



Руководителю

Исх. № 04 от 20 марта 2026 года

Федеральным законом от 30.11.2024 № 420-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях" усилена ответственность за нарушения в сфере обработки персональных данных, увеличены штрафы за «утечки» персональных данных.  
<http://publication.pravo.gov.ru/document/0001202411300011?index=15>.

Мы подготовили рекомендации по порядку действий для выполнения новых требований законодательства и возможностям снижения рисков. Рассмотрим случаи, когда к ответственности привлекают только руководителя, а когда только организацию. Проработаем все 16 документов по персональным данным, какие подпадают под штрафы по обработке персональных данных и т.д.:

## 14 - 16 апреля 2026 года ДИСТАНЦИОННЫЙ ПРАКТИЧЕСКИЙ КУРС

### «ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ПРАКТИЧЕСКОЕ ПОГРУЖЕНИЕ» для ответственных за организацию обработки персональных данных с учетом изменений законодательства и требований РОСКОНАДЗОРА в 2026 году

**Цель обучения:** формирование компетенций у ответственных за организацию обработки персональных данных, специалистов отделов кадров, HR-подразделений, бухгалтеров, специалистов по защите информации в сфере обработки персональных данных согласно требованиям законодательства и Роскомнадзора.

**Приглашаем:** руководителей, заместителей руководителя, ответственных за организацию обработки персональных данных, ответственных за безопасность персональных данных в ИСПДн, специалистов отделов, непосредственно обрабатывающих персональные данные, в том числе специалистов организаций, обрабатывающих персональные данные по поручению операторов.

#### День 1 (14.04.26): Обработка персональных данных

1. Новые требования законодательства в области обработки персональных данных (далее – ПДн).
2. Первоочередные действия ответственного за организацию обработки ПДн в организации, учреждении и предприятии.
3. Какие документы в организации необходимо актуализировать в соответствии с изменениями законодательства? Какие новые документы необходимо разработать в организации?
4. Какие новые обязанности появились у операторов ПДн в связи с изменением законодательства: информирование об инцидентах с персональными данными, уведомление о трансграничной передаче, уведомление о обработке ПДн, взаимодействие с ГосСОПКОЙ, порядок взаимодействия с субъектом ПДн и т.д.
5. Проблемные вопросы обработки персональных данных работников, клиентов, граждан, контрагентов, соискателей, бывших работников, практикантов и иных категорий субъектов. Какие данные нельзя собирать? Какие данные при сборе регулятор считает избыточными? Кадровые службы: сбор, обработка персональных данных работника, родственника работника, соискателя.
6. Алгоритм действий ответственного за организацию обработки персональных данных при выполнении требований по ст.10.1 ФЗ-152 «О персональных данных». Что изменилось и кого коснулись изменения?
7. Обработка ПДн на страницах официальных групп организаций в социальных сетях.
8. Персональные данные на сайте организации. Новые требования к размещению. Санкции за распространение ПДн без отдельного согласия. Полный запрет использования ПДн из Интернета-как быть?
9. Проблемные вопросы хранения персональных данных работников и клиентов. Какие внутренние документы регламентируют процедуры хранения ПДн? Электронное хранение документов.
10. Новые требования к Согласиям. Почему форм согласий в организации должно быть не две, «как обычно» (по работнику и клиенту), а от 5 до 15? Что значит, что теперь «общее» Согласие – под запретом?
11. Принципиальные изменения передачи персональных данных работников, граждан, клиентов. Что нужно изменить в процессах обработки и внутренних локальных документах? Главные риски передачи персональных данных. Новые требования к трансграничной передаче ПДн.

12. Случаи обязательного размещения Политики по обработке и защите персональных данных на официальном сайте организации. Что необходимо изменить в содержание документа. Случаи размещения дополнительных документов, определяющих политику обработки персональных данных. Количество и содержание документов.
13. Какой минимум документов по персональным данным должен быть в каждой организации, исходя из практики проверок Роскомнадзора? Формы и содержание этих документов. Как привести работу с бумажными носителями персональных данных в соответствие с Постановлением Правительства №687.
14. Проведение аудита (внутреннего контроля) обработки и системы защиты персональных данных.

