ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ВЕТЕРИНАРНОМУ И
ФИТОСАНИТАРНОМУ НАДЗОРУ
(Россельхознадзор)

УПРАВЛЕНИЕ ПО ТВЕРСКОЙ И ПСКОВСКОЙ ОБЛАСТЯМ

П Р И К А З

от 25 марта 2015 года № 75-П

г. Тверь

Об утверждении Политики Управления
Россельхознадзора по Тверской и Псковской областям
в отношении обработки и защиты персональных данных

В соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных", приказом Федеральной службы по ветеринарному и фитосанитарному надзору от 24.12.2014 № 779 «О персональных данных в Федеральной службы по ветеринарному и фитосанитарному надзору», п р и к а з ы в а ю:

1. Утвердить Политику Управления Россельхознадзора по Тверской и Псковской областям в отношении обработки и защиты персональных данных согласно приложению № 1 к настоящему приказу.
2. Приказы Управления от 28.02.2013 №48-П «Об утверждении Правил обработки и защиты персональных данных в Управлении Россельхознадзора по Тверской и Псковской областям» и от 17.12.2012 № 473-П № Об утверждении Правил рассмотрения запроса субъектов персональных данных или его представителя в Управлении Россельхознадзора по Тверской и Псковской областям» считать утратившими силу с момента подписания настоящего приказа.
3. В отношении обработки персональных данных в Управлении руководствоваться приказом Федеральной службы по ветеринарному и фитосанитарному надзору от 24.12.2014 № 779 «О персональных данных в Федеральной службы по ветеринарному и фитосанитарному надзору» и настоящим приказом.

4. Организационно-аналитическому отделу (Д.С. Богунова) разместить Политику, утвержденную настоящим приказом, на официальном сайте Управления в разделе "Работа с персональными данными".

5. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель Управления  М.В.Зорин

Приложение № 1
к приказу Управления
от 25.03.2015 № 75-П

ПОЛИТИКА УПРАВЛЕНИИЯ РОССЕЛЬХОЗНАДЗОРА ПО ТВЕРСКОЙ И ПСКОВСКОЙ ОБЛАСТЯМ В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Термины и определения

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного

государства, иностранному физическому лицу или иностранному юридическому лицу.

1.2. Назначение и правовая основа документа

Политика Управления Россельхознадзора по Тверской и Псковской областям (далее - Управление) в отношении обработки и защиты персональных данных (далее - Политика) определяет систему взглядов на проблему обеспечения безопасности персональных данных и представляет собой систематизированное изложение целей и задач защиты как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется Управление в своей деятельности, а также основных принципов построения организационных, технологических и процедурных аспектов обеспечения безопасности персональных данных.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский, Уголовный и Трудовой кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России, приказ Федеральной службы по ветеринарному и фитосанитарному надзору от 24.12.2014 № 779 «О персональных данных в Федеральной службы по ветеринарному и фитосанитарному надзору».

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности персональных данных Управления позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

2. Цели и задачи обеспечения безопасности персональных данных

2.1. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Управления от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

– доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем Управления, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);

– целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах Управления и передаваемой по каналам связи;
– конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

2.2. Основные задачи системы обеспечения безопасности персональных данных

Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности Управления должна обеспечивать эффективное решение следующих задач:
– своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Управления;
– создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
– защиту от вмешательства в процесс функционирования информационных систем Управления посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
– разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Управления (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
– обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
– защиту от несанкционированной модификации используемых в информационных системах Управления программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
– защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

2.3. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

– строгим учетом всех подлежащих защите ресурсов информационных систем Управления (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

– полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Управления по вопросам обеспечения безопасности информации;

– подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;

– наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Управления;

– четким знанием и строгим соблюдением всеми пользователями информационных систем Управления требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

– персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Управления;

– непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Управления;

– применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

– эффективным контролем над соблюдением пользователями информационных ресурсов Управления требований по обеспечению безопасности информации.

3. Основные принципы построения системы безопасности персональных данных

Построение системы обеспечения безопасности персональных данных Управления и ее функционирование должны осуществляться в соответствии со следующими основными принципами.

