УДК 34

Развитие законодательства о защите персональных данных

Байкалова Ольга Алексеевна

Магистрант,
Новосибирский национальный исследовательский
государственный университет,
630090, Российская Федерация, Новосибирск, ул. Пирогова, 2;
e-mail: ol.podshivalova@mail.ru

Гулиева Земфира Адыгезаловна

Магистрант,
Новосибирский национальный исследовательский
государственный университет,
630090, Российская Федерация, Новосибирск, ул. Пирогова, 2;
e-mail: gulieva01@internet.ru

Аннотация

В статье рассматриваются актуальные изменения в законодательстве о персональных данных, включая ограничения на проверки Роскомнадзора и ужесточение ответственности за нарушения, вступающие в силу в 2025 году. Описаны меры, которые компании должны предпринять для минимизации рисков, начиная с регистрации в реестре операторов персональных данных и публикации необходимых документов и заканчивая внедрением системного управления защитой данных. Особое внимание уделяется практическим шагам и необходимости перехода от формального подхода к эффективной защите персональной информации. Внедрение системы защиты персональных данных – это постепенный и непрерывный процесс развития компании и ее процессной зрелости. На первых этапах необходимо перейти от хаотичных действий к упорядоченным и задокументированным процессам. Это создает базу для дальнейшего контроля и интеграции защиты персональных данных в общую структуру бизнес-процессов. Цель – построить полностью управляемую и адаптивную систему, способную оперативно реагировать на изменения и новые угрозы. Законодательство о персональных данных предъявляет настолько обширные требования, что достичь полного соответствия практически невозможно, – совершенствование процессов необходимо постоянно. А простого наличия документов недостаточно для предотвращения рисков проверок и утечек данных. Только системный подход, включающий регулярный анализ регуляторных требований, управление процессами обработки данных, контроль за их выполнением, а также обучение сотрудников, позволит минимизировать риски и поддерживать высокий уровень защиты информации. С каждым новым этапом компания снижает уровень угроз, а система защиты персональных данных становится все более зрелой и эффективной.

Для цитирования в научных исследованиях

Байкалова О.А., Гулиева З.А. Развитие законодательства о защите персональных данных // Вопросы российского и международного права. 2024. Том 14. № 9А. С. 199-205.

Ключевые слова

Роскомнадзор, мораторий, персональные данные, внеплановые проверки, защита данных, 2025, КоАП, ответственность, риск-ориентированный подход, система управления данными.

Введение

Сейчас действует мораторий на проверки Роскомнадзора [Постановление Правительства РФ от 10.03.2022 № 336, 2022]: плановые проверки ограничены до 2030 года [Постановление Правительства от 14.12.2023 № 2140, 2023], а внеплановые проверки (документарные, выездные, инспекционные визиты) ограничены до 2024 года [Постановление Правительства РФ от 10.03.2023 № 372, 2023].

Но проверки именно ограничены, а не запрещены. Например, если компания допускает какие-то нарушения, то Роскомнадзор может провести внеплановую проверку по согласованию с прокуратурой. Основанием для проверки может стать утечка персональных данных, отсутствие компании в реестре операторов, осуществляющих обработку персональных данных или любая жалоба (а их количество ежегодно растет, за 2023 г. прирост жалоб составил 30% [Итоги работы с обращениями граждан в Роскомнадзоре в 2023 году и 2024 году, www]).

Также Роскомнадзор ввел практику систематического наблюдения за сайтами операторов персональных данных. Если будет выявлено три несоответствия между сайтом и реестром, то Роскомнадзор также может провести внеплановую проверку [Приказ Минцифры России от 17.08.2023 № 720; зарег. в Минюсте 07.11.2023, www].

Основная часть

С 11 декабря 2024 года введена новая ст. 272.1 в УК РФ за незаконные использование, передачу, сбор и хранение компьютерной информации, содержащей персональные данные, а равно создание и обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и распространения [Федеральный закон от 30.11.2024 № 421-ФЗ, 2024]. Санкции предусматривают штрафы от 300 000 до 3 000 000 рублей, принудительные работы от 4 до 5 лет, лишение свободы от 4 до 10 лет, запрет должности или деятельности от 2 до 5 лет.

С 30 мая 2025 года будет значительно ужесточена ответственность за нарушения в области персональных данных по КоАП [Федеральный закон от 30.11.24 № 420-ФЗ, 2024]. Таким образом, самые крупные штрафы по КоАП будут выглядеть так, как представлено в таблице 1.