## **День 2 (15.04.26): Разработка ключевых документов по персональным данным**

1. Перечень обязательных документов, необходимый оператору для выполнения требований законодательства и успешного прохождения контрольно-надзорных мероприятий Роскомнадзора.
2. **Уведомления** о начале обработки ПДн. Уведомления о внесении изменений: практика заполнения.
3. Подготовка форм **Согласий**:
  - Согласие работника - при передаче третьим лицам (по каждому третьему лицу в отдельности + по каждой цели третьему лицу в отдельности);
  - Согласие работника - на распространение персональных данных (сайт; страницы в ВКонтакте, Одноклассники, визитки; рекламные буклеты; бейдж; информационный стенд лучших работников т.д.);
  - Согласие работника - при трансграничной передаче (при случаях выезда работников в командировку за границу, отправке за границу документов по запросу из некоторых стран СНГ и т.д)
  - Согласие работника - при обработке специальных категорий (например, диагнозов о хронических заболеваниях, справок по антителям)
  - Согласие работника - при обработке биометрических данных (при изготовлении служебного удостоверения, при выпуске электронного пропуска и т.д.)
  - Согласие клиента (гражданина)-при передаче ПДн третьему лицу (при обязательных случаях)
  - Согласие контрагента - физического лица (при обязательных случаях)
  - Согласие кандидата на вакансию (например, при кадровом резерве)
  - Согласие бывшего работника (например, ветерана)
  - Согласие временного работника/стажер/ученик (при случаях передачи)
4. **Формы договоров** с третьими лицами, при передаче им на обработку персональных данных работников (банки, поликлиники, учебные центры ДПО, операторы связи, аутсорсинговые компании, операторы информационных систем, арендодатели, ресурсоснабжающие компании и т.д.).
5. **Типовые формы бумажных документов**, включающие персональные данные (заявления, анкеты, журналы, книги и т.д.)
6. **Политика** по обработке и защите персональных данных в соответствии с рекомендациями Роскомнадзора от 27.07.2017 г. (ч. 1 п.2 ст. 18.1 ФЗ №152).
7. Необходимые документы для назначения ответственного за организацию обработки ПДн: приказ, должностная инструкция, план внутреннего контроля.
8. **Правила передачи** ПДн сторонним организациям (ч. 1 п. 2 ст. 18.1 ФЗ №152).
9. **Акт оценки вреда субъектам ПДн** (ч. 1 п. 5 ст. 18.1 ФЗ №152).
10. **Регламент рассмотрения запросов субъектов ПДн.**
11. **Регламент проведения внутреннего контроля** соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.
12. **Итоговый документ внутреннего контроля**-заполним Проверочный лист за обработкой персональных данных, утвержденный Приказом Роскомнадзором от 24.12.2021 № 253.

## **День 3 (16.04.26): Подготовка к контрольно-надзорным и профилактическим мероприятиям Роскомнадзора. Ответы на вопросы слушателей курса.**

1. Что важно знать из постановления Правительства №1046 от 29.06.2021 «О федеральном государственном контроле (надзоре) за обработкой персональных данных»?
2. «Объекты» контроля. Что вам нужно подготовить к проверке?
3. Какой необходимый пакет документов по обработке и защите персональных данных обязаны подготовить? Что, кроме документов, будет проверять Роскомнадзор?
4. Что необходимо знать руководителю, ответственному и работникам организации при общении с представителями Роскомнадзора? Каковы их действия? Практика ошибок.
5. Как правильно проинструктировать всех сотрудников перед проверкой Роскомнадзора? Какие вопросы, как правило, задают инспектора? Что нужно обязательно знать сотрудникам и как правильно отвечать на вопросы инспекторов Роскомнадзора? На каких «коварных» вопросах «попадаются» сотрудники?

