



РОСКОМНАДЗОР

МЕРЫ, НАПРАВЛЕННЫЕ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОБЯЗАННОСТЕЙ, ПРЕДУСМОТРЕННЫХ ЗАКОНОДАТЕЛЬСТВОМ РФ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРАМИ, ЯВЛЯЮЩИМИСЯ

Суховерхова Екатерина Вадимовна
Начальник отдела по защите
персональных данных и надзору
за операторами информационных технологий

ВОРОНЕЖ, 2018



**УПОЛНОМОЧЕННЫЙ ОРГАН ПО
ЗАЩИТЕ ПРАВ СУБЪЕКТОВ
ПЕРСОНАЛЬНЫХ ДАННЫХ**



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

Полномочия территориальных органов Роскомнадзора в области персональных данных

- 1
 - Государственный контроль и надзор на подведомственной территории за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных
- 2
 - Ведение реестра операторов, осуществляющих обработку персональных данных
- 3
 - Уполномоченный орган (территориальное управление) по защите прав субъектов персональных данных

Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»



Персональные данные (ПДн) – это любая информация, относящаяся к прямо или косвенно определенному или определённом **физическому** лицу.

Оператор – государственный или муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами **организующие и/или осуществляющие** обработку ПДн, а так же **определяющие** цели обработки ПДн, состав ПДн, подлежащих обработке, действия, совершаемые с ПДн.

**Ст. 18.1 Федерального закона от 27.07.2006 №152-ФЗ
«О персональных данных»**

Ст. 18.1 Федерального закона от 27.07.2006 №152-ФЗ
«О персональных данных»

К таким мерам относятся:

- 1 Назначение ответственного за организацию обработки персональных данных оператором, являющимся юридическим лицом.



О НАЗНАЧЕНИИ ЛИЦА, ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Типовые ошибки

- ✘ Назначение ответственного за обеспечение безопасности персональных данных;
- ✘ Назначение нескольких лиц, ответственных за организацию обработку персональных данных;
- ✘ Назначение в качестве ответственного за организацию обработки персональных данных специалиста в узкопрофильной сфере деятельности

Обязанности ответственного за организацию обработки персональных данных

РОСКОМНАДЗОР

ст. 22.1 Федерального закона от 27.07.2006 №152-ФЗ
«О персональных данных»

- 1
 - осуществление внутреннего контроля за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.
- 2
 - доведение до сведения работников оператора положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- 3
 - организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.



Ст. 18.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»

2 Издание документов, определяющих политику в отношении обработки ПД, локальные акты по вопросам обработки



✓ Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных размещены на сайтах Роскомнадзора - rkn.gov.ru; 36.rkn.gov.ru.

- **Рекомендации**
- **Роскомнадзора по составлению документа, определяющего политику Оператора**
 - **Общие положения**
 - **Цели обработки персональных данных**
 - **Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов**
 - **Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных.**
 - **Правовые основания обработки персональных данных**
 - **Порядок и условия обработки персональных данных**

**Постановление
Правительства Российской
Федерации от 15.09.2008 г. №687
"Об утверждении Положения об
особенностях обработки
персональных данных,
осуществляемой без
использования средств
автоматизации"**

- - определение мест хранения материальных носителей,
- - установление перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- - раздельное хранение материальных носителей с персональными данными, обработка которых осуществляется в различных целях;
- - инструкции по заполнению типовых форм документов;
- - ведение журналов, содержащих персональные данные, необходимые для однократного пропуска субъекта ПДн на территорию оператора, должное

ТИПОВЫЕ НАРУШЕНИЯ

Отсутствие места (мест) хранения персональных данных (материальных носителей), перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ (П. 13 ПОСТАНОВЛЕНИЯ ПРАВИТЕЛЬСТВА РФ ОТ 15.09.2008 № 687)*

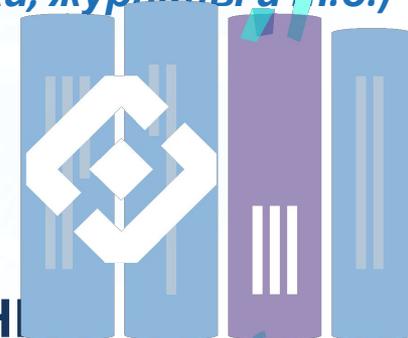
**распространяется исключительно на материальные носители персональных данных (дела, папки, журналы и т.д.)*

ПРИЗНАКИ НАРУШЕНИЯ:

ОТСУТСТВИЕ ДОКУМЕНТА, ПОДТВЕРЖДАЮЩЕГО

УТВЕРЖДЕНИЕ ОПЕРАТОРОМ ПЕРЕЧНЯ КОНКРЕТНЫХ

МЕСТ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ (МАТЕРИАЛЬНЫХ НОСИТЕЛЕЙ).



