Работа с персональными данными в учреждении

Шаг 1

Проанализировать все эксплуатируемые информационные системы и традиционные хранилища данных, выявить все, где присутствуют и обрабатываются персональные данные.

Шаг 2

Оценить наличие предусмотренных законом оснований для обработки персональных данных, в случаях, когда они отсутствуют - получить согласие субъекта.

Отдельный вопрос - передача персональных данных

Шаг 3

Пересмотреть договора с работниками и физическими лицами в части обработки персональных данных и, особенно, их распространения

Шаг 4

Сформировать Перечень обрабатываемых персональных данных

Шаг 5

Определить и зафиксировать документально предельные сроки хранения персональных данных после расторжения (прекращения) договора с работником, клиентом, абонентом (физическими лицами), исходя из сроков:

- ✓ требований законодательства:
  - Трудового
  - Пенсионного
  - Об ОРД (например, постановления правительства № 538 2005 г.)
  - …
- ✓ исковой давности взаимных претензий оператора и клиента

ОПУБЛИКОВАНИЕ

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ ОТ 10 ИЮЛЯ 2013 Г. N 582 "ОБ УТВЕРЖДЕНИИ ПРАВИЛ РАЗМЕЩЕНИЯ НА ОФИЦИАЛЬНОМ САЙТЕ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ" И ОБНОВЛЕНИЯ ИНФОРМАЦИИ ОБ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ"

ОБЗОР ДОКУМЕНТА

Какую информацию должны публиковать образовательные организации?

Образовательные организации размещают на своих сайтах некоторые данные.

Это, в частности, сведения о дате создания организации, ее учредителях, месте нахождения, графике работы, уровне образования, формах обучения. Также публикуется информация о сроке действия госаккредитации образовательной программы, учебном плане, бюджетных местах, языках, на которых ведется обучение, педагогических работниках, выплачиваемых стипендиях, наличии общежития.

Помимо этого на сайте размещаются копии следующих документов. Это устав образовательной организации, лицензия на осуществление деятельности, свидетельство о госаккредитации, план финансово-хозяйственной деятельности и др. Также опубликованию подлежит отчет о результатах самообследования.

Сведения обновляются в течение 10 рабочих дней после их изменения. Информация представляется в текстовом формате или в форме таблиц.

Сведения публикуются на русском языке. Также могут быть использованы языки республик и иностранные языки. На сайте обязательно должна быть ссылка на сайт Минобрнауки России.

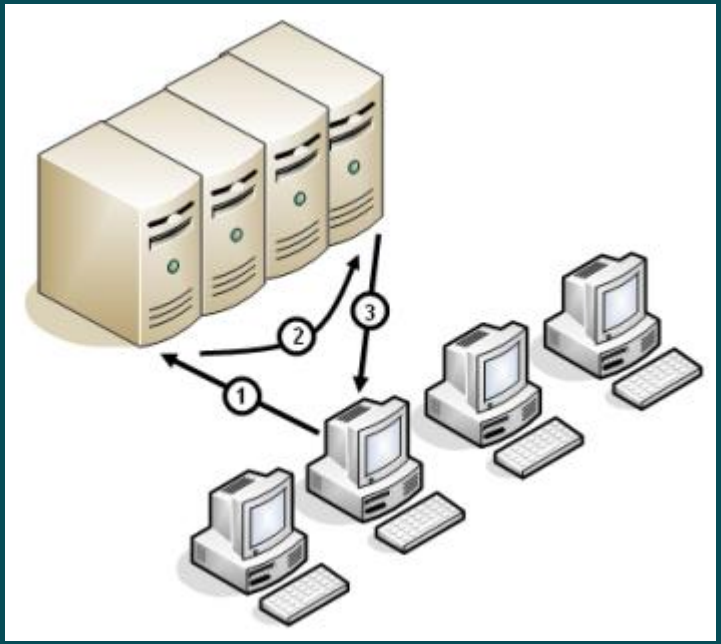
Установлены требования к используемым технологическим и программным средствам.

Прежний порядок утрачивает силу.

Постановление вступает в силу с 1 сентября 2013 г.

Ограничение доступа к персональным данным. Учет лиц, допущенных к персональным данным.

