

ПЕРСОНАЛЬНЫЕ ДАННЫЕ В 2026 ГОДУ

Изменения законодательства РФ, автоматический контроль Роскомнадзора
и сканер корпоративных сайтов «ИНАРИ»

30.05.2025

Кратный рост штрафов,
оборотная ответственность

01.09.2025

Согласие — отдельным
документом

01.09.2026

Идентификация доменов
.ru / .рф / .su через ЕСИА

ТЕМАТИКА

01

Что изменилось в 2025–2026

Новые обязанности операторов, ужесточение административной и уголовной ответственности, требования к согласию и локализации.

02

Как теперь проверяет Роскомнадзор

Сплошной автоматический мониторинг сайтов, риск-ориентированный отбор на проверки, предписания со сроком 10 рабочих дней.

03

Сканер сайтов «ИНАРИ»

Инструмент автоматизированной проверки корпоративных сайтов на соответствие законодательству о персональных данных.

04

Рекомендации по применению

Сценарии использования, событийные запуски и журнал сканирований, границы применимости.

КЛЮЧЕВЫЕ ДАТЫ: ОТ УЖЕСТОЧЕНИЯ К СПЛОШНОМУ КОНТРОЛЮ

11.12.2024**Ст. 272.1 УК РФ**

Введена 421-ФЗ: уголовная ответственность за незаконные использование, передачу, сбор и хранение компьютерной информации с ПДн, полученной незаконным путём.

30.05.2025**Новая шкала штрафов**

420-ФЗ: кратный рост санкций по ст. 13.11 КоАП РФ, оборотные штрафы за повторную утечку, отдельный состав за неуведомление об утечке.

01.07.2025**Локализация баз данных**

23-ФЗ: запрещены запись, хранение, уточнение и извлечение ПДн граждан РФ с использованием баз данных за пределами РФ (ч. 5 ст. 18).

01.09.2025**Согласие — отдельно**

156-ФЗ: согласие оформляется отдельно от иных документов, которые подписывает субъект. Явной переходной нормы для ранее выданных согласий нет.

01.03.2026**Реестр ЦОД**

244-ФЗ и ПП РФ № 1932: правила формирования и ведения реестра центров обработки данных, требования к включаемым площадкам.

01.09.2026**Идентификация доменов**

569-ФЗ: регистрация доменов в зонах .ru, .рф, .su — после идентификации через ЕСИА. Переходный период по решению КЦ — до 18.01.2027.

ЦЕНА НЕСООТВЕТСТВИЯ: СТ. 13.11 КОАП РФ

Суммы указаны для юридических лиц; для ИП по ряду составов ответственность совпадает.

Политика обработки ПДн не размещена в открытом доступе	30–60 тыс. ₽
Обработка ПДн без надлежащего согласия	300–700 тыс. ₽ · повторно до 1,5 млн ₽
Неуведомление Роскомнадзора о начале обработки ПДн	100–300 тыс. ₽
Нарушение требований локализации баз данных	1–6 млн ₽ · повторно 6–18 млн ₽
Неуведомление Роскомнадзора об утечке ПДн	1–3 млн ₽
Утечка ПДн	3–20 млн ₽ по объёму и категории данных
Повторная утечка от 1 000 субъектов (для биометрии — минимум 25 млн ₽)	1–3 % годовой выручки · 20–500 млн ₽

Источник: ст. 13.11 КоАП РФ в редакции ФЗ от 30.11.2024 № 420-ФЗ (действует с 30.05.2025).

СОГЛАСИЕ ОФОРМЛЯЕТСЯ ОТДЕЛЬНЫМ ДОКУМЕНТОМ

ЧТО ИЗМЕНИЛОСЬ В ЗАКОНЕ

- Согласие оформляется отдельно от иных документов, которые подписывает субъект (ст. 9 152-ФЗ в редакции 156-ФЗ)
- Его нельзя «вшивать» в договор, оферту или пользовательское соглашение
- Для исполнения договора с субъектом согласие не нужно — это отдельное основание (п. 5 ч. 1 ст. 6 152-ФЗ)
- Явной переходной нормы нет: «вшитые» в договоры согласия лучше переоформить отдельно