ПРИМЕР УСТРАНЕНИЯ.

ПРИКАЗ

об утверждении мест хранения материальных носителей персональных данных

В целях исполнения требований Федерального закона от 26.07.2006 № 152-ФЗ «О персональных данных» и Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» при обработке персональных данных в *(название)*

ПРИКАЗЫВАЮ:

1. Определить перечень мест хранения персональных данных обрабатываемых в *(название)*. (Приложение 1).
2. Контроль за исполнением настоящего приказа возложить на *ответственного за организацию обработки персональных данных Иванова В.В.*

(руководитель организации)

(подпись)

расшифровка подписи

« ____ » _____ 201_ г.

Приложение 1

ПЕРЕЧЕНЬ мест хранения персональных данных (ПДн), обрабатываемых в ____.

№ п/п	Подразделение	Место нахождения	Наименование документа, содержащего ПДн
1	Отдел кадров	Ул. Ленина 123, кабинет 1, шкаф/сейф	Личные дела сотрудников, трудовые книжки, приказы директора по личному составу.
2	Бухгалтерия	Ул. Ленина 123, кабинет 2	Индивидуальные сведения о трудовом стаже, заработке (вознаграждении), доходе и начисленных страховых взносах застрахованного лица; Расчетные (расчетно-платежные) ведомости; Листки нетрудоспособности
3	Библиотека	Ул. Ленина 123, кабинет 3	Учётные карточки и формуляры читателей библиотеки
4

ТИПОВЫЕ НАРУШЕНИЯ

Отсутствие места (мест) хранения персональных данных (материальных носителей), перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ (П. 13 ПОСТАНОВЛЕНИЯ ПРАВИТЕЛЬСТВА РФ ОТ 15.09.2008 № 687)*

ПРИЗНАКИ НАРУШЕНИЯ:

ОТСУТСТВИЕ ДОКУМЕНТА, ПОДТВЕРЖДАЮЩЕГО УТВЕРЖДЕНИЕ ПЕРЕЧНЯ ЛИЦ, ОСУЩЕСТВЛЯЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИБО ИМЕЮЩИХ К НИМ ДОСТУП.