3.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности персональных данных Управления в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с персональными данными. Принятые меры безопасности персональных данных не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи информационной системы Управления должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

3.2. Системность

Системный подход к построению системы защиты информации в Управлении предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем Управления, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников). Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

3.3. Непрерывность защиты

Обеспечение безопасности персональных данных - процесс, осуществляемый руководством Управления, ответственным за организацию обработки персональных данных и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри Управления и каждый сотрудник Управления должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности Управления. И ее эффективность зависит от участия руководства Управления в обеспечении информационной безопасности персональных данных.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления защиты.

3.4. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем в целом и их систем защиты, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть

требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

3.5. Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты персональных данных на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем Управления и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

3.6. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационных систем Управления. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока персональные данные находятся в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

3.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

3.8. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к персональным данным должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

3.9. Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находиться под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования персональными данными и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями Управления. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

3.10. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе Управления. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственным за организацию обработки персональных данных.

3.11. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Управлением своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры Управления;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

3.12. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

3.13.Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

3.14. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты персональных данных должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности персональных данных.

3.15. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты персональных данных специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Управления (ответственными за организацию обработки персональных данных).

3.16. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности персональных данных, на основе используемых систем и средств защиты

персональных данных, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками Управления должны немедленно доводиться до сведения руководителя Управления и оперативно устраняться. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

4. Меры обеспечения информационной безопасности

4.1. Все меры обеспечения безопасности информационных систем Управления подразделяются на:

правовые - это действующие в стране законы, указы и нормативные правовые акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил.

организационные (административные) - это меры организационного характера, регламентирующие процессы функционирования системы обработки персональных данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

5. Условия и порядок обработки персональных данных государственных гражданских служащих Управления

5.1. Персональные данные государственных гражданских служащих Управления, граждан, претендующих на замещение должностей государственной гражданской службы Управления, обрабатываются в целях обеспечения кадровой работы, в том числе в целях содействия государственным служащим Управления в прохождении государственной службы, формирования кадрового резерва

государственной гражданской службы, обучения и должностного роста, учета результатов исполнения государственными служащими Управления должностных обязанностей, обеспечения личной безопасности государственных служащих Управления, и членов их семьи, обеспечения государственным служащим Управления установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества, а также в целях противодействия коррупции.

5.2. В целях, указанных в пункте 5.1 настоящей Политики, обрабатываются следующие категории персональных данных государственных служащих Управления, а также граждан, претендующих на замещение должностей государственной гражданской службы Управления:

- фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
- число, месяц, год рождения;
- место рождения;
- информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- адрес места жительства (адрес регистрации, фактического проживания);
- номер контактного телефона или сведения о других способах связи;
- реквизиты страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- реквизиты страхового медицинского полиса обязательного медицинского страхования;
- реквизиты свидетельства государственной регистрации актов гражданского состояния;
- семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);
- сведения о трудовой деятельности;
- сведения о воинском учете и реквизиты документов воинского учета;
- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);
- сведения об ученой степени;
- информация о владении иностранными языками, степень владения;
- медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению;
- фотография;
- сведения о прохождении государственной гражданской службы, в том числе: дата, основания поступления на государственную гражданскую службу и назначения на должность государственной гражданской службы, дата, основания

назначения, перевода, перемещения на иную должность государственной гражданской службы, наименование замещаемых должностей государственной гражданской службы с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности государственной гражданской службы, а также сведения о прежнем месте работы;

- информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту;
- сведения о пребывании за границей;
- информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы);
- информация о наличии или отсутствии судимости;
- информация об оформленных допусках к государственной тайне;
- государственные награды, иные награды и знаки отличия;
- сведения о профессиональной переподготовке и (или) повышении квалификации;
- информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;
- сведения о доходах, об имуществе и обязательствах имущественного характера;
- номер расчетного счета;
- номер банковской карты;
- иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 5.1 настоящей Политики.

5.3. Обработка персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы Управления, осуществляется при условии получения согласия указанных лиц в следующих случаях:

- при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации о государственной гражданской службе;
- при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

5.4. В случаях, предусмотренных пунктом 5.3. настоящей Политики, согласие субъекта персональных данных оформляется в письменной форме согласно приложению №1 и № 3 к настоящей Политике, если иное не установлено Федеральным законом "О персональных данных".

