Приложение № 3
к приказу ФГБУ «Рослесинфорг»
от «25» 07 2016 г. № 231

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Федеральном государственном бюджетном учреждении «Рослесинфорг»

I. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Федеральном государственном бюджетном учреждении «Рослесинфорг» (далее – Правила, Учреждение) разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и законодательством Российской Федерации о персональных данных.

1.2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Учреждении и действуют постоянно.

1.3. Под Учреждением понимается ФГБУ «Рослесинфорг» и его филиалы.

II. Тематика проведения внутреннего контроля

2.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

а) соответствие полномочий пользователя правилам доступа;

б) соблюдение пользователями информационных систем персональных данных Учреждения парольной политики;

в) соблюдение пользователями информационных систем персональных данных Учреждения антивирусной политики;

г) соблюдение пользователями информационных систем персональных данных Учреждения правил работы со сменными (съемными) носителями персональных данных;

д) соблюдение порядка доступа в помещения Учреждения, в которых ведется автоматизированная (с использованием информационных систем персональных данных) обработка персональных данных;

е) соблюдение порядка резервирования баз данных и хранения резервных копий;

ж) соблюдение порядка работы со средствами защиты информации;

з) знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях.

2.2. Тематика проверок обработки персональных данных без использования средств автоматизации:

а) соответствие полномочий работников правилам доступа к бумажным носителям с персональными данными;

б) организация работы с бумажными носителями с персональными данными;

в) организация хранения бумажных носителей с персональными данными;

г) соблюдение порядка доступа к бумажным носителям с персональными данными;

д) соблюдение порядка доступа в помещения Учреждения, в которых ведется обработка персональных данных без использования средств автоматизации и хранятся бумажные носители с персональными данными.

III. Порядок организации и проведения внутренних проверок

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных Учреждение организует проведение периодических проверок соблюдения порядка и условий обработки персональных данных.

3.2. Организация проверки соблюдения порядка и условий обработки персональных данных поручается ответственному за организацию обработки персональных данных (далее – ответственный за организацию обработки ПДн):

3.2.1. В центральном аппарате – отдела информационной безопасности;

3.2.2. В филиале – подразделения, обеспечивающего информационную безопасность филиала,

и оформляется приказом директора ФГБУ «Рослесинфорг» (директора филиала Учреждения) либо лица, его замещающего.

3.3. В случае отсутствия в филиале:

3.3.1. Подразделения, обеспечивающего его информационную безопасность, организация проверки соблюдения порядка и условий обработки ПДн поручается специалисту, выполняющему данные обязанности, ответственному за организацию обработки ПДн;

3.3.2. Штатной единицы специалиста, выполняющего обязанности по обеспечению информационной безопасности филиала, организация проверки соблюдения порядка и условий обработки ПДн поручается ответственному за организацию обработки ПДн отдела информационной безопасности центрального аппарата Учреждения.

3.4. Проведение проверки соблюдения порядка и условий обработки персональных данных поручается:

3.4.1. В центральном аппарате:

- отделу информационной безопасности;
- отделу кадров;
- отделу бухгалтерского учета и отчетности;
- отделу правовой экспертизы, договоров и локально-нормативных актов.

3.4.2. В филиале:

- специалисту или подразделению, обеспечивающему информационную безопасности, филиала;
- специалисту или подразделению, осуществляющему кадровую работу, филиала;
- отделу бухгалтерского и налогового учета и отчетности;
- специалисту или подразделению, осуществляющему юридическое (правовое) сопровождение деятельности филиала.

3.5. Для проведения проверки соблюдения порядка и условий обработки персональных данных приказом директора ФГБУ «Рослесинфорг» (директора филиала), либо лица, его замещающего, формируется комиссия, в состав которой включаются работники Учреждения, указанные в пунктах 3.3.1 и 3.3.2 настоящих Правил, занимающие должности, по которым предусматривается осуществление обработки персональных данных либо доступ к персональным данным которым разрешен.

3.6. При проведении проверки соблюдения порядка и условий обработки персональных данных, содержащихся в документах, составляющих государственную тайну, комиссия формируется с учетом положений законодательства о государственной тайне.

3.7. Проверки соблюдения порядка и условий обработки персональных данных проводятся по необходимости, но не реже 1 раза в год.