Организация доступа пользователей к ИСПДн



1. Инвентаризация информационных ресурсов, выявление приложений, где ведется обработка персональных данных
2. Назначение и обучение лиц, ответственных за конкретный ресурс, содержащий персональные данные
3. Определение и документирование процедуры предоставления доступа к ИСПДн (роли: пользователь, линейный руководитель, ответственный за ресурс, принимающий решение, администратор, супервизор)
4. Организация контроля за соблюдением процедуры

Организация доступа пользователей к ИСПДн

Роль	Полномочия
Пользователь	Имеет доступ к персональным данным, обрабатываем в ИСПДн, для выполнения служебных (трудовых) обязанностей
Линейный руководитель	Руководитель структурного подразделения, где работает пользователь, имеющий право инициировать заявку на доступ к ИСПДн с указанием требуемых прав
Ответственный за ресурс	Лицо, в чьих интересах создан ресурс ИСПДн, согласовывающий заявку на пользователя
Принимающий решение	Лицо, утверждающее заявку и разрешающий конфликты между Линейным руководителем и ответственным за ресурс
Администратор	Администратор ИС (сервера, сети), выполняющий технические действия по предоставлению пользователю доступа к ресурсу в соответствии заявкой
Супервизор	Работник СИБ (администратор безопасности), контролирующий соблюдение процедуры предоставления доступа и фактические списки пользователей ресурсов ИСПДн (без доступа к персональным данным)

Внутренние нормативные документы по охране конфиденциальности сведений:

1. Перечень персональных данных
2. Модель угроз и нарушителя безопасности персональных данных
3. Акт об установлении уровня защищенности ПДн
4. Положение (инструкция, руководство) об обеспечении безопасности персональных данных при их обработке
5. Описание системы защиты, обеспечивающей нейтрализацию угроз для соответствующего уровня защищенности ПДн
6. Заключения о возможности эксплуатации средств защиты персональных данных

ФЗ «О персональных данных»

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Постановление Правительства РФ от 1 ноября 2012 г. №1119

«Об утверждении требований к защите персональных данных

при их обработке в информационных системах

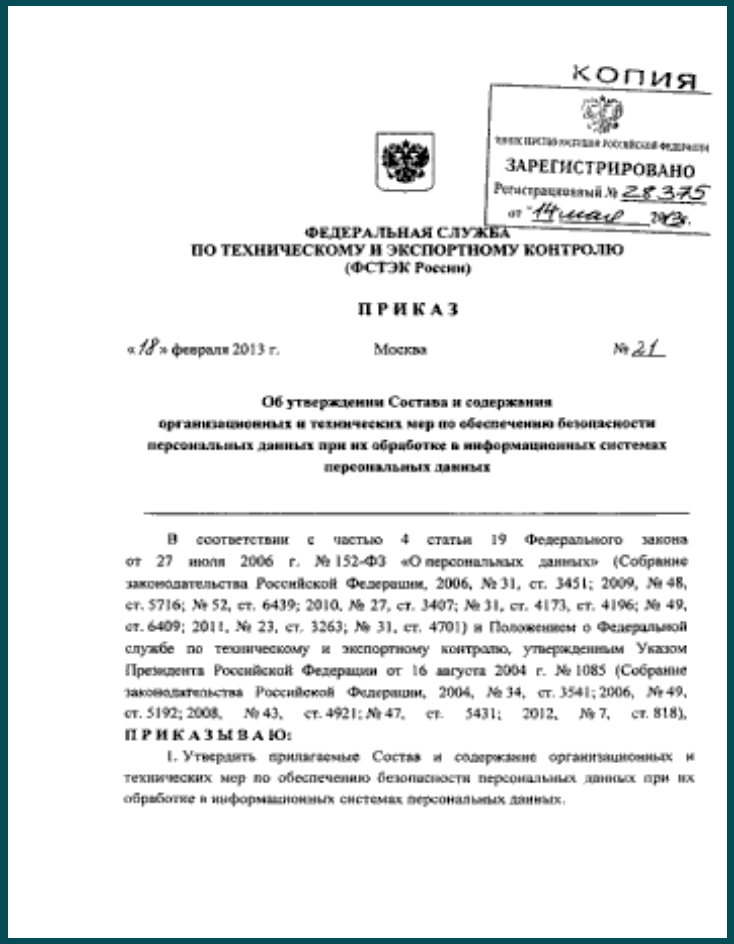
персональных данных»

В соответствии со статьей 19 Федерального закона "О персональных данных» Правительство Российской Федерации п о с т а н о в л я е т :

1. Утвердить прилагаемые требования к защите персональных данных при их обработке в информационных системах персональных данных.

2. Признать утратившим силу постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2007, № 48, ст. 6001).