5.5. Обработка персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы Управления, осуществляется Отделом кадров Управления и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение,

уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5.6. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы Управления, осуществляется путем:

- получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые в отдел кадров);
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- формирования персональных данных в ходе кадровой работы;
- внесения персональных данных в информационные системы Управления.

5.7. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы Управления.

5.8. В случае возникновения необходимости получения персональных данных государственного служащего Управления у третьей стороны, следует известить об этом государственного служащего заранее, получить их письменное согласие согласно приложению № 2 к настоящей Политике и сообщить им о целях, предполагаемых источниках и способах получения персональных данных.

5.9. Запрещается получать, обрабатывать и приобщать к личному делу государственного служащего Управления персональные данные, не предусмотренные пунктом 5.2 настоящей Политики, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

5.10. При сборе персональных данных сотрудник отдела кадров Управления, осуществляющий сбор (получение) персональных данных непосредственно от государственных служащих Управления обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные (Приложение № 6 к Политике).

5.11. В Управлении утверждается Перечень должностей государственных служащих, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (Приложение № 4 к настоящей Политике).

5.12. Передача (распространение, предоставление) и использование персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы Управления, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

5.13. Государственные служащие, непосредственно осуществляющие обработку персональных данных в Управлении, дают обязательство о неразглашении информации, содержащей персональные данные (Приложение № 7 к Политике).

5.14. В случае расторжения служебного контракта с государственным

служащим, непосредственно осуществляющим обработку персональных данных в Управлении, с него берется обязательство о прекращении обработки персональных данных, ставших ему известными в связи с исполнением должностных обязанностей (Приложение № 5 к Политике).

6. Условия и порядок обработки персональных данных государственных служащих Управления и лиц, состоящих с ними в родстве (свойстве), в связи с рассмотрением вопроса о предоставлении единовременной субсидии на приобретение жилого помещения

6.1. В Управлении осуществляется обработка персональных данных государственных служащих Управления и лиц, состоящих с ними в родстве (свойстве), в связи с рассмотрением вопроса о предоставлении единовременной субсидии на приобретение жилого помещения.

6.2. Перечень персональных данных, подлежащих обработке в связи с предоставлением единовременной субсидии на приобретение жилого помещения, определяется постановлением Правительства Российской Федерации "О предоставлении федеральным государственным гражданским служащим единовременной субсидии на приобретение жилого помещения", и включает в себя:

- фамилию, имя, отчество;
- вид, серию, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дату выдачи;
- адрес места жительства (адрес постоянной регистрации, адрес временной регистрации, адрес фактического места жительства);
-. сведения о составе семьи;
- персональные данные, содержащиеся в выписке из домовой книги, копиях финансового лицевого счета, свидетельства о браке, свидетельства о рождении ребенка (детей), трудовой книжки, документов о наличии в собственности государственного служащего и (или) членов его семьи жилых помещений, кроме жилого помещения, в котором они зарегистрированы (с предоставлением при необходимости их оригиналов), документа, подтверждающего право на дополнительную площадь жилого помещения;
- иные персональные данные, предусмотренные законодательством Российской Федерации.

6.3. Обработка персональных данных государственных служащих Управления при постановке на учет для получения единовременной выплаты осуществляется на основании заявления государственного служащего, представляемого на имя руководителя Управления в территориальную подкомиссию Комиссии Россельхознадзора для рассмотрения вопросов предоставления федеральным государственным гражданским служащим единовременной субсидии на приобретение жилого помещения (далее –подкомиссия Управления).

6.4. Обработка персональных данных государственных служащих Управления в связи с предоставлением единовременной субсидии на приобретение жилого помещения, в частности сбор, запись, систематизация, накопление и уточнение

(обновление, изменение) персональных данных, осуществляется должностными лицами Управления, входящими в состав подкомиссии Управления, путем:

- получения оригиналов необходимых документов;
- предоставления заверенных в установленном порядке копий документов.

6.5. Подкомиссия Управления вправе проверять сведения, содержащиеся в документах, представленных государственными служащими Управления о наличии условий, необходимых для постановки государственного служащего на учет для получения единовременной субсидии на получение жилья.

6.6. Передача (распространение, предоставление) и использование персональных данных государственных служащих Управления, полученных в связи с предоставлением единовременной субсидии на приобретение жилого помещения, осуществляется лишь в случаях и в порядке, предусмотренных законодательством Российской Федерации.