Таблица 1 – Штрафы, за нарушения в сфере персональных данных

Нарушения ст.13.11 КоАП в сфере персональных данных (ПДн)	Штраф за первое нарушение, (в руб.)	Штраф за повторное нарушение, (в руб.)
ч. 1: обработка ПДн в не предусмотренных законом случаях или несовместимая с целями сбора	150–300 тыс.	300–500 тыс.

Нарушения ст.13.11 КоАП в сфере персональных данных (ПДн)	Штраф за первое нарушение, (в руб.)	Штраф за повторное нарушение, (в руб.)
ч. 2: обработка ПДн без согласия или с ненадлежащим согласием	300–700 тыс.	1–1,5 млн
ч. 5: невыполнение обязанностей по уточнению, блокировке или уничтожению ПДн	50–90 тыс.	300–500 тыс.
ч. 8: нарушение локализации ПДн на территории РФ	1–6 млн	6–18 млн
ч. 11: неуведомление и (или) несвоевременное уведомление об утечке ПДн	1–3 млн	–
ч. 12-14: утечка ПДн от 1000 субъектов или 10 000 идентификаторов	1–15 млн. (зависит от объема утечки)	1-3% годовой выручки (20–500 млн)
ч. 16-17: утечка специальных или биометрических ПДн	10 – 15 млн	

Таким образом, несмотря на мораторий, у Роскомнадзора есть множество оснований для проведения внеплановых проверок, а с 2025 года мораторий на внеплановые проверки будет снят. Уже сейчас вступила в действие новая статья УК РФ, а в мае 2025 года будет значительное ужесточение ответственности по КоАП.

В условиях усиливающегося контроля и растущих штрафов за нарушения в области персональных данных компаниям необходимо заранее подготовиться к изменениям. Следование новым требованиям требует не просто формального соблюдения правил, а выстраивания последовательной и эффективной системы защиты персональных данных.

Роскомнадзор применяет риск-ориентированный подход, поэтому для минимизации рисков важно действовать последовательно и начинать с наиболее приоритетных направлений. Полноценная система защиты персональных данных не создается одномоментно, это процесс постепенного развития компании. Поэтому следует переходить от устранения критичных нарушений к выстраиванию системного управления.

Шаг 1. Это первоочередные меры для минимизации рисков, которые могут быть выявлены Роскомнадзором при контрольных мероприятиях без вашего участия:

1. Если ваша компания не зарегистрирована в реестре операторов персональных данных, вы находитесь в зоне повышенного риска. В уведомлении следует подробно указать все цели обработки персональных данных, перечислить конкретные категории обрабатываемых данных, субъектов, чьи данные обрабатываются, способы обработки, а также правовые основания для такой обработки. Для определения этих данных целесообразно провести минимальный аудит процессов компании.

2. Материалы на сайте – необходимо опубликовать политику конфиденциальности, согласие на обработку персональных данных, иметь правильные формы согласий, регистраций, cookie-баннер и т.д.

Шаг 2. Устраняем основные нарушения, которые помогут избежать наиболее распространенных нарушений:

1) приказ об утверждении плана мероприятий по приведению деятельности Компании в соответствие с требованиями законодательства РФ в области персональных данных, назначении лица, ответственного за обработку и защиту персональных данных, и утверждении его должностной инструкции;

2) общая политика конфиденциальности компании;

3) положение по организации обработки и обеспечению безопасности персональных данных вместе с формами документов, которые организационно необходимы в процессах

обработки персональных данных: акт об уничтожении персональных данных; отзыв согласия; журнал учета обращений субъектов персональных данных;

4) правила контроля защищенности персональных данных и процессов обработки персональных данных;

5) акт оценки вреда, который может быть причинен субъектам персональных данных;

6) формы согласий на обработку персональных данных: согласие на обработку персональных данных; согласие об обработке персональных данных обязательной письменной формы; согласие на обработку персональных данных, разрешенных для распространения.

7) документы, регламентирующие взаимодействие с третьим лицами по обработке персональных данных (договор поручения, соглашение о сооператорстве);

8) документы, регламентирующие работу сотрудников с персональными данными (порядок их доступа к персональным данным, перечень работников с допуском) и внесение правок в трудовые договоры и должностные инструкции.