Федеральная служба по техническому и экспортному контролю (ФСТЭК РФ)



КОПИЯ

ЗАРЕГИСТРИРОВАНО
Регистрационный № 28375
от "14" мая 2013 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

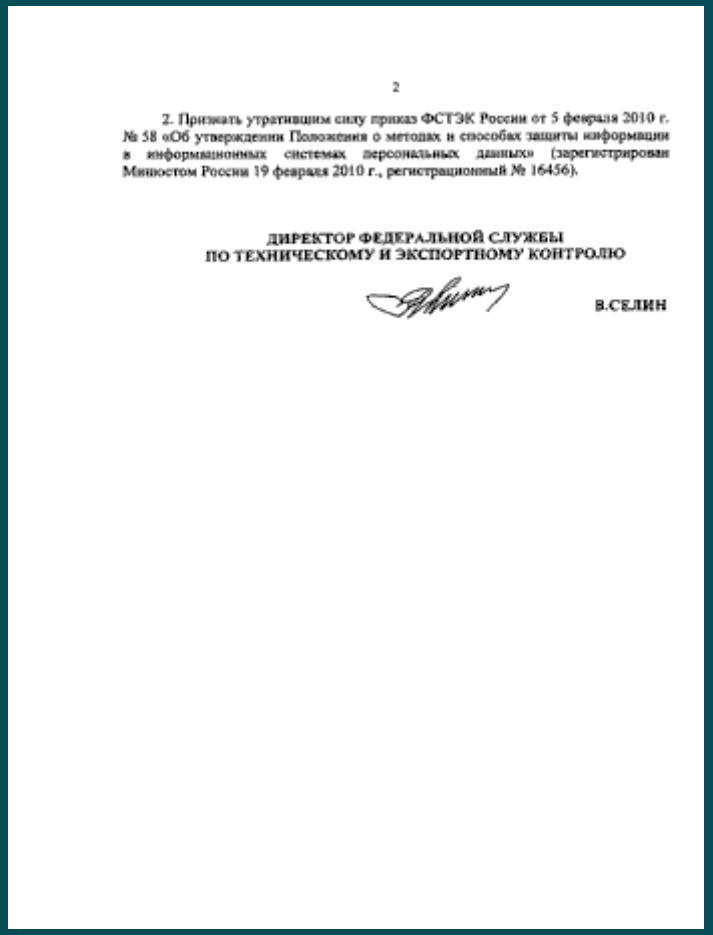
«18» февраля 2013 г. Москва № 21

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; 2011, № 23, ст. 3263; № 31, ст. 4701) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818),

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.



2

2. Признать утратившим силу приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» (зарегистрирован Минюстом России 19 февраля 2010 г., регистрационный № 16456).

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Что же нового для операторов персональных данных несет данный документ?

1. Приказ ФСТЭК России от 5 февраля 2010 №58 официально утратил силу. Это было вполне ожидаемо в связи с выходом ПП1119, ведь последняя идеология СЗПДн (уровни защищенности) требовала внесения существенных правок в прежние требования к защите.

2. Изменился подход к выбору мер защиты. Процедура стала чуть сложнее, чем была до ПП1119, но теперь операторы ПДн могут отказываться от обязательных мер в угоду компенсирующим, учитывая их экономическую целесообразность.

3. Существенно изменился перечень мер защиты (по сравнению с подходом из ПП 781 и Приказа ФСТЭК №58). Сейчас стало 15 групп мер.
4. Появились дополнительные меры, направленные на снижение актуальных угроз к 1 и 2 типа (НДВ).
5. Появилось требование по регулярной (1 раз в 3 года) оценке эффективности реализованных мер (п.6).
6. Прописана возможность привлечения лицензиатов ФСТЭК для выполнения работ по обеспечению безопасности ПДн и (или) оценки эффективности реализованных мер (п.2, п.6).