7. Условия и порядок обработки персональных данных субъектов в связи с предоставлением государственных услуг и исполнением государственных функций

7.1. В Управлении обработка персональных данных физических лиц осуществляется в целях предоставления следующих государственных услуг и исполнения государственных функций:

7.1.1. организация приема граждан, обеспечение своевременного и в полном объеме рассмотрения устных и письменных обращений граждан по вопросам, относящимся к компетенции Управления;

7.1.2. разрешительная деятельность в области карантина растений;

7.1.3. лицензирование фармацевтической деятельности.

7.2. Персональные данные граждан, обратившихся в Управление лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением заявителей о результатах рассмотрения.

В соответствии с законодательством Российской Федерации в Управлении подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан и лиц без гражданства.

7.3. В рамках рассмотрения обращений граждан подлежат обработке следующие персональные данные заявителей:

- фамилия, имя, отчество (последнее при наличии);
- почтовый адрес;
- адрес электронной почты;
- указанный в обращении контактный телефон;
- иные персональные данные, указанные заявителем в обращении (жалобе), а также ставшие известными в ходе личного приема или в процессе рассмотрения поступившего обращения.

7.4. При лицензировании фармацевтической деятельности осуществляется обработка следующих персональных данных заявителей:

- фамилия, имя, отчество (последнее при наличии);
- вид, серия, номер документа, удостоверяющего личность;
- адрес места жительства;
- номер контактного телефона и, при наличии, адрес электронной почты.

7.5. В рамках разрешительной деятельности в области карантина растений обрабатываются следующие персональные данные заявителей:
- фамилия, имя, отчество (последнее при наличии);
- вид, серия, номер документа, удостоверяющего личность;
- адрес места жительства;
- номер контактного телефона и, при наличии, адрес электронной почты.

7.6. Обработка персональных данных, необходимых в связи с предоставлением государственных услуг и исполнением государственных функций, указанных в пункте 7.1 настоящей Политики, осуществляется без согласия субъектов персональных данных в соответствии с пунктом 4 части 1 статьи 6 Федерального закона "О персональных данных", Федеральными законами "Об организации предоставления государственных и муниципальных услуг", "О порядке рассмотрения обращений граждан Российской Федерации", "О лицензировании отдельных видов деятельности", и иными нормативными правовыми актами, определяющими предоставление государственных услуг и исполнение государственных функций в установленной сфере ведения Управления.

7.7. Обработка персональных данных, необходимых в связи с предоставлением государственных услуг и исполнением государственных функций, указанных в пункте 7.1 настоящей Политики, осуществляется структурными подразделениями Управления, предоставляющими соответствующие государственные услуги и (или) исполняющими государственные функции, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

7.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, обратившихся в Управление для получения государственной услуги или в целях исполнения государственной функции, осуществляется путем:

7.8.1. получения оригиналов необходимых документов (заявление);

7.8.2. заверения копий документов;

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

7.8.4. внесения персональных данных в прикладные программные подсистемы Единой информационной системы Управления.

7.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (заявителей).

7.10. При предоставлении государственной услуги или исполнении государственной функции Управлением запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные в

случаях, не предусмотренных законодательством Российской Федерации.

7.11. При сборе персональных данных уполномоченное должностное лицо структурного подразделения Управления, осуществляющее получение персональных данных непосредственно от субъектов персональных данных, обратившихся за предоставлением государственной услуги или в связи с исполнением государственной функции, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

7.12. Передача (распространение, предоставление) и использование персональных данных заявителей (субъектов персональных данных) Управления осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

8. Порядок обработки персональных данных субъектов персональных данных в информационных системах

8.1. Обработка персональных данных в Управлении осуществляется:

8.1.1. в Единой финансово-кадровой системе (ЕФКС);

8.1.2. в Единой информационной системе персональных данных Управления «Бухгалтерия и кадры»;

8.1.3. на автоматизированных рабочих местах сотрудников отдела кадров и отдела экономики и финансов, бухгалтерского учета и отчетности Управления;

8.1.4. в системе межведомственного электронного взаимодействия.

8.2. Для обработки персональных данных используется следующее программное обеспечение:

- Единая финансово-кадровая система (ЕФКС);
- 1С:Предприятие 8. Бухгалтерия государственного учреждения;
- 1С:Зарплата и кадры бюджетного учреждения 8;
- Контур-Персонал Государственная служба;
- 1С:Документооборот 8 КОРП.

