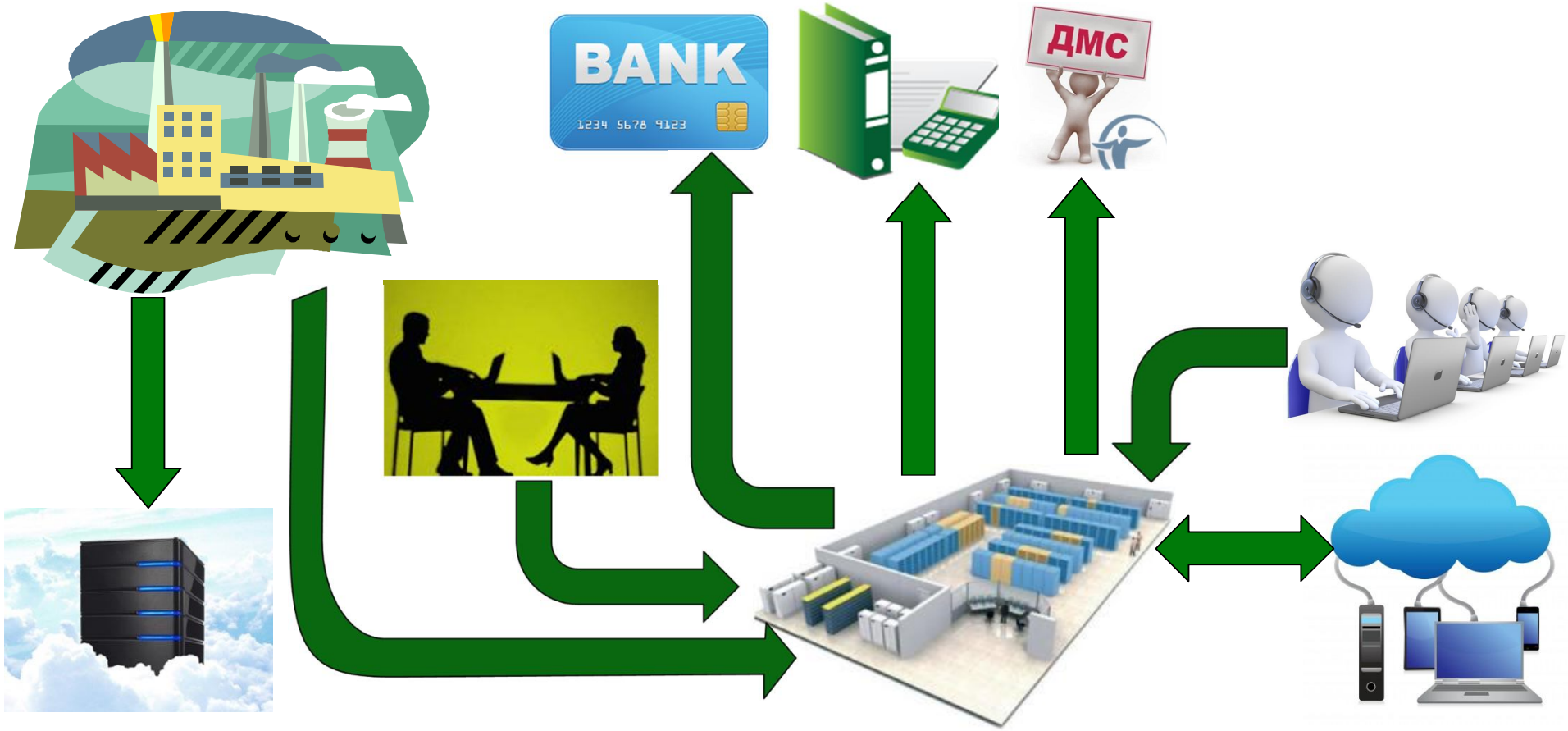
Персональные данные россиян в облаках и дата-центрах: границы допустимого