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

11 февраля 2013 г. Москва № 17

Об утверждении Требований
о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196; 2011, № 15, ст. 2038; № 30, ст. 4600; 2012, № 31, ст. 4328) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818), **П Р И К А З Ы В А Ю:**

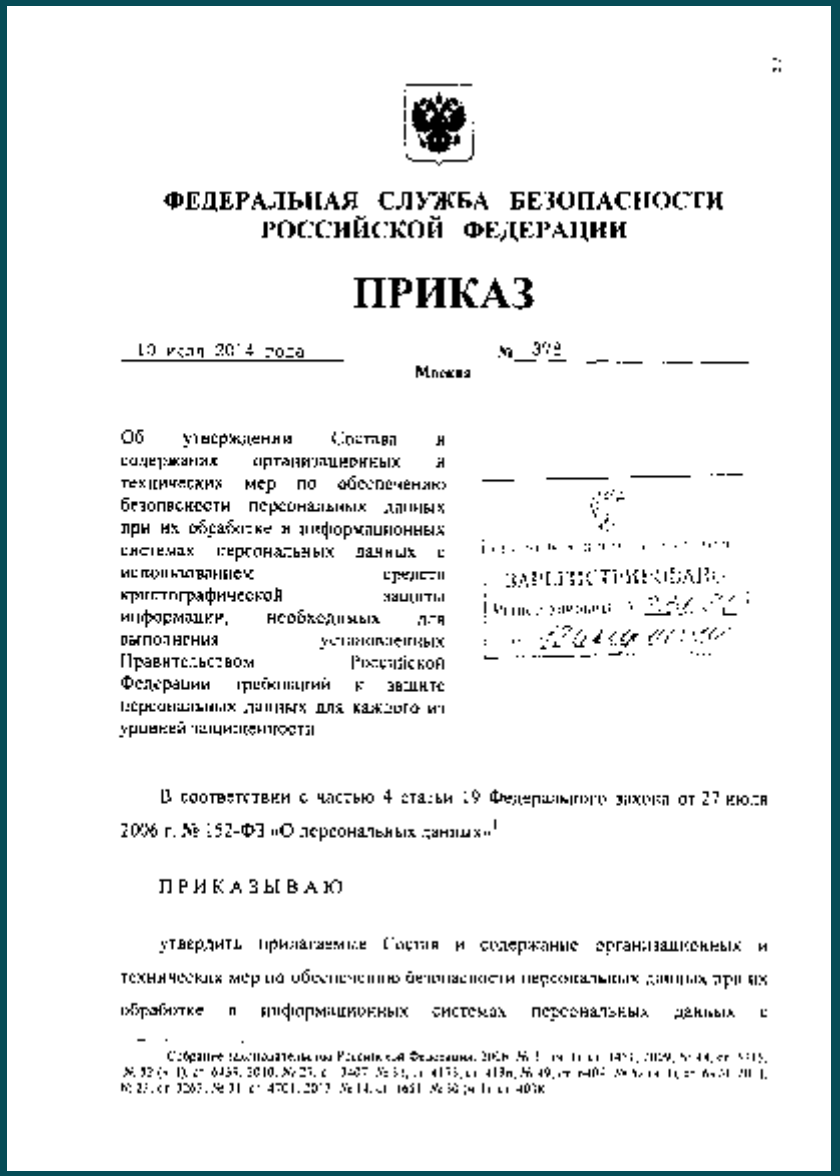
1. Утвердить прилагаемые Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

2. Установить, что указанные в пункте 1 настоящего приказа Требования применяются для защиты информации в государственных информационных системах с 1 сентября 2013 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Техническая защита персональных данных в информационных системах



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

19 июня 2013 года № 378

Москва

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[1]

ПРИКАЗЫВАЮ

утвердить прилагаемые Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с

Собрание законодательства Российской Федерации, 2006, № 1, ст. 10; 2010, № 31, ст. 4196; 2011, № 15, ст. 2038; № 30, ст. 4600; 2012, № 31, ст. 4328; 2013, № 14, ст. 1658; № 23, ст. 2870; № 27, ст. 3479; № 51, ст. 6683; 2014, № 23, ст. 2927.

1.Даны разъяснения (имеющие характер обязательных) положений ПП-1119. Например, что такое "организация режима обеспечения безопасности помещений", "сохранность персональных данных", "электронный журнал сообщений" и т.п.

2.Средства криптографической защиты персональных данных могут быть ТОЛЬКО сертифицированными.

3.Ограничено применение для защиты ПДн СКЗИ классом КС3 (!) и выше.