3.8. Проверки соблюдения порядка и условий обработки персональных данных проводятся непосредственно на месте обработки персональных данных путем:

- опроса работников, осуществляющих обработку персональных данных либо участвующих в процессе их обработки;
- осмотра рабочих мест работников, осуществляющих обработку персональных данных либо участвующих в процессе их обработки;
- проверки посредством применения электро-вычислительных устройств утечки, несанкционированного использования и проникновения к информации, содержащей персональные данные, с автоматизированных рабочих мест

работников, осуществляющих обработку персональных данных либо участвующих в процессе их обработки.

3.9. По результатам проведения проверки соблюдения порядка и условий обработки персональных данных составляется акт. Форма акта по результатам проведения проверки соблюдения порядка и условий обработки персональных данных (далее – Акт) приведена в приложении к настоящим Правилам. В Акте указывается:

3.9.1. номер и дата составления акта;

3.9.2. фамилия, инициалы, должности членов комиссии;

3.9.3. тематика проверки;

3.9.4. наименование и реквизиты (дата регистрации и номер) документа/нормативного правого акта, на основании требований которого проводится проверка;

3.9.5. краткое описание проведенных мероприятий в ходе проверки;

3.9.6. выявленные в процессе проведения проверки нарушения;

3.9.7. меры по устранению нарушений;

3.9.8. сроки устранения выявленных нарушений.

3.10. Акт подписывается всеми членами комиссии, принимавшими участие в проверке соблюдения порядка и условий обработки персональных данных и утверждается директором ФГБУ «Рослесинфорг» (директором филиала) либо лицом, его замещающим.

3.11. О результатах проверки соблюдения порядка и условий обработки персональных данных и мерах, необходимых для устранения нарушений, директору ФГБУ «Рослесинфорг» (директору филиала) либо лицу, его замещающему, докладывает ответственный за организацию обработки ПДн.

3.12. В случае выявления в процессе проведения проверки нарушений, касающихся соблюдения порядка и условий обработки персональных данных в Учреждении, на основании Акта (центрального аппарата и/или филиала) директор ФГБУ «Рослесинфорг» либо лицо, его замещающее, может принять решение о проведении в отношении работников Учреждения, ответственных за организацию обработки персональных данных, а также осуществляющих обработку персональных данных, служебной проверки и применения к виновным лицам мер дисциплинарной ответственности.

3.13. Акты хранятся:

3.13.1. В центральном аппарате:

- в отделе информационной безопасности.

3.13.2. В филиале:

- у специалиста, ответственного за информационную безопасность.

3.13.3. Акты хранятся в течение 1 года, а после истечения указанного срока подлежат уничтожению. При необходимости Акты могут храниться до полного устранения нарушений.

3.14. Уничтожение актов проводится работником, ответственным за организацию обработки персональных данных, у которого или в отделе, где он занимает должность, они хранятся, с составлением соответствующего документа в произвольной форме.

Приложение
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям к
защите персональных данных в ФГБУ
«Рослесинфорг»

УТВЕРЖДАЮ
Директор ФГБУ «Рослесинфорг»
(Директор филиала (указывается
наименование филиала) ФГБУ
«Рослесинфорг»)
_____ (Ф.И.О.)
«___»_____20____ г.

АКТ № ____
проведения проверки соблюдения порядка и условий обработки персональных данных

Настоящий Акт составлен в том, что «____» _____ 20____ года, комиссией для проведения проверки соблюдения порядка и условий обработки персональных данных в составе:
председателя комиссии:

_____,
(замещаемая должность гражданской службы, Ф.И.О. гражданского служащего)
членов комиссии:

_____;
(замещаемая должность гражданской службы, Ф.И.О. гражданского служащего)

_____;
(замещаемая должность гражданской службы, Ф.И.О. гражданского служащего)

_____,
(замещаемая должность гражданской службы, Ф.И.О. гражданского служащего)
проведена проверка _____
(тематика проверки)

Проверка соблюдения порядка и условий обработки персональных данных осуществлялась в соответствии с требованиями _____

_____

_____

_____
(наименование и реквизиты (дата регистрации и номер) документа/нормативного правого акта)

В ходе проверки проведены следующие мероприятий:

_____

_____

_____

_____

_____

В процессе проведения проверки выявлены нарушения:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Меры по устранению нарушений:

_____

_____

_____

_____

_____

_____

Сроки устранения выявленных нарушений: _____.

Председатель комиссии _____ (И.О. Фамилия)

Члены комиссии: _____ (И.О. Фамилия)

_____ (И.О. Фамилия)

_____ (И.О. Фамилия)

Должность начальника проверяемого отдела _____ (И.О. Фамилия)