6. О каких внутренних процессах работы с персональными данными нужно рассказывать инспектору во время проверки, о чём молчать.
7. Контроль за оператором без взаимодействия, какие риски, на что необходимо обратить внимание?
8. Как Роскомнадзор использует информацию из Уведомления при проведении контрольно-надзорных мероприятий?
9. Какие нарушения Роскомнадзор традиционно находит в разделе «Правовые основания обработки персональных данных»? - а это предписание и штраф.
10. Какие документы по персональным данным необходимо синхронизировать с Уведомлением и Политикой в области обработки и защиты персональных данных?
11. Каким локальным актам организации будет уделено «особое» внимание РКН? Какие «слабые» места в документах находит Роскомнадзор при проведении контрольно-надзорных мероприятий?
12. Какие внутренние типовые формы документов, содержащих персональные данные, будут подвергаться жесткому анализу, а на какие формы документов законодательные требования при проверках не распространяются?
13. Какие традиционные нарушения находит Роскомнадзор по гл14 ТК и, в особенности, - по ст.88? 10 «традиционных» нарушений отдела кадров по ведению документов работников, соискателей, в т.ч. хранению и уничтожению, которые приводят к штрафам по ч.1 и ч.6 ст.13.11 КоАП.
14. Как правильно подготовить отдел кадров к проверке? Какие документы подвергаются контролю? Какие процессы подвергаются анализу?
15. Как правильно подготовить бухгалтерию к проверке? Какие формы, какие документы предъявлять, какие нет?
16. Как правильно подготовить к проверке отделы, работающие с гражданами (клиентами)?
17. Как Роскомнадзор контролирует выполнение требований по наличию отдельных письменных Согласий работника?
18. Как правильно хранить носители персональных данных? За «Хранение» и «Согласия» – самые высокие штрафы по ст.13.11 КоАП.
19. Какие требования предъявляются при проверке к осуществлению внутреннего контроля и аудита соответствия обработки персональных данных? Как правильно документировать процедуры внутреннего контроля? Статус «Правил и Плана осуществления внутреннего контроля» или «Аудиторского заключения по оценке соответствия обработки ПДн по персональным данным? Ваши действия.
20. Судебная практика по итогам контрольно-надзорных мероприятий Роскомнадзора за нарушения в сфере персональных данных по каждой части ст.13.11 КоАП.
21. Что инспектор Роскомнадзора находит «незаконного» на компьютере отдела кадров, бухгалтерии, в отделе по работе с гражданами (клиентами), даже если вы считаете, что готовы к проверке?
22. Какие должностные инструкции подвергаются особому анализу в суде в случаях наложения административного штрафа? Какие позиции инструкций нужно переутвердить? Что нужно обязательно прописать в трудовом договоре, должностной инструкции работника?

### АВТОР и ПРЕПОДАВАТЕЛЬ КУРСА

**Астахов Александр Геннадьевич** - руководитель Института мониторинга и оценки информационной безопасности. Специалист-практик в сфере обработки и защиты персональных данных. Руководил более **600** проектами по защите ПДн, провел более **520 курсов** и семинаров по персональным данным, на которых прошли очное обучение более 5000 слушателей в **53** регионах России. Лично подготовил более **30** организаций к проверкам Роскомнадзора по персональным данным.

### УСЛОВИЯ УЧАСТИЯ ОБУЧЕНИЕ С ПРИМЕНЕНИЕМ ДИСТАНЦИОННЫХ ТЕХНОЛОГИЙ:

Даты обучения (вебинар)	14 – 16 апреля 2026 г.
Время подключения к вебинару	09.00 – 12.00 (МСК)/ 3 часа
Доступ к материалам	постоянно в период обучения
Место обучения	удаленное место слушателя
Стоимость участия в 1 дне вебинара на выбор слушателя	<b>5 990 руб.</b>

СТОИМОСТЬ ОБУЧЕНИЯ НА КУРСЕ		
	пакет «Специалист»	пакет «Профи»
Участие в обучении	✓	✓
Видеозапись вебинаров	✓	✓
Презентации лектора	✓	✓
Методические материалы	✓	✓

Сертификат о прохождении обучения	✓	✓
Подключение к семинару «Персональные данные: реагирование на утечки, взаимодействие с регуляторами» + видеозапись семинара и презентация лектора	✓	✓
Подключение ко 2 модулю курса «Обеспечение безопасности персональных данных в ИСПДн» + видеозапись модуля и презентация лектора		✓
Индивидуальная консультация по организации обработки ПДн в Вашей организации (1 час)		✓
<b>СТОИМОСТЬ</b>	<b>12 990</b>	<b>16 990</b>

**Лицензии ГК:**

1. Лицензия на право осуществления образовательной деятельности № 038554 от 24.07.2017г Департамента образования города Москвы. Лицензия действует бессрочно.
2. Лицензия ФСТЭК России № 1028 от 04.03.2010 на деятельность по технической защите конфиденциальной информации. Лицензия действует бессрочно.
3. Лицензия Управления ФСБ России № 271 от 30.12.2014 на осуществление деятельности по распространению шифровальных (криптографических) средств. Лицензия действует бессрочно.

**ПРЕДВАРИТЕЛЬНАЯ РЕГИСТРАЦИЯ ОБЯЗАТЕЛЬНА**

тел. 8 (906) 055-25-35 тел. 8 (495) 268-13-42 e-mail: [info@imoib.ru](mailto:info@imoib.ru); [www.imoib.ru](http://www.imoib.ru)

**ЭЛЕКТРОННАЯ РЕГИСТРАЦИЯ НА САЙТЕ:** <https://imoib.ru/training/course/1884>

Руководитель Института МОИБ

А.Г. Астахов