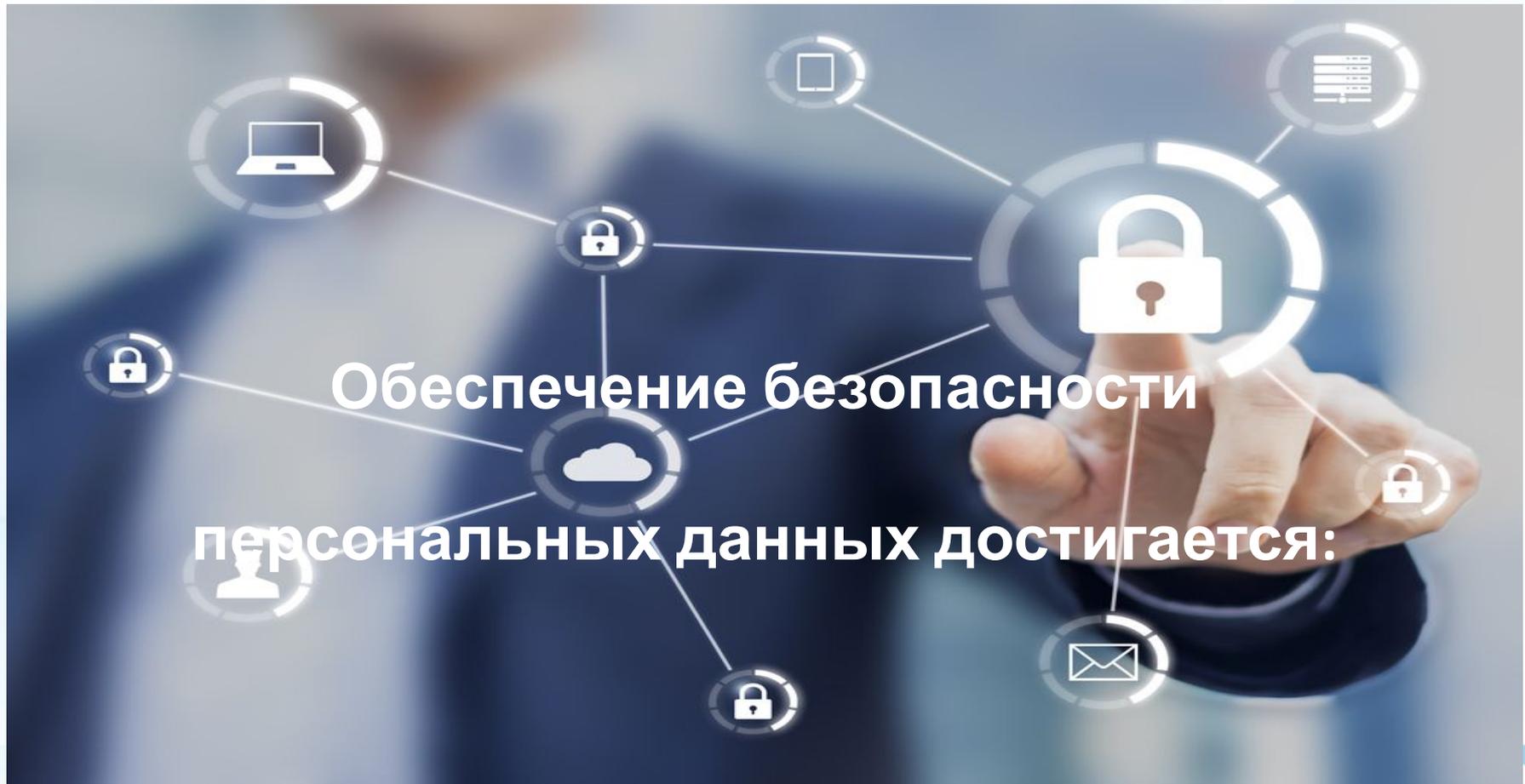
ПОРЯДОК УСТРАНЕНИЯ: ИЗДАНИЕ ПРИКАЗА ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ ЛИЦ, ОСУЩЕСТВЛЯЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИБО ИМЕЮЩИХ К НИМ ДОСТУП:

- ФИО,
- должности конкретных сотрудников,
- структурное подразделение

ИЛИ

- перечень должностей,
- структурное подразделение

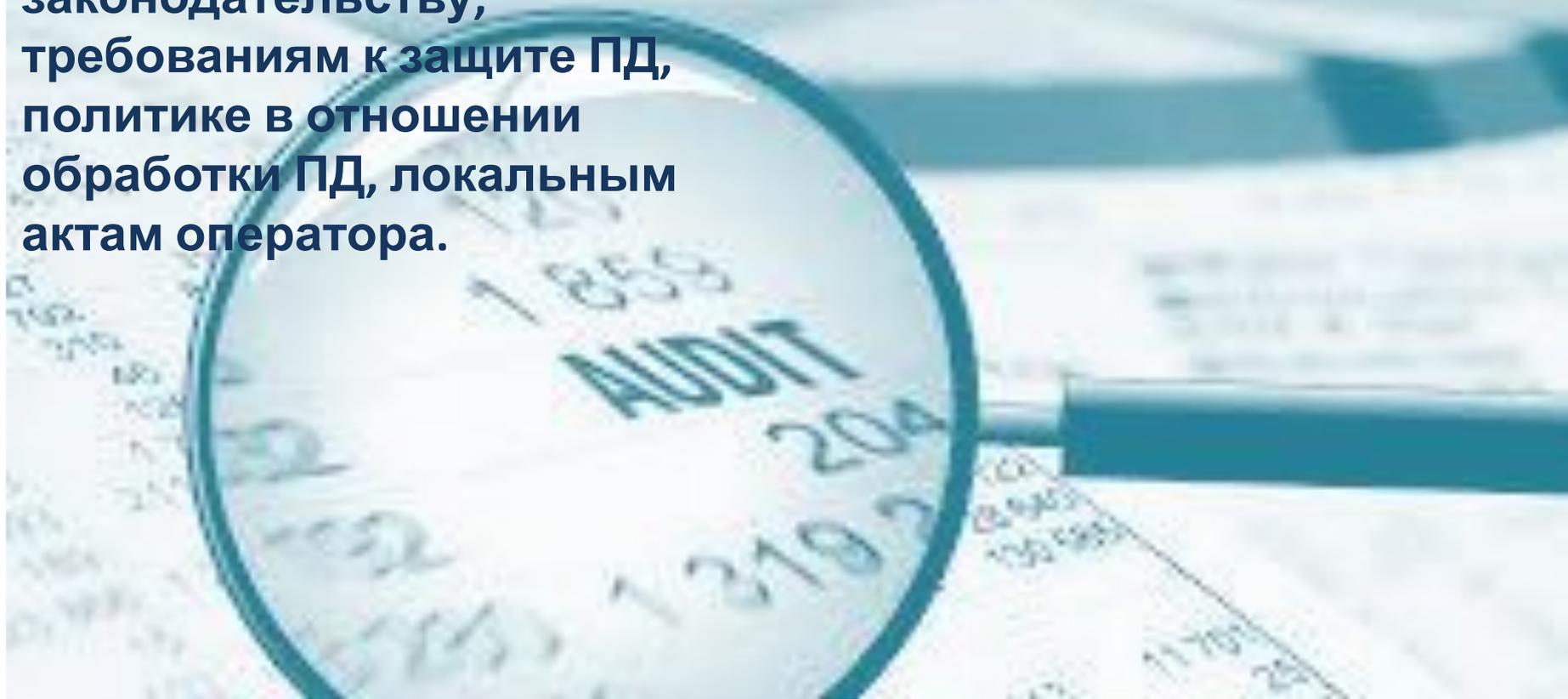
4 Применение правовых, организационных и технических мер по обеспечению безопасности ПД в соответствии со ст. 19 ФЗ «О персональных данных».