Емельянников
Михаил Юрьевич,
Управляющий партнер

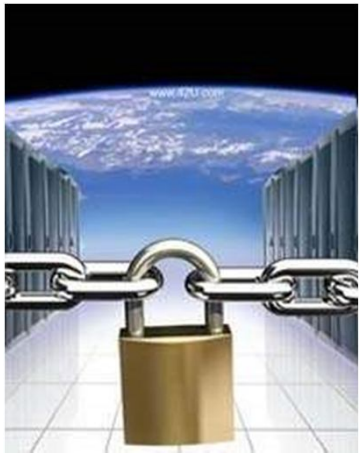
Мир с точки зрения ETS-108 и 152-ФЗ

Реальный мир (упрощенная версия)



Возникающие проблемы

- **доступ контрагентов (в том числе – персонала дата-центров и облачного провайдера)** – это передача персональных данных, поручение на их обработку или не то и не другое?
- **согласие субъекта на обработку** – надо ли получать и если да – то как?
- **моделирование угроз и построение** системы защиты – как выполнить закон?



Возникающие проблемы

Перенос обработки персональных данных в дата-центр или облако:

Это поручение другому лицу?

- Аренда программного обеспечения
- Аренда сервера
- Размещение оборудования клиента на территории провайдера

- SaaS
- PaaS
- IaaS

Идеальный случай

- Персонал провайдера не имеет доступа к обрабатываемым данным клиента и принимает меры по предотвращению физического доступа любых лиц к оборудованию и данным клиента (закреплено в договоре)
- Провайдер принял меры по обеспечению безопасности в дата-центре (облачной инфраструктуре) на сетевом уровне как минимум, соответствующие требованиям к защите персональных данных

Но есть проблема

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 …

Передача или поручение?

Передача без поручения

Поручение обработки

Нет передачи и поручения

Содержание поручения на обработку

В поручении оператора должны быть определены:

- перечень действий (операций) с персональными данными
- цели обработки персональных данных
- обязанность соблюдать конфиденциальность персональных данных
- обязанность обеспечивать безопасность персональных данных при их обработке
- требования к защите персональных данных в соответствии со ст.19 Федерального закона «О персональных данных»

А что же написано в статье 19

1) определить угрозы безопасности ПДн;

2) применять организационные и технические меры по обеспечению безопасности ПДн, необходимые для выполнения установленных требований к защите, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности ПДн;

3) применять прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;

4) оценить эффективность принимаемых мер до ввода в эксплуатацию ИСПДн;

5) учитывать машинные носители ПДн;

6) обеспечить обнаружение фактов НСД к ПДн;

7) обеспечить восстановление модифицированных или уничтоженных ПДн;

8) установить правила доступа к ПДн и обеспечить регистрацию и учет всех действий, совершаемых с ПДн в ИСПДн;

9) обеспечить контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

Получение согласия субъекта

- операторы и иные лица, получившие доступ к персональным данным, обязаны **не раскрывать третьим лицам** и не распространять персональные данные **без согласия субъекта** персональных данных, если иное не предусмотрено федеральным законом
- оператор **вправе поручить** обработку персональных данных другому лицу **с согласия субъекта** персональных данных, если иное не предусмотрено федеральным законом, **на основании** заключаемого с этим лицом **договора**