8.3. Государственным служащим структурных подразделений Управления, имеющим право осуществлять обработку персональных данных в информационных системах Управления, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными регламентами государственных служащих Управления.

8.4. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Управления, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

8.4.1. определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Управления;

8.4.2. применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах

персональных данных Управления, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

8.4.3. применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

8.4.4. оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

8.4.5. учет машинных носителей персональных данных;

8.4.6. обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

8.4.7. восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;

8.4.8. установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных Управления, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Управления;

8.4.9. контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

8.5. Структурное подразделение Управления, ответственное за обеспечение функционирования информационных систем персональных данных, организует и контролирует ведение учета материальных носителей персональных данных.

8.6. Структурное подразделение Управления, ответственное за обеспечение функционирования информационных систем персональных данных при их обработке в информационных системах персональных данных Управления, должно обеспечить:

8.6.1. своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в Управлении и руководителя Управления;

8.6.2. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

8.6.3. возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8.6.4. постоянный контроль за обеспечением уровня защищенности персональных данных;

8.6.5. знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

8.6.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

8.6.7. при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных

пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;

8.6.8. разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

8.7. Структурное подразделение Управления, ответственное за обеспечение функционирования информационных систем персональных данных в Управлении, принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

8.8. Обмен персональными данными при их обработке в информационных системах персональных данных Управления осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

8.9. Доступ государственных служащих Управления к персональным данным, находящимся в информационных системах персональных данных Управления, предусматривает обязательное прохождение процедуры идентификации и аутентификации.

8.10. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных Управления уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

9. Обработка персональных данных в рамках межведомственного информационного взаимодействия с применением единой системы межведомственного электронного взаимодействия

9.1. Управление в соответствии с законодательством Российской Федерации осуществляет обработку персональных данных в рамках межведомственного электронного информационного взаимодействия в электронном виде с федеральными органами государственной власти с применением единой системы межведомственного электронного взаимодействия (далее - СМЭВ).

9.2. Управление в рамках СМЭВ вправе направить межведомственные запросы о предоставлении информации, включающей персональные данные субъектов, в следующие федеральные органы исполнительной власти:

9.2.1. в УФНС по Тверской области, УФНС по Псковской области -

о предоставлении информации из Единого государственного реестра юридических лиц и Единого государственного реестра индивидуальных

предпринимателей (сведения об учредителях - физических лицах);

9.2.2. в Федеральную службу государственной регистрации, кадастра и картографии - о предоставлении информации из Единого государственного реестра прав на недвижимое имущество в отношении правообладателей (фамилия, имя, отчество, дата рождения, серия и номер основного документа, удостоверяющего личность, место рождения, адрес места жительства, гражданство).

10. Сроки обработки и хранения персональных данных

10.1. Сроки обработки и хранения персональных данных государственных служащих Управления, граждан, претендующих на замещение должностей государственной службы Управления, определяются в соответствии с законодательством Российской Федерации. С учетом положений законодательства Российской Федерации, устанавливаются следующие сроки обработки и хранения персональных данных государственных служащих:

10.1.1. Персональные данные, содержащиеся в приказах по личному составу государственных служащих Управления (о приеме, о переводе, об увольнении, об установлении надбавок), подлежат хранению в отделе кадров Управления в течение двух лет, с последующим формированием и передачей указанных документов в архив Управления или государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение 75 лет.

10.1.2. Персональные данные, содержащиеся в личных делах государственных служащих Управления, а также личных карточках государственных служащих Управления, хранятся в отделе кадров Управления в течение десяти лет, с последующим формированием и передачей указанных документов в архив Управления или государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение 75 лет.

10.1.3. Персональные данные, содержащиеся в приказах о поощрениях, материальной помощи государственных служащих Управления, подлежат хранению в течение двух лет в отделе кадров Управления с последующим формированием и передачей указанных документов в архив Управления или государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение 75 лет.

10.1.4. Персональные данные, содержащиеся в приказах о предоставлении отпусков, о краткосрочных внутрироссийских и зарубежных командировках, о дисциплинарных взысканиях государственных служащих Управления, подлежат хранению в отделе кадров Управления в течение пяти лет с последующим уничтожением.