Шаг 3. Чтобы система защиты персональных данных была эффективной и работала на практике, переходите от формальной подготовки документов к системному управлению:

1) вводим реестр всех процессов компании, связанных с обработкой персональных данных, и реестр информационных баз, в которых проходит их обработка, –это единая «база знаний», где содержатся цели и основания обработки персональных данных; категории субъектов персональных данных; объем обрабатываемых персональных данных; описание процессов хранения, уничтожения, передачи данных по каждой цели обработки и т.д.

В отсутствие такого реестра все остальные документы компании остаются неработающими шаблонами вне действующих бизнес-процессов.

2) внедряем процессы контроля, мониторинга и обучения

Необходимо регулярно анализировать и актуализировать перечень регуляторных требований, а также проверять соответствие внутренних и внешних документов стандартам обработки персональных данных. Регулярные аудиты, консультации для подразделений, обучающие тренинги для сотрудников — всё это неотъемлемые элементы эффективной системы защиты данных. Также необходимо поддерживать актуальность реестра процессов обработки персональных данных, своевременно вносить изменения в документы и оценивать соблюдение требований контрагентами. Контроль за ключевыми процессами (например, уничтожение персональных данных) обеспечивает дополнительную защиту и минимизирует риски. Такой системный подход позволяет компаниям не только соответствовать требованиям законодательства, но и поддерживать высокий уровень безопасности персональных данных.

Заключение

Внедрение системы защиты персональных данных – это постепенный и непрерывный процесс развития компании и ее процессной зрелости. На первых этапах необходимо перейти от хаотичных действий к упорядоченным и задокументированным процессам. Это создает базу для дальнейшего контроля и интеграции защиты персональных данных в общую структуру бизнес-процессов. Цель – построить полностью управляемую и адаптивную систему, способную оперативно реагировать на изменения и новые угрозы.

Законодательство о персональных данных предъявляет настолько обширные требования, что достичь полного соответствия практически невозможно, – совершенствование процессов необходимо постоянно. А простого наличия документов недостаточно для предотвращения

рисков проверок и утечек данных.

Только системный подход, включающий регулярный анализ регуляторных требований, управление процессами обработки данных, контроль за их выполнением, а также обучение сотрудников, позволит минимизировать риски и поддерживать высокий уровень защиты информации. С каждым новым этапом компания снижает уровень угроз, а система защиты персональных данных становится все более зрелой и эффективной.

Библиография

1. Об особенностях организации и осуществления государственного контроля (надзора), муниципального контрол»: постановление Правительства РФ от 10.03.2022 № 336 (ред. от 11.09.2024) // Собрание законодательства РФ. 2022. № 11. Ст. 1715.
2. О внесении изменений в некоторые акты Правительства РФ и признании утратившим силу отдельного положения акта Правительства РФ: постановление Правительства РФ от 10.03.2023 № 372 // Собрание законодательства РФ. 2023. № 12. Ст. 2025.
3. Итоги работы с обращениями граждан в Роскомнадзоре в 2023 году и 2024 году // Официальный сайт Роскомнадзора. URL: https://rkn.gov.ru/treatments/p436.
4. О внесении изменения в перечень индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных, утвержденный приказом Министерства цифрового развития, связи и массовых коммуникаций РФ от 15.11.2021 г. № 1187: приказ Минцифры России от 17.08.2023 № 720; зарег. в Минюсте 07.11.2023 // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru.
5. О внесении изменения в постановление Правительства РФ от 10 марта 2022 г. № 336: постановление Правительства от 14.12.2023 № 2140 // Собрание законодательства РФ. 2023. № 51. Ст. 9388.
6. О внесении изменений в УК РФ: федер. закон от 30.11.2024 № 421-ФЗ // Российская газета. 2024. № 278.
7. О внесении изменений в КоАП РФ: федер. закон от 30.11.24 № 420-ФЗ // Российская газета. 2024. № 278.