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

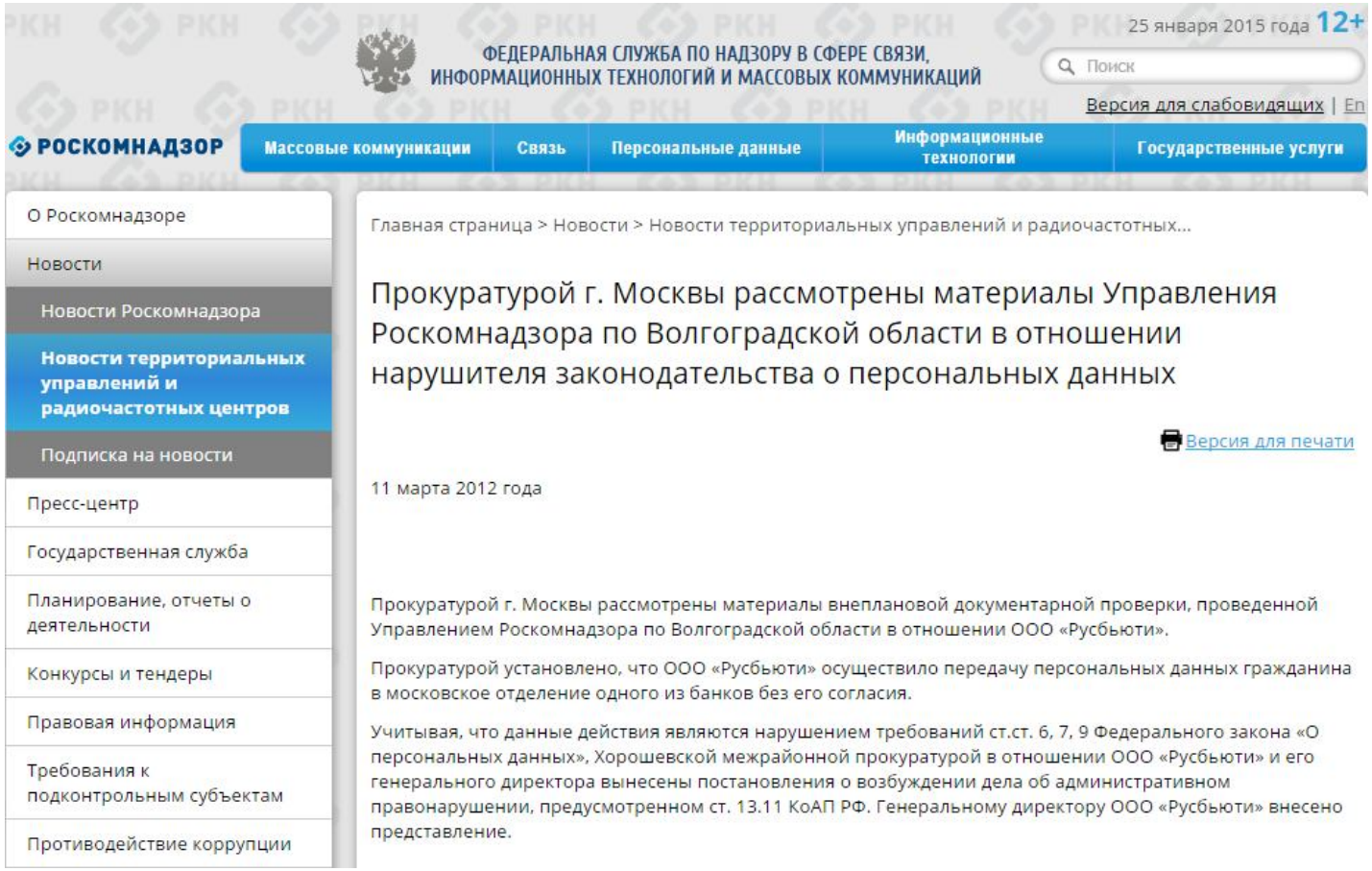
- не сообщать персональные данные работника третьей стороне **без письменного согласия** работника …;
- не сообщать персональные данные работника в коммерческих целях **без его письменного согласия;**

В то же время

Статья 6. Условия обработки персональных данных

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, **не обязано получать согласие субъекта** персональных данных на обработку его персональных данных.

Последствия могут быть серьезными



25 января 2015 года 12+

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

Поиск

Версия для слабовидящих | En

РОСКОМНАДЗОР

Массовые коммуникации | Связь | Персональные данные | Информационные технологии | Государственные услуги

- О Роскомнадзоре
- Новости
- Новости Роскомнадзора
- **Новости территориальных управлений и радиочастотных центров**
- Подписка на новости
- Пресс-центр
- Государственная служба
- Планирование, отчеты о деятельности
- Конкурсы и тендеры
- Правовая информация
- Требования к подконтрольным субъектам
- Противодействие коррупции

Главная страница > Новости > Новости территориальных управлений и радиочастотных...

Прокуратурой г. Москвы рассмотрены материалы Управления Роскомнадзора по Волгоградской области в отношении нарушителя законодательства о персональных данных

Версия для печати

11 марта 2012 года

Прокуратурой г. Москвы рассмотрены материалы внеплановой документарной проверки, проведенной Управлением Роскомнадзора по Волгоградской области в отношении ООО «Русбьюти».

