

28.10.2026

ГЛАВНЫЕ СОБЫТИЯ В СФЕРЕ РЕГУЛИРОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ИТОГАМ ЛЕТА 2026 ГОДА

Уважаемые коллеги,

Настоящий обзор посвящен ключевым событиям в сфере регулирования персональных данных, которые произошли летом 2026 года и на которые мы бы хотели обратить Ваше внимание:

Ужесточение трансграничной передачи персональных данных

26.07.2026 вступил в силу [Федеральный закон № 265-ФЗ](#) «О внесении изменений в статью 12 Федерального закона «О персональных данных» и отдельные законодательные акты Российской Федерации» (далее – «Федеральный закон № 265-ФЗ»), целью которого стало усиление защиты персональных данных при их передаче за границу.

Что поменялось?

Согласно ранее действовавшей редакции статьи 12 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» Роскомнадзором утверждался перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, (далее – «Перечень») в который включались:

- **государства, являющиеся сторонами Конвенции Совета Европы** о защите физических лиц при автоматизированной обработке персональных данных (далее – «Конвенция»), а также
- **иностранное государство, не являющееся сторонами Конвенции, при условии соответствия положениям Конвенции** действующих в соответствующем государстве норм права и применяемых мер по обеспечению конфиденциальности и безопасности персональных данных при их обработке.

В настоящее время в указанный Перечень должны быть включены **только государства, в которых правовое регулирование** в области персональных данных и **применяемые указанными государствами меры** по соблюдению основополагающих принципов защиты, обеспечению конфиденциальности и безопасности персональных данных при их обработке **соответствуют положениям Конвенции**.

Таким образом, теперь один лишь факт того, что иностранное государство является стороной Конвенции, не является достаточным для включения этого государства в Перечень. Значение имеют содержание законодательства соответствующего

иностранного государства, **фактически применяемые меры** по защите персональных данных, а также обеспечение их конфиденциальности и безопасности.

Утвержден ли в настоящее время Перечень?

В настоящее время все еще действует [Перечень, утвержденный Приказом Роскомнадзора от 05.08.2022 № 128](#).

Однако Роскомнадзором уже подготовлен [проект нового Перечня](#), в котором сохранены все государства, включенные в действующий Перечень, **за исключением Украины**. Кроме того, вместо деления государств на участников и неучастников Конвенции установлен единый алфавитный список.

Что это значит для бизнеса?

Если ваша организация осуществляет трансграничную передачу данных (например, использует зарубежные облачные сервисы, отправляет данные иностранных клиентов или сотрудников в головные офисы за границу), вам необходимо строго отслеживать обновляемый Перечень Роскомнадзора. Изменение статуса любой страны потребует незамедлительной приостановки передачи персональных данных и подачи нового уведомления в адрес ведомства.

Итоги дня открытых дверей Роскомнадзора

14.08.2026 Роскомнадзор провел масштабный [День открытых дверей](#), на котором подвел итоги проверок за 2025 г. и первую половину 2026 г. Главный вывод встречи – ведомство полностью перешло на **риск-ориентированный подход**: вместо массовых выездных инспекций упор делается на автоматический дистанционный аудит сайтов.

Вот ключевые итоги, о которых нужно знать бизнесу:

- **Повторные утечки сведены к минимуму.** Заместитель руководителя Роскомнадзора Милош Вагнер [официально заявил](#), что за последние полтора года ведомство **не зафиксировало ни одного повторного инцидента** утечки персональных данных у компаний, которые уже привлекались к ответственности. Бизнес стал серьезнее относиться к безопасности на фоне обсуждения крупных оборотных штрафов.
- **Автоматизация надзора (дистанционный мониторинг).** Роскомнадзор проверил почти 160 тыс. интернет-ресурсов в зонах *.ru*, *.рф* и *.su*. Проверки проходят незаметно для компаний: автоматизированные системы непрерывно сканируют формы сбора данных на сайтах. Алгоритмы ищут типичные нарушения: отсутствие политики конфиденциальности, предустановленные галочки согласия, сбор данных без уведомления Роскомнадзора или скрытые скрипты. При обнаружении нарушений оператор сначала получает официальное письмо с требованием всё исправить, и только при игнорировании выносятся предписание или штраф.

4 главных принципа комплаенса от регулятора:

- **Осознанный сбор данных.** Нельзя собирать информацию «про запас». Компании обязаны четко определять конкретную цель для каждого типа данных. Сбор избыточных анкетных строк без обоснованной деловой цели – это гарантированное нарушение.
- **Контроль передачи данных.** Бизнес должен точно знать весь путь данных: кому, как и зачем они передаются (включая подрядчиков, облачные сервисы и аналитические платформы). Любая передача должна быть юридически обоснована.
- **Отказ от «универсальных» согласий.** Согласие не должно использоваться как универсальное основание для любой обработки: в ряде случаев обработка может осуществляться на основании договора или требований закона. Избыточные, гигантские согласия «обо всем сразу» Роскомнадзор считает нарушением.
- **Управление жизненным циклом.** Данные нельзя хранить вечно. Необходимо прописать жесткие сроки хранения и, главное, внедрить процедуру гарантированного уничтожения персональных данных (с составлением актов), как только цель их сбора достигнута.

Будем рады ответить на любые вопросы и проверить сайт Вашей компании на соответствие новым требованиям 2026 года. Также мы готовы провести аудит движения персональных данных в Ваших ИТ-системах, включая проверку и легализацию трансграничных потоков.

Ваши контактные лица по этой теме:

Мария Матросова, партнер, руководитель проектов

М: maria.matrossowa@swilar.ru

Юлия Белоконь, заместитель руководителя проектов

М: yulia.belokon@swilar.ru