ПРАКТИКА ДЛЯ САЙТА (РЕКОМЕНДАЦИИ)

- Чекбокс согласия пустой по умолчанию — предустановленная галочка не подтверждает волю субъекта
- Рядом с чекбоксом — прямая ссылка на полный текст согласия, открывающийся отдельной страницей
- Отдельная галочка на каждую цель: обработка заявки, рассылка, передача партнёрам
- Факт согласия фиксируется в логах: IP-адрес, время, версия текста
- Собираются только те данные, которые необходимы для заявленной цели

Штраф за обработку без надлежащего согласия — 300–700 тыс. Р, при повторном нарушении до 1,5 млн Р (ч. 2 ст. 13.11 КоАП РФ).

ГДЕ ФИЗИЧЕСКИ НАХОДЯТСЯ ДАННЫЕ ВАШИХ ПОЛЬЗОВАТЕЛЕЙ

ПРАВИЛО

Запись, систематизация, накопление, хранение, уточнение и извлечение ПДн граждан РФ с использованием баз данных за пределами РФ не допускаются, кроме случаев, предусмотренных законом (ч. 5 ст. 18 152-ФЗ).

ТИПИЧНЫЕ НАРУШЕНИЯ

Первичный сбор сразу на иностранный сервер; зарубежный хостинг, почта и CRM; зарубежные системы аналитики без уведомления о трансграничной передаче.

ЧТО ДЕЛАТЬ

Локализовать сбор и все операции из ч. 5 ст. 18; трансграничную передачу вести только по ст. 12 152-ФЗ с уведомлением РКН; получить от провайдера подтверждение размещения серверов в РФ.

Нарушение требований локализации — штраф 1–6 млн ₽, при повторном нарушении 6–18 млн ₽ (ч. 8–9 ст. 13.11 КоАП). Передача данных в Google Analytics, Meta Pixel и подобные сервисы без уведомления РКН — отдельное нарушение требований ст. 12 152-ФЗ, а не локализации.

ЧТО ДОБАВИЛ 2026 ГОД

01.03.2026

Реестр ЦОД

ПП РФ от 28.11.2025 № 1932 в развитие 244-ФЗ: правила формирования и ведения реестра центров обработки данных в РФ и требования к включаемым площадкам. Для операторов ПДн — ориентир при выборе площадки.

01.09.2026

Идентификация доменов

ФЗ от 29.12.2025 № 569-ФЗ: домены .ru, .rf и .su регистрируются только после идентификации администратора через ЕСИА. Решение КЦ № 05-42: переходный период до 18.01.2027.

26.07.2026

Адекватная защита ПДн

Подписан закон: при включении страны в перечень с адекватной защитой ПДн оценивается и практика применения законодательства; привязка к участию в Конвенции исключена.

НА РАССМОТРЕНИИ И В ПЛАНАХ — В СИЛУ НЕ ВСТУПИЛО

Определение допустимого объема собираемых ПДн для хозяйствующих субъектов (план мероприятий по распоряжению Правительства РФ № 2207-р, ориентир — IV квартал 2026 г.) · запрет иностранных корпоративных облачных сервисов для крупного бизнеса (предложение Минцифры, ориентир — 01.09.2027).

СТ. 13.1 152-ФЗ И ЕИП НСУД

ЧТО РЕГУЛИРУЕТСЯ

Статья 13.1, введённая ФЗ от 08.08.2024 № 233-ФЗ, устанавливает особенности обработки обезличенных персональных данных при формировании составов данных и предоставлении доступа к ним.

Практический смысл для оператора: по требованию Минцифры России данные обезличиваются установленными методами и передаются в Единую информационную платформу национальной системы управления данными (ЕИП НСУД).

ПОДЗАКОННАЯ БАЗА (ДЕЙСТВУЕТ С 01.09.2025)

- ПП РФ № 538 — перечень случаев формирования составов обезличенных данных
- ПП РФ № 702 — проверка соответствия пользователей ЕИП НСУД
- ПП РФ № 961 и № 966 — правила формирования составов, доступа и взаимодействия с Минцифры
- ПП РФ № 1154 — требования к обезличиванию, методы и правила обезличивания
- Приказ Роскомнадзора № 140 — требования и методы обезличивания, заменил приказ № 996

Для большинства коммерческих операторов это пока «спящее» требование, но оно становится обязательным в момент получения запроса от Минцифры — процессы обезличивания стоит подготовить заранее.