Ст. 19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»

- 1
 - определением угроз безопасности ПД при их обработке в ИСПДн;
- 2
 - применением организационных и технических мер по обеспечению безопасности ПД при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности ПД (Постановление Правительства от 01.2012г. № 1119)
- 3
 - применением средств защиты информации;
- 4
 - учетом машинных носителей ПДн;
- 5
 - обнаружением фактов несанкционированного доступа к ПДн и принятием мер;
- 6
 - восстановлением ПДн, уничтоженных вследствие несанкционированного доступа к ним;
- 7
 - установлением правил доступа к ПДн, обрабатываемым в ИСПДн, обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн.

5 Осуществление внутреннего контроля соответствия обработки ПД законодательству, требованиям к защите ПД, политике в отношении обработки ПД, локальным актам оператора.



ПРАВИЛА ВНУТРЕННЕГО КОНТРОЛЯ

утверждаются
актом
руководителя

- порядок осуществления внутреннего контроля
- методы осуществления внутреннего контроля
- основание
- порядок оформления результатов
- меры по устранению нарушений

При реализации внутреннего контроля оператор оценивает:

- порядок ознакомления лиц с локальными актами оператора;
- перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ;
- соблюдение правил доступа к персональным данным;
- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных;
- эффективность принимаемых мер по обеспечению безопасности в информационных системах персона
- целостности персональных данных



План осуществления мероприятий внутреннего контроля

- объект внутреннего контроля
- проверяемый период
- срок проведения мероприятия

7 знакомление работников оператора с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных (в том числе с требованиями к защите персональных данных) и (или) обучение указанных работников



ОЗНАКОМЛЕНИЕ РАБОТНИКОВ ОПЕРАТОРА С ЗАКОНОДАТЕЛЬСТВОМ В СФЕРЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ЛОКАЛЬНЫМИ АКТАМИ ОПЕРАТОРА В ДАННОЙ СФЕРЕ.

ТИПОВЫЕ ОШИБКИ.

-  Не проведение ознакомления сотрудников оператора с законодательством Российской Федерации в сфере персональных данных.
-  Отсутствие документального подтверждения проведения работы по ознакомлению сотрудников с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных.

Оператор обязан

- **Документы, определяющие политику Оператора в отношении обработки персональных данных.**
- **Опубликовать или иным образом обеспечить неограниченный доступ к ним.**
- **ОГВ и ОМСУ публикуют на официальном сайте в течение 10 дней после их утверждения.**



Статья 22 . Уведомление об обработке персональных данных



9 Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи

Общедоступный Реестр операторов в Роскомнадзоре персональных данных



The screenshot displays the website of the Federal Service for Supervision of Communications, Information Technologies, and Mass Communications (Roskomnadzor). The page is titled "ПОРТАЛ ПЕРСОНАЛЬНЫХ ДАННЫХ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ". A search bar is prominently featured with the text "Поиск по реестру" and "В настоящее время в реестре содержится информация о 363 192 операторах персональных данных". Below the search bar is a "Найти" button and a link to "Расширенный поиск". The "Новости и события" section lists several news items with dates and brief descriptions, such as seminars on data protection and conferences for education workers. A sidebar on the left contains navigation links like "Главная", "Об уполномоченном органе", and "Реестр операторов". The bottom of the page shows a Windows taskbar with various application icons and the system clock displaying 9:46 on 10.10.2016.