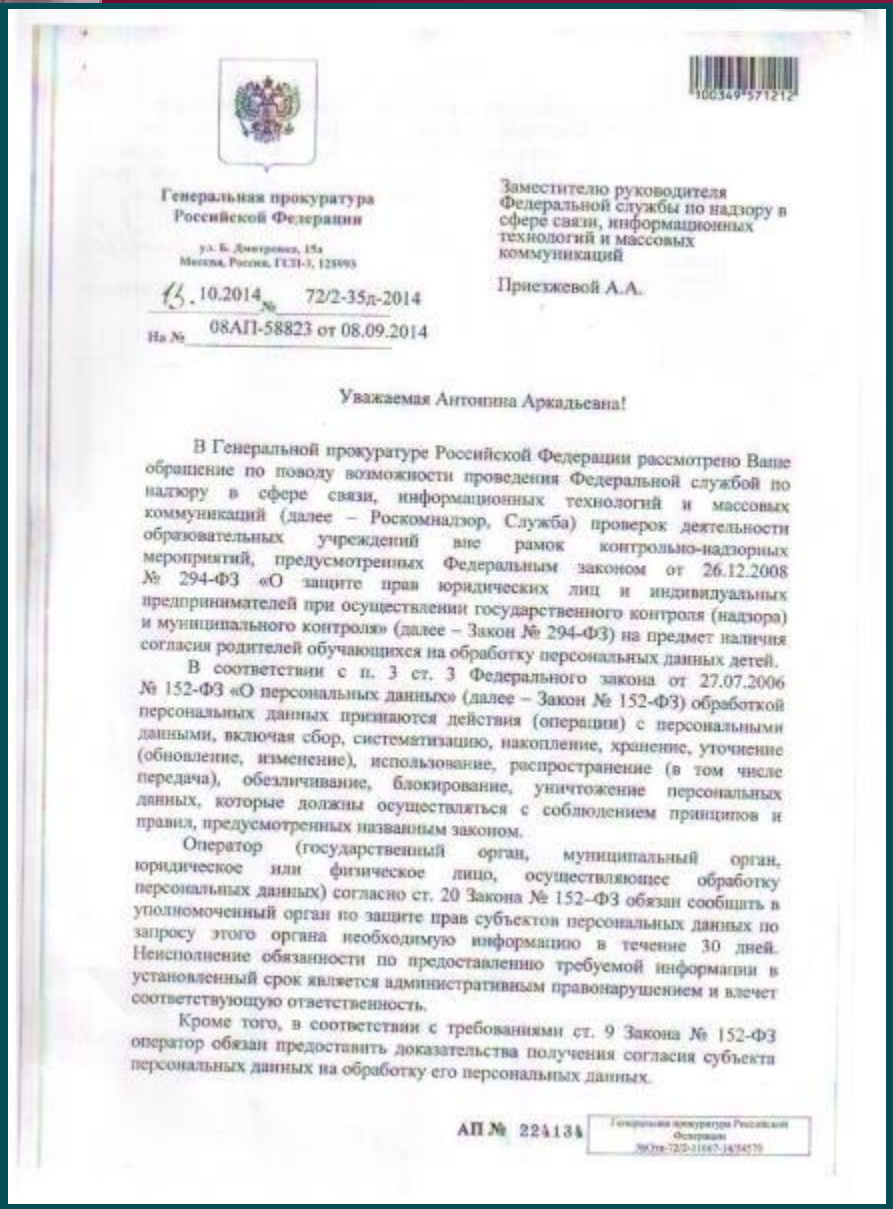
4.СКЗИ КВ2 применяются, когда могут быть использованы недекларированные возможности в прикладном ПО или у нарушителя есть исходные коды прикладного ПО.

5.СКЗИ КА1 применяются, когда могут быть использованы недекларированные возможности в системном ПО.

6.Все помещения, в которых ведется обработка ПДн, должны по окончании рабочего дня не просто закрываться, а опечатываться.

7.Все носители персональных данных должны учитываться поэкземплярно.

Требования законодательства



Генеральная прокуратура
Российской Федерации

ул. Б. Дмитровка, 15а
Москва, Россия, ГСП-3, 125993

13.10.2014 № 72/2-35д-2014

На № 08АП-58823 от 08.09.2014

Заместителю руководителя
Федеральной службы по надзору в
сфере связи, информационных
технологий и массовых
коммуникаций

Приезжевой А.А.

Уважаемая Антонина Аркадьевна!