КАК СЕЙЧАС ПРОВЕРЯЕТ РОСКОМНАДЗОР

1

Автоматический скан

Бот РКН автоматически анализирует сайты: код страниц, скрипты, файлы cookie, формы сбора данных и внешние подключения.

2

Проверка инспектором

Материалы уходят живому инспектору: сверяются сведения из уведомления оператора, документы на сайте и фактическое поведение кода.

3

Предписание

При подтверждении нарушения направляется требование об устранении. Срок задаёт РКН; по практике — от 10 дней.

4

Санкция

РКН составляет протокол по ст. 13.11 КоАП, штраф назначает суд. Внеплановая проверка — при основаниях по 248-ФЗ и с согласованием прокуратуры.

Отбор операторов на проверку ведётся по риск-ориентированной модели: категория риска определяет частоту плановых контрольных мероприятий. Положение о контроле — постановление Правительства РФ от 29.06.2021 № 1046.

ГДЕ ЧАЩЕ ВСЕГО ЛОМАЕТСЯ КОРПОРАТИВНЫЙ САЙТ

Шаблонная политика

Скопированный из интернета документ не отражает реальные процессы; при проверке признаётся ненадлежащим.

Предустановленный чекбокс

Галочка, проставленная по умолчанию, не является действием субъекта — согласие не считается полученным.

Одна галочка на все цели

Обработка заявки, рассылка и передача партнёрам требуют отдельных согласий.

Cookie-баннер без отказа

Нет выбора категорий и нет блокировки аналитических скриптов до получения согласия.

Зарубежные трекеры и хостинг

Скрытая передача данных в иностранные системы аналитики, CRM и почтовые сервисы.

Расхождения с реестром

Компании нет в реестре операторов либо данные юрлица в реестре не совпадают с владельцем сайта.

СКАНЕР САЙТОВ «ИНАРИ»

ЗАЧЕМ

Сайт — самый динамичный элемент цифровой инфраструктуры компании. Формы, аналитика, cookie-механизмы и другие изменения часто внедряются без согласования с юридической службой и ИБ.

В результате нарушения выявляются уже в ходе проверки регулятора — когда исправлять их поздно и дорого.

ЧТО ЭТО

«ИНАРИ» — инструмент автоматизированной проверки корпоративных сайтов на соответствие требованиям законодательства о персональных данных.

Проверка выполняется по внешнему наблюдаемому контуру сайта: публичные документы, формы, cookie-механизмы, внешние подключения и запись компании в реестре Роскомнадзора.

Логика продукта проста: находить те же несоответствия, что ищет автоматический мониторинг регулятора, — но раньше него.

ЧТО ПРОВЕРЯЕТ «ИНАРИ»

1

Наличие компании в реестре Роскомнадзора как лица, осуществляющего обработку ПДн, — включая проверку по ИНН и актуальность записи

2

Наличие и корректность политики обработки персональных данных

3

Корректность форм сбора данных и текстов согласия

4

Наличие cookie-механизма и реальной возможности отказаться от обработки

5

Использование Google Analytics и отражение трансграничной передачи данных

6

Размещение сайта на сервере с учётом требований локализации данных

СТРУКТУРИРОВАННЫЙ ОТЧЕТ

НАРУШЕНИЕ

Прямое несоответствие требованиям законодательства. Требуется немедленного устранения — именно эти пункты становятся основанием для предписания или штрафа.

НЕКОРРЕКТНОСТЬ

Расхождения и потенциально спорные формулировки. Формально требование исполнено, но текст или реализация могут быть оспорены регулятором.

РЕГУЛЯТОРНЫЙ РИСК

Факторы, требующие дополнительной оценки: неоднозначные сценарии обработки, внешние сервисы, спорные основания обработки.