Development of legislation on personal data protection

Ol'ga A. Baikalova

Master's Student,
Novosibirsk National Research State University,
630090, 2 Pirogova str., Novosibirsk, Russian Federation;
e-mail: ol.podshivalova@mail.ru

Zemfira A. Gulieva

Master's Student,
Novosibirsk National Research State University,
630090, 2 Pirogova str., Novosibirsk, Russian Federation;
e-mail: gulieva01@internet.ru

Abstract

The article examines recent changes in personal data legislation, including limitations on Roskomnadzor inspections and the tightening of penalties for violations set to take effect in 2025. It outlines the measures companies should take to mitigate risks, starting with registration in the personal data operators' registry and publishing necessary documents, and extending to the

implementation of systematic data protection management. Particular attention is given to practical steps and the need to shift from a formal approach to effective personal data protection. The introduction of a personal data protection system is a gradual and continuous process of company development and its process maturity. In the first stages, it is necessary to move from chaotic actions to orderly and documented processes. This creates the basis for further control and integration of personal data protection into the overall structure of business processes. The goal is to build a fully managed and adaptive system capable of responding promptly to changes and new threats. The legislation on personal data imposes such extensive requirements that it is almost impossible to achieve full compliance, as process improvement is constantly necessary. And the mere presence of documents is not enough to prevent the risks of checks and data leaks. Only a systematic approach, including regular analysis of regulatory requirements, management of data processing processes, monitoring their implementation, as well as employee training, will minimize risks and maintain a high level of information protection. With each new stage, the company reduces the threat level, and the personal data protection system becomes more mature and effective.

For citation

Baikalova O.A., Gulieva Z.A. (2024) Razvitie zakonodatel'stva o zashchite personal'nykh dannykh [Development of legislation on personal data protection]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (9A), pp. 199-205.

Keywords

Roskomnadzor, moratorium, personal data, unscheduled inspections, data protection, 2025, Code of Administrative Offenses (KoAP), liability, risk-based approach, data management system.

References

1. Itogi raboty s obrashcheniyami grazhdan v Roskomnadzore v 2023 godu i 2024 godu [Results of working with citizens' appeals to Roskomnadzor in 2023 and 2024]. *Ofitsial'nyi sait Roskomnadzora* [Official website of Roskomnadzor]. Available at: https://rkn.gov.ru/treatments/p436.
2. O vnesenii izmenenii v KoAP RF: feder. zakon ot 30.11.24 № 420-FZ [On Amendments to the Code of Administrative Offenses of the Russian Federation: Federal Law of November 30, 2024 No. 420-FZ]. *Rossiiskaya Gazeta* [Russian Newspaper]. 2024. № 278.
3. O vnesenii izmenenii v nekotorye akty Pravitel'stva RF i priznanii utrativshim silu otdel'nogo polozheniya akta Pravitel'stva RF: postanovlenie Pravitel'stva RF ot 10.03.2023 № 372 [On amending certain acts of the RF Government and recognizing as invalid a separate provision of an act of the RF Government: RF Government Resolution No. 372 of March 10, 2023] (2023). *Sobranie zakonodatel'stva RF. St. 2025* [Collected Legislation of the Russian Federation. Art. 2025].. № 12. St. 2025.
4. O vnesenii izmenenii v UK RF: feder. zakon ot 30.11.2024 № 421-FZ [On Amendments to the Criminal Code of the Russian Federation: Federal Law of November 30, 2024 No. 421-FZ]. *Rossiiskaya Gazeta* [Russian Newspaper]. 2024. № 278.
5. O vnesenii izmeneniya v perechen' indikatorov riska narusheniya obyazatel'nykh trebovanii pri osushchestvlenii federal'nogo gosudarstvennogo kontrolya (nadzora) za obrabotkoi personal'nykh dannykh, utverzhdennyi prikazom Ministerstva tsifrovogo razvitiya, svyazi i massovykh kommunikatsii RF ot 15.11.2021 g. № 1187: prikaz Mintsifry Rossii ot 17.08.2023 № 720; zareg. v Minyuste 07.11.2023 [On amending the list of risk indicators for violation of mandatory requirements in the exercise of federal state control (supervision) over the processing of personal data, approved by Order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation dated November 15, 2021 No. 1187: Order of the Ministry of Digital Development, Communications and Mass Media of Russia of August 17, 2023 No. 720; reg. in the Ministry of Justice on November 7, 2023]. *Ofitsial'nyi internet-portal pravovoi informatsii* [Official Internet Portal of Legal Information]. Available at: http://pravo.gov.ru.
6. O vnesenii izmeneniya v postanovlenie Pravitel'stva RF ot 10 marta 2022 g. № 336: postanovlenie Pravitel'stva ot 14.12.2023 № 2140 [On amending Resolution of the Government of the Russian Federation dated March 10, 2022 No. 336: Resolution of the Government of the Russian Federation of December 14, 2023 No. 2140] (2