Прокуратурой установлено, что ООО «Русбьюти» осуществило передачу персональных данных гражданина в московское отделение одного из банков без его согласия.

Учитывая, что данные действия являются нарушением требований ст.ст. 6, 7, 9 Федерального закона «О персональных данных», Хорошевской межрайонной прокуратурой в отношении ООО «Русбьюти» и его генерального директора вынесены постановления о возбуждении дела об административном правонарушении, предусмотренном ст. 13.11 КоАП РФ. Генеральному директору ООО «Русбьюти» внесено представление.

И даже очень серьезными

Персональные данные из психиатрической больницы попали в коммерческий банк

allNW.ru

Единый портал Северо-Запада России
и недвижимости Ленинградской

Опубликовано: 18:50 18.02.2014

Тихвинская городская прокуратура Ленинградской области направила материалы для возбуждения уголовного дела о нарушении неприкосновенности частной жизни.

Как сообщили корреспонденту 47news в пресс-службе прокуратуры Ленобласти, Тихвинская городская прокуратура провела проверку по обращению работников ГКУЗ ЛО "Тихвинская психиатрическая больница" о нарушении их прав.

Установлено, что в сентябре 2013 года и.о. главного врача государственного казенного учреждения Ленинградской области "Тихвинская психиатрическая больница" заключено соглашение с одним из коммерческих банков о предоставлении услуг по зачислению выплат на счета работников учреждения на основании поступивших платежных документов.

В результате руководством больницы без согласия работников медучреждения в указанный банк были переданы конфиденциальные сведения персонифицированного учета, чем были грубо нарушены права работников на неприкосновенность частной жизни.

Тихвинским городским прокурором направлены материалы проверки в следственные органы для решения вопроса об уголовном преследовании по ч. 1 ст. 137 УК РФ (нарушение неприкосновенности частной жизни).

Кое-кто об этом уже позаботился

- В случае, если оператор связи поручает обработку персданных абонента-гражданина третьему лицу **в целях** заключения и (или) **исполнения договора**, и (или) в целях **осуществления прав и законных интересов** оператора связи или абонента-гражданина, **согласие** абонента-гражданина **на это поручение**, в том числе **на передачу его персданных такому третьему лицу**, их **обработку таким третьим лицом** в соответствии с поручением оператора связи, **не требуется**.
- Фонд **вправе поручить** обработку персональных данных … организациям, которые, в соответствии с договором, осуществляют ведение пенсионных счетов, а также **иным организациям**, если это необходимо **для исполнения договора**, и **не обязан получать согласие субъектов** персональных данных **на поручение обработки** персональных данных всем этим третьим лицам

Кое-кто об этом уже позаботился

- **При привлечении** лицами, указанными в части 15 настоящей статьи, **представителей для осуществления расчетов** с нанимателями жилых помещений государственного и муниципального жилищных фондов, собственниками жилых помещений **и взимания платы за жилое помещение** и коммунальные услуги **согласие субъектов** персональных данных на передачу персональных данных таким представителям **не требуется**.

Защита персональных данных

Оператор при обработке персональных данных **обязан принимать** необходимые правовые, организационные и технические меры или **обеспечивать их принятие для защиты персональных данных** от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных **неправомерных действий** в отношении персональных данных.

Защита персональных данных

Постановление Правительства от 01.11.2012 № 1119

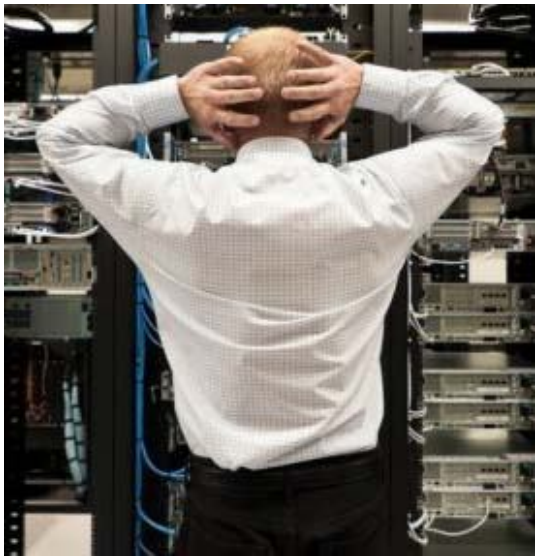
«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

3. Безопасность персональных данных при их обработке в информационной системе обеспечивает **оператор** этой системы, который обрабатывает персональные данные, или **лицо, осуществляющее обработку персональных данных** по поручению оператора на основании заключаемого с этим лицом договора.