Практическая ценность формата: результат сразу раскладывается на задачи для разных команд. Нарушения уходят юристам и подрядчику по сайту, некорректности — юридической службе, регуляторные риски — в план работ ИБ. Отчёт можно использовать как повестку встречи, а не как справочный документ.

ЧЕТЫРЕ РАБОЧИХ СЦЕНАРИЯ

1 Разовый аудит перед проверкой

Быстрый срез по всем доменам компании до того, как несоответствия найдёт автоматический мониторинг регулятора. Даёт понятный список того, что нужно закрыть в первую очередь.

2 Регулярный мониторинг

Контроль после каждого релиза сайта, подключения новой формы, виджета, чата или системы аналитики. Именно эти изменения чаще всего вносятся без согласования с ИБ и юристами.

3 Группа компаний и множество доменов

Единая картина по всем сайтам холдинга, включая промо-лендинги, региональные и продуктовые сайты, которые обычно выпадают из периметра контроля.

4 Контроль подрядчиков

Проверка сайтов, которые ведут внешние агентства, и приёмка работ по устранению: отчёт сканера служит объективным критерием готовности.

Событийные запуски

Внеплановый скан после релиза сайта, подключения формы, аналитики, чата, CDN или смены хостинга.

Журнал сканирований

Хранить отчёты и подтверждения устранения как доказательство внутреннего контроля (ст. 18.1, 19 152-ФЗ).

ЧТО СКАНЕР ЗАКРЫВАЕТ, А ЧТО ОСТАЁТСЯ ВНЕ ЕГО ПЕРИМЕТРА

ЗАКРЫВАЕТ

- Публичные документы сайта: политика, тексты согласий
- Формы сбора данных и механику чекбоксов
- Cookie-механизм и возможность отказа
- Внешние подключения и системы аналитики
- Запись компании в реестре операторов Роскомнадзора
- Признаки размещения сайта с учётом локализации

НЕ ЗАМЕНЯЕТ

- Юридическую экспертизу формулировок документов
- Аудит внутренних процессов обработки и ИСПДн
- Модель угроз и определение уровня защищённости (ПП № 1119)
- Проверку фактического места хранения данных в CRM и бэкенде
- Анализ договоров поручения обработки с подрядчиками
- Кадровый и бумажный контур обработки ПДн

Сканер снимает регуляторный риск цифрового периметра. Полное соответствие 152-ФЗ требует работ по документам, процессам и инфраструктуре.

ОТ СКАНИРОВАНИЯ — К УСТОЙЧИВОМУ СООТВЕТСТВИЮ

1

Сканирование «ИНАРИ»

Фиксация нарушений,
некорректностей и
регуляторных рисков по всем
сайтам компании.

2

Устранение

Политика, тексты согласий,
чекбоксы, cookie-баннер, отказ
от зарубежных трекеров,
локализация.

3

Аудит процессов обработки ПДн

Внутренние документы,
перечень ИСПДн, модель угроз,
уровень защищённости,
договоры поручения.

4

Консалтинг

Поддержание соответствия,
сопровождение проверок
регулятора, организация
процессов обезличивания ПДн.

ИС Лаб закрывает весь цикл: собственный продукт для контроля цифрового периметра, аудит ИТ/ИБ-процессов, полный цикл исполнения требований 152-ФЗ и 187-ФЗ, а также сервисная модель — vCISO и аутсорсинг информационной безопасности.

Попробуйте тестовую проверку бесплатно – зарегистрируйтесь на inari.islg.ru

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«ЛАБОРАТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

КОНТАКТЫ

Проверим ваш цифровой периметр так, как это делает регулятор, — и поможем закрыть найденное до предписания.

ПОЧТА

info@islg.ru

ТЕЛЕФОН

8-495-723-72-75

TELEGRAM

@information_security_lab

САЙТ И СКАНЕР

islg.ru · inari.islg.ru

ЛИЦЕНЗИИ

ФСТЭК России
Лицензия № Л024-00107-00/00583070

ФСБ России
Лицензия № Л051-00105-00/00011599

РЕКВИЗИТЫ

ООО «ИС Лаб»
ИНН 7725831654 · ОГРН 1147746651997
г. Москва, ул. Большая Почтовая, д. 26В, стр. 1