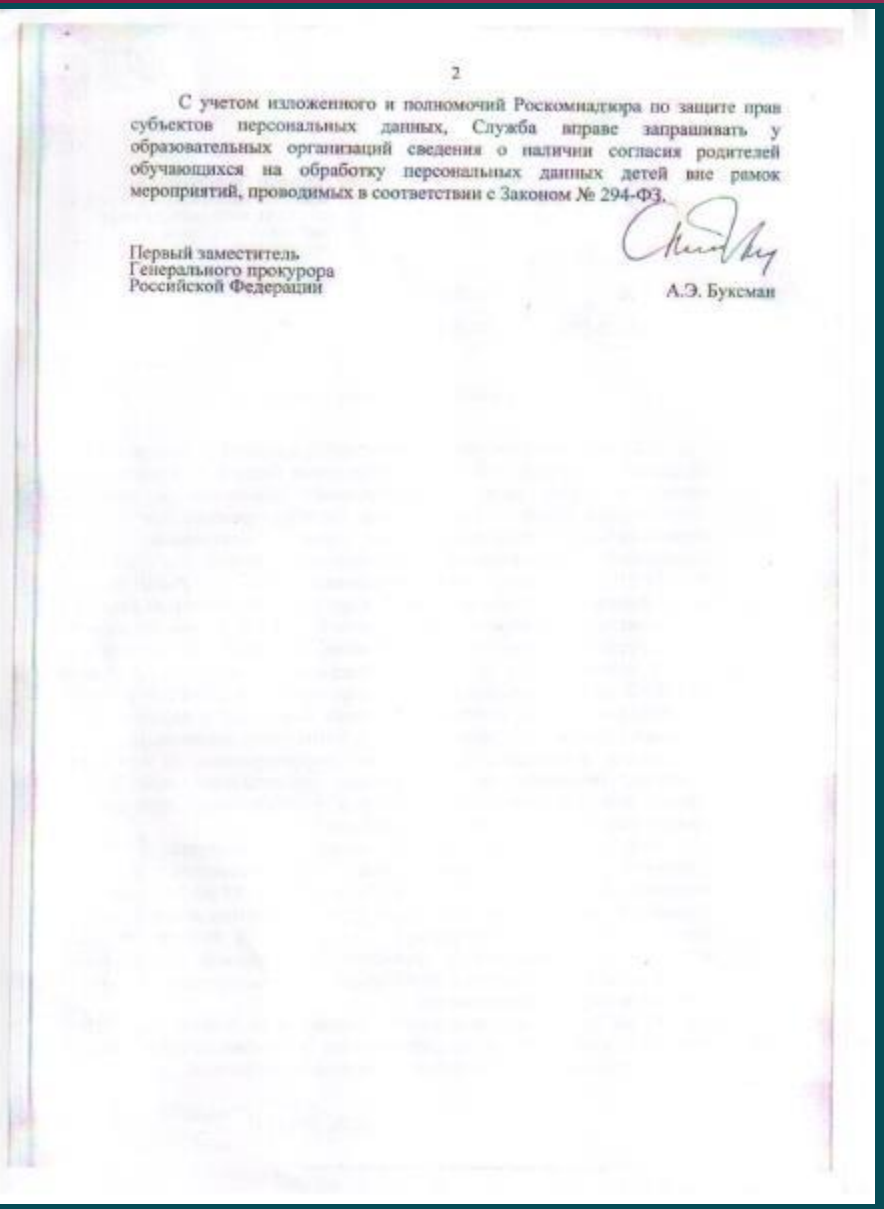
В Генеральной прокуратуре Российской Федерации рассмотрено Ваше обращение по поводу возможности проведения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор, Служба) проверок деятельности образовательных учреждений вне рамок контрольно-надзорных мероприятий, предусмотренных Федеральным законом от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (далее – Закон № 294-ФЗ) на предмет наличия согласия родителей обучающихся на обработку персональных данных детей.

В соответствии с п. 3 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ) обработкой персональных данных признаются действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных, которые должны осуществляться с соблюдением принципов и правил, предусмотренных названным законом.

Оператор (государственный орган, муниципальный орган, юридическое или физическое лицо, осуществляющее обработку персональных данных) согласно ст. 20 Закона № 152-ФЗ обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 дней. Неисполнение обязанности по предоставлению требуемой информации в установленный срок является административным правонарушением и влечет соответствующую ответственность.

Кроме того, в соответствии с требованиями ст. 9 Закона № 152-ФЗ оператор обязан предоставить доказательства получения согласия субъекта персональных данных на обработку его персональных данных.

АП № 224134



2

С учетом изложенного и полномочий Роскомнадзора по защите прав субъектов персональных данных, Служба вправе запрашивать у образовательных организаций сведения о наличии согласия родителей обучающихся на обработку персональных данных детей вне рамок мероприятий, проводимых в соответствии с Законом № 294-ФЗ.

Первый заместитель
Генерального прокурора
Российской Федерации

А.Э. Буксман