персональных данных Управление обязано соблюдать следующие требования:

14.3.1. при определении объема и содержания обрабатываемых персональных данных Управление должно действовать в соответствии с Конституцией Российской Федерации, действующим законодательством Российской Федерации и иными нормативными правовыми актами, закрепляющими полномочия Управления и порядок их реализации;

14.3.2. защита персональных данных от неправомерного их использования или утраты должна быть обеспечена Управлением за счет денежных средств в порядке, установленном действующим законодательством Российской Федерации;

Государственные служащие и работники Управления должны быть ознакомлены под роспись с документами Управления, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

15. Меры по обеспечению безопасности персональных данных при их обработке

15.1. Защита персональных данных субъектов от неправомерного их использования или утраты обеспечивается Управлением в порядке, установленном действующим законодательством и локальными актами Управления, а также выполнением комплекса организационно-технических мер, обеспечивающих их безопасность.

15.2. Документы, содержащие персональные данные, должны храниться в надежно запираемых помещениях (кабинетах), а также в не запираемых шкафах, при условии, что бесконтрольный доступ посторонних лиц в помещения (кабинеты) исключен.

15.3. Организация защиты персональных данных в информационных системах Управления осуществляется в рамках действующей в Управлении системы защиты информации. Доступ к информационным системам Управления, содержащим персональные данные, обеспечивается системой паролей, а также программно-техническими средствами защиты информации.

15.4. Помещения (кабинеты), в которых ведется обработка персональных данных, должны обеспечивать их сохранность, исключать возможность бесконтрольного проникновения в них посторонних лиц.

15.5. В течение рабочего дня ключи от шкафов (ящиков, хранилищ), в которых содержатся персональные данные, а также помещений (кабинетов), где находятся средства вычислительной техники, предназначенные для обработки персональных данных, находятся на хранении у ответственных работников.

15.6. По окончании рабочего времени помещения (кабинеты), предназначенные для обработки персональных данных, должны быть закрыты на ключ, бесконтрольный доступ в такие помещения (кабинеты) должен быть исключен (путем применения печатывания, видеонаблюдения и (или) систем контроля доступа).

15.7. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

15.8. При принятии решений, затрагивающих интересы субъекта, Управление не

имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.

15.9. Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

16. Права и обязанности субъекта в области защиты персональных данных

16.1 Субъект обязан:

- передавать Управлению достоверные, документированные персональные данные, состав которых установлен нормативно-правовыми актами Российской Федерации;

- своевременно сообщать Управлению об изменении своих персональных данных.

Обязанности субъекта фиксируются в письменном виде в тексте согласия на обработку персональных данных, которое он подписывает при приеме на государственную гражданскую службу (работу).

16.2. Субъект в целях обеспечения защиты персональных данных, хранящихся в Управлении, имеет право на:

- свободный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации;

- исключение или исправление неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства Российской Федерации.

- дополнение персональных данных оценочного характера заявлением, выражающим его собственную точку зрения;

- требование об извещении Управлением всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях и дополнениях;

- отзыв согласия на обработку персональных данных;

- обжалование в суде любых неправомерных действий или бездействия должностных лиц Управления при обработке и защите его персональных данных.

Получение от Управления:

- сведений о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

- перечня обрабатываемых персональных данных и информации об источнике их получения;

- информации о сроках обработки персональных данных, в том числе сроках их хранения;

- сведений о том, какие юридические последствия может повлечь за собой обработка его персональных данных.

17. Лицо, ответственное за организацию обработки и обеспечение безопасности персональных данных

17.1. Права, обязанности и юридическая ответственность лица, ответственного за организацию обработки и обеспечение безопасности персональных данных,

установлены Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и настоящей Политикой.

17.2. Назначение на должность лица, ответственного за организацию обработки и обеспечение безопасности персональных данных, и освобождение от нее осуществляется приказом начальника Управления. При назначении учитываются полномочия, компетенции и личностные качества должностного лица, призванные позволить ему надлежащим образом и в полном объеме реализовывать свои права и выполнять обязанности как лица, ответственного за организацию обработки и обеспечение безопасности персональных данных.

17.3. Лицо, ответственное за организацию обработки и обеспечение безопасности персональных данных:

17.3.1. организует осуществление внутреннего контроля над соблюдением Управлением и ее должностными лицами законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

17.3.2. организует доведение до сведения работников Управления положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

17.3.3. организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществляет контроль над приемом и обработкой таких обращений и запросов.

18. Ответственность за нарушение требований обработки и защиты персональных данных субъекта

18.1. Должностные лица Управления, имеющие доступ к персональным данным, несут личную ответственность за нарушение режима защиты персональных данных в соответствии с законодательством Российской Федерации.

18.2. Каждое должностное лицо Управления, получающее для работы конфиденциальный (содержащий персональные данные) документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

18.3. Должностные лица Управления, которым сведения о персональных данных стали известны в силу их служебного положения, несут ответственность за их разглашение.

18.4. Обязательства по соблюдению конфиденциальности персональных данных остаются в силе и после окончания работы с ними вышеуказанных лиц.

18.5. За неисполнение или ненадлежащее исполнение должностным лицом Управления по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера, работодатель вправе применять дисциплинарные взыскания, предусмотренные Федеральным законом от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации» или Трудовым кодексом Российской Федерации.

18.6. Должностные лица Управления, в обязанность которых входит обработка персональных данных, обязаны обеспечить каждому гражданскому служащему (работнику) Управления, при необходимости, возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы,

если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременно предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – может повлечь наложение на должностных лиц административного штрафа в размере, определяемом Кодексом Российской Федерации об административных правонарушениях.

18.7. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной ответственности в порядке, установленном Федеральным законом от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации», Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном действующим законодательством.

19. Доступ к Политике

19.1. Действующая редакция Политики на бумажном носителе хранится по адресу Управления, указанному в п. 1.3. настоящей Политики.

19.2. Электронная версия Политики общедоступна на сайте Управления в сети Интернет, указанному в п. 1.3. настоящей Политики

20. Актуализация и утверждение Политики

20.1. Политика утверждается и вводится в действие приказом начальника Управления.

20.2. Актуализация Политики производится по мере необходимости. Внесение изменений (дополнений) в Политику производится приказом начальника Управления.

21. Заключительные положения

21.1. Положения настоящей Политики обязательны для соблюдения государственными гражданскими служащими (работниками) Управления.

21.2. Режим конфиденциальности персональных данных снимается в случаях их обезличивания, если иное не определено действующим законодательством Российской Федерации.