Защита персональных данных

Оператор (**клиент**!) должен при передаче обработки персональных данных в дата-центр или облако **определить провайдеру**:

- тип актуальных угроз
- уровень защищенности персональных данных, который должен быть обеспечен провайдером



Типы актуальных угроз в Постановлении № 1119

Тип угроз	Характеристика
1	Связанные с наличием недокументированных (недекларированных) возможностей **в системном программном обеспечении**, используемом в ИСПДн
2	Связанные с наличием недокументированных (недекларированных) возможностей в **прикладном программном обеспечении**, используемом в информационной системе
3	**Не связанные** с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе

Выбор средств защиты

Выбор средств защиты информации для системы защиты ПДн **осуществляется оператором** в соответствии с нормативными правовыми актами, принятыми ФСБ и ФСТЭК во исполнение части 4 статьи 19 Федерального закона «О персональных данных».

Как оператору (!) выбрать средства защиты для дата-центра или облачной инфраструктуры?

Как обойти грабли?

Провайдеру:

- получить лицензии ФСТЭК и ФСБ
- определить тип актуальных угроз и максимальный уровень защищенности для дата-цента (предоставляемой облачной инфраструктуры)
- построить частную модель актуальных угроз для дата-цента (защищенного сегмента, облачной инфраструктуры)
- реализовать систему защиты на серверной стороне
- помочь клиенту с реализацией мер защиты на клиентской стороне

Что нас ждет 1 сентября 2015 года?

Внести в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» следующие изменения:

1) ст.18 дополнить частью 5 следующего содержания:

5. **При сборе персональных данных**, в том числе посредством ИТКС «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ с использованием баз данных, **находящихся на территории РФ**, за исключением случаев, указанных в пунктах 2, 3, 4, 8 ч.1 ст.6 настоящего ФЗ.

Когда ИСПДн можно будет хостить за рубежом

- **для достижения целей**, предусмотренных международным договором или **законом**, для осуществления и выполнения возложенных законодательством на оператора **функций, полномочий и обязанностей**
- для осуществления правосудия, **исполнения судебного акта**
- для исполнения полномочий ФОИВ, органов государственных внебюджетных фондов, исполнительных органов госвласти субъектов РФ, органов местного самоуправления и функций организаций, участвующих **в предоставлении государственных и муниципальных услуг**
- для осуществления **профессиональной деятельности журналиста** и (или) законной деятельности **СМИ,** научной, литературной или иной творческой деятельности

Как же так?

Федеральный закон от 31.12.2014 № 531-ФЗ «О внесении изменений в статьи 13 и 14 Федерального закона «Об информации, информационных технологиях и о защите информации» и Кодекс Российской Федерации об административных правонарушениях»

Технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, должны **размещаться на территории Российской Федерации**

С 1 июля 2015 года!

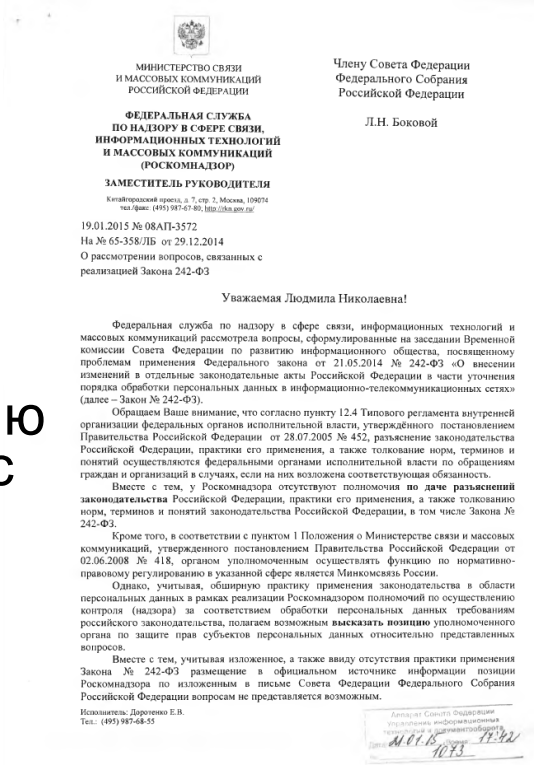
Трактовка Роскомнадзора

Ответ Роскомнадзора на запрос члена Совета Федерации Л.Н.Боковой от 9.01.2015

Формирование и актуализация баз персональных данных российских граждан должно осуществляться **на территории России**.

Законом допускаются передача персональных данных граждан России, содержащихся в базах данных, находящихся в РФ, в том числе на территорию иностранных государств, в порядке и в соответствии с условиями, определенными законодательством о персональных данных.

В отношении, передачи (распространения, предоставления доступа), обезличивания, блокирования, удаления, уничтожения персональных данных граждан России Законом № 242-ФЗ **не вносится никаких изменений**, касающихся обработки персональных данных указанными способами.



МИНИСТЕРСТВО СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО НАДЗОРУ В СФЕРЕ СВЯЗИ,
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И МАССОВЫХ КОММУНИКАЦИЙ
(РОСКОМНАДЗОР)**

ЗАМЕСТИТЕЛЬ РУКОВОДИТЕЛЯ

Китайгородский проезд, д. 7, стр. 2, Москва, 109074
тел./факс: (495) 987-67-80; http://rkn.gov.ru/

Члену Совета Федерации
Федерального Собрания
Российской Федерации

Л.Н. Боковой

19.01.2015 № 08АП-3572
На № 65-358/ЛБ от 29.12.2014
О рассмотрении вопросов, связанных с реализацией Закона 242-ФЗ

Уважаемая Людмила Николаевна!

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций рассмотрела вопросы, сформулированные на заседании Временной комиссии Совета Федерации по развитию информационного общества, посвященному проблемам применения Федерального закона от 21.05.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» (далее – Закон № 242-ФЗ).

Обращаем Ваше внимание, что согласно пункту 12.4 Типового регламента внутренней организации федеральных органов исполнительной власти, утверждённого постановлением Правительства Российской Федерации от 28.07.2005 № 452, разъяснение законодательства Российской Федерации, практики его применения, а также толкование норм, терминов и понятий осуществляются федеральными органами исполнительной власти по обращениям граждан и организаций в случаях, если на них возложена соответствующая обязанность.

Вместе с тем, у Роскомнадзора отсутствуют полномочия **по даче разъяснений законодательства** Российской Федерации, практики его применения, а также толкованию норм, терминов и понятий законодательства Российской Федерации, в том числе Закона № 242-ФЗ.

Кроме того, в соответствии с пунктом 1 Положения о Министерстве связи и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 02.06.2008 № 418, органом уполномоченным осуществлять функцию по нормативно-правовому регулированию в указанной сфере является Минкомсвязь России.

Однако, учитывая, обширную практику применения законодательства в области персональных данных в рамках реализации Роскомнадзором полномочий по осуществлению контроля (надзора) за соответствием обработки персональных данных требованиям российского законодательства, полагаем возможным **высказать позицию** уполномоченного органа по защите прав субъектов персональных данных относительно представленных вопросов.

Вместе с тем, учитывая изложенное, а также ввиду отсутствия практики применения Закона № 242-ФЗ размещение в официальном источнике информации позиции Роскомнадзора по изложенным в письме Совета Федерации Федерального Собрания Российской Федерации вопросам не представляется возможным.

Исполнитель: Дороненко Е.В.
Тел.: (495) 987-68-55

Спасибо!
Вопросы?

Емельянников
Михаил Юрьевич
Управляющий партнер
+7 (495) 761 5865
info@mezp.ru

Консалтинговое агентство
Емельянников, Попова и партнеры

Cloud & Mobility
CONFERENCE