- ФОРМА УВЕДОМЛЕНИЯ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ;
- ФОРМА ИНФОРМАЦИОННОГО ПИСЬМА О ВНЕСЕНИИ ИЗМЕНЕНИЙ;
- РЕКОМЕНДАЦИИ ПО ЗАПОЛНЕНИЮ (приказ Роскомнадзора от 30.05.2017г. № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения».



Портал персональных
данных

pd.rkn.gov.ru



Сайт Управления
Роскомнадзора по
Воронежской области

36.rkn.gov.ru

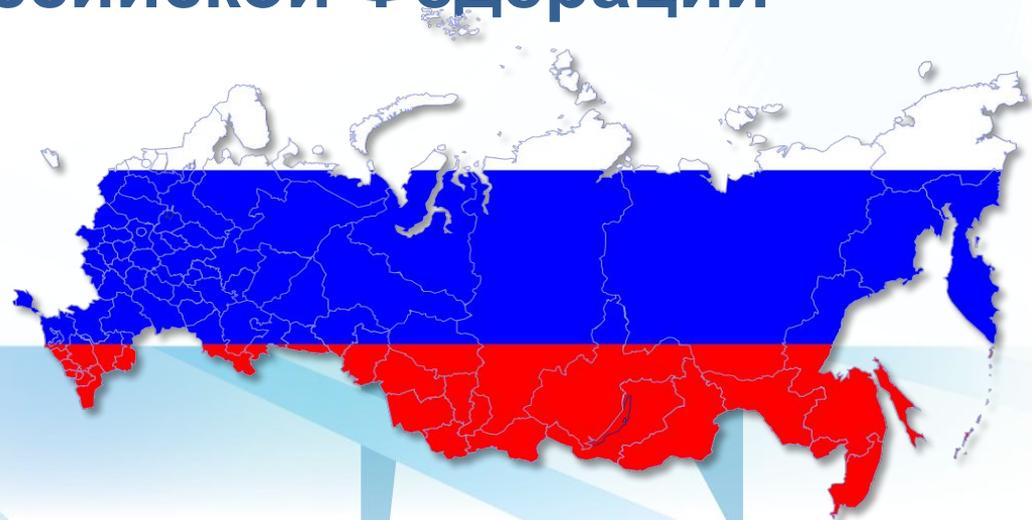
Федеральный закон от 21.07.2014 N 242-ФЗ **РОСКОМНАДЗОР**
"О внесении изменений в отдельные законодательные акты
Российской Федерации в части уточнения порядка обработки
персональных данных в информационно-телекоммуникационных
сетях"



НЕУВЕДОМЛЕНИЕ О МЕСТАХ РАСПОЛОЖЕНИЯ БАЗ
ПЕРСОНАЛЬНЫХ ДАННЫХ (с 1 сентября 2015 года)

сведения о месте нахождения базы
данных информации, содержащей
персональные данные граждан
Российской Федерации

размещение
БАЗ ДАННЫХ





Ч.3 СТ. 22 ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ!

ОБЯЗАННОСТЬ ОПЕРАТОРА ПО УВЕДОМЛЕНИЮ
УПОЛНОМОЧЕННОГО ОРГАНА (ИЗМЕНЕНИЕ СВЕДЕНИЙ В
РЕЕСТРЕ; ПРЕКРАЩЕНИЕ ОБРАБОТКИ)!

(ч. 7 ст. 22 Федерального закона «О персональных данных»)

ИНФОРМАЦИОННОЕ ПИСЬМО



10 рабочих дней

Обязанности оператора при обработке персональных данных в сети Интернет.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных

 **данных».**
Ч. 2 ст. 18.1 Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, **обязан опубликовать** в соответствующей сети **документ, определяющий его политику** в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также **обеспечить возможность доступа к указанному документу.**

 **Ст. 7** 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**



РОСКОМНАДЗОР

СПАСИБО ЗА ВНИМАНИЕ!