10.1.5. Персональные данные, содержащиеся в документах претендентов на замещение вакантной должности государственной службы в Управлении, не допущенных к участию в конкурсе, и кандидатов, участвовавших в конкурсе, хранятся в отделе кадров Управления в течение 3 лет со дня завершения конкурса, после чего подлежат уничтожению.

10.2. Сроки обработки и хранения персональных данных, предоставляемых

субъектами персональных данных в Управление в связи с получением государственных услуг и исполнением государственных функций, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

10.3. Персональные данные граждан, обратившихся в Управление лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в течение пяти лет.

10.4. Персональные данные, предоставляемые субъектами на бумажном носителе в связи с предоставлением Управлением государственных услуг и исполнением государственных функций, хранятся на бумажных носителях в структурных подразделениях Управления, к полномочиям которых относится обработка персональных данных в связи с предоставлением государственной услуги или исполнением государственной функции, в соответствии с утвержденными положениями о соответствующих структурных подразделениях Управления.

10.5. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

10.6. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных Политикой.

10.7. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители структурных подразделений Управления.

10.8. Срок хранения персональных данных, внесенных в информационные системы персональных данных Управления, должен соответствовать сроку хранения бумажных оригиналов.

11. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

11.1. Структурными подразделениями Управления осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

11.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании комиссии Управления, состав которой утверждается приказом Управления.

По итогам заседания составляются протокол и Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами комиссии и утверждается руководителем Управления.

11.3. Уничтожение документов, содержащих персональные данные,

осуществляется в порядке, установленном законодательством Российской Федерации.

11.4. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

Приложение № 1
к Политике

СОГЛАСИЕ
на передачу (предоставление) персональных данных третьим лицам

Я,_____
(должность, Ф.И.О.)
Зарегистрированный по адресу:_____
Паспорт №_____серия_____,
выдан_____
в соответствии со ст.ст.7 и 9 Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" даю согласие оператору - Управлению Федеральной службы по ветеринарному и фитосанитарному надзору (Россельхознадзора) по Тверской и Псковской областям (Управление Россельхознадзора по Тверской и Псковской областям), расположенному по адресу: 170008, г. Тверь, ул. Озерная, 9, на передачу моих персональных данных о _____
кому_____с
целью_____
способом_____
Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

(дата) (подпись) (расшифровка подписи)

Приложение № 2 к Политике

СОГЛАСИЕ
на получение персональных данных у третьих лиц

Я,_____
(должность, Ф.И.О.)

Зарегистрированный по адресу:_____

Паспорт №_____серия_____, выдан_____

в соответствии со ст.ст.7 и 9 Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" даю согласие оператору - Управлению Федеральной службы по ветеринарному и фитосанитарному надзору (Россельхознадзора) по Тверской и Псковской областям (Управление Россельхознадзора по Тверской и Псковской областям), расположенному по адресу: 170008, г. Тверь, ул. Озерная, 9, на получение моих персональных данных о _____

от кого_____

с целью_____

способом_____

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

(дата) (подпись) (расшифровка подписи)

Приложение № 3
к Политике

СОГЛАСИЕ
на обработку персональных данных

Я,_____
_____ (фамилия, имя, отчество субъекта персональных данных)
зарегистрированный(ая) по адресу:_____
основной документ, удостоверяющий личность: паспорт № серия_____№_____выдан_____
в соответствии с п. 4 ст. 9 Федерального закона от 27.07.2006 г. N 152-ФЗ "О персональных данных" в целях обеспечения соблюдения Конституции Российской Федерации, трудового законодательства, других законов и иных нормативных правовых актов, содействия гражданскому служащему (гражданину) в прохождении гражданской службы (в трудоустройстве), обучении и продвижения по службе (работе), обеспечения личной безопасности гражданского служащего (работника) и членов его семьи, контроля количества и качества выполняемой работы и обеспечения сохранности имущества даю согласие оператору: Управлению Федеральной службы по ветеринарному и фитосанитарному надзору (Россельхознадзора) по Тверской и Псковской областям, находящемуся по адресу: 170008, г. Тверь, ул. Озерная, 9,
на обработку моих персональных данных, а именно: фамилия, имя, отчество; число, месяц, год и место рождения; номер основного документа, удостоверяющего личность; сведения о дате выдачи указанного документа и выдавшем его органе; адрес регистрации; адрес проживания; семейное положение; образование, в том числе сведения о документах подтверждающих его; социальное, имущественное положение; профессия;сведения с места работы; доходы; другие сведения, предоставленные мною при приеме на службу (работу) и совершение над ними следующих действий: обработку, сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), подтверждение, использование, уничтожение по истечению срока действия Согласия, то есть на совершение действий, предусмотренных п. 3 ч. 1 ст. 3 от 27.07.2006 г. N 152-ФЗ Федерального закона "О персональных данных".

Настоящее согласие действует с момента подписания и до момента прекращения хранения личного дела, или его отзыва в письменной форме.

Дата Подпись

Приложение № 4
к Политике

Перечень должностей
государственных гражданских служащих в структурных
подразделениях Управления Россельхознадзора
по Тверской и Псковской областям, замещение которых
предусматривает осуществление обработки
или доступа к персональным данным

1. Помощник руководителя Управления
2. Начальники структурных подразделений (отделов)
3. Заместители начальников структурных подразделений (отделов)

В отделе экономики и финансов, бухгалтерского учета и отчетности:

4. Главный специалист-эксперт
5. Ведущий специалист-эксперт
6. Старший специалист 1 разряда

В отделе правовой работы:

7. Главный специалист-эксперт
8. Ведущий специалист-эксперт

В организационно-аналитическом отделе:

9. Главный специалист-эксперт
10. Ведущий специалист-эксперт
11. Старший специалист 1 разряда

В отделе кадров:

12. Главный специалист-эксперт
13. Ведущий специалист-эксперт
14. Старший специалист 1 разряда

В отделе материально-технического обеспечения:

15. Специалист – эксперт

В Псковском хозяйственно-техническом отделе:

16. Главный специалист-эксперт

Приложение № 5
к Политике

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
о прекращении обработки персональных данных лица,
непосредственно осуществляющего обработку персональных данных,
в случае расторжения с ним контракта

Я _____
(фамилия, имя, отчество)
_____
(должность)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта (договора), освобождения меня от замещаемой должности и увольнения.

В соответствии со статьей 7 Федерального закона от 27 июля 2006г № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная Федеральным законом от 27 июля 2006г № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснена.

дата подпись

Приложение № 6
к Политике

ТИПОВАЯ ФОРМА
разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Мне _____,
(фамилия, имя, отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные оператору – Управлению Россельхознадзора по Тверской и Псковской областям.

В соответствии с Постановлением Правительства Российской Федерации от 21.03.2012г. № 211 «Перечень мер направленных на обеспечение выполнения обязанностей предусмотренных Федеральным законом «О персональных данных», приказом Федеральной службы по ветеринарному и фитосанитарному надзору от 24.12.2014г. № 779 «О персональных данных в Федеральной службы по ветеринарному и фитосанитарному надзору», Политикой Управления Россельхознадзора по Тверской и Псковской областям в отношении обработки и защитыперсональных данных определён перечень персональных данных, которые субъект персональных данных обязан предоставить в целях обеспечения соблюдения Конституции Российской Федерации, трудового законодательства, других законов и иных нормативных правовых актов, содействия гражданскому служащему (гражданину) в прохождении гражданской службы (в трудоустройстве), обучении и продвижения по службе (работе), обеспечения личной безопасности гражданского служащего (работника) и членов его семьи, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Я предупрежден, что в случае несогласия на обработку моих персональных данных, (далее нужное подчеркнуть) мои права могут быть реализованы не в полном объеме.

Без представления субъектом персональных данных обязательных для заключения служебного контракта сведений, служебный контракт не может быть заключен.

На основании пункта 11 части 1 статьи 33 Федерального закона от 27.07.2004г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» служебный контракт прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности гражданской службы.

Дата подпись

Приложение № 7
к Политике

ОБЯЗАТЕЛЬСТВО
о неразглашении информации, содержащей персональные данные

Я,_____
(фамилия, имя, отчество лица, допущенного к обработке персональных данных)
исполняющий(ая) должностные обязанности по замещаемой должности
_____
предупрежден(а) о том, что на период исполнения должностных обязанностей 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 случае расторжения договора (контракта) и (или) 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 нарушение данного обязательства является основанием привлечения к дисциплинарной ответственности и (или) иной ответственности в соответствии с законодательством Российской Федерации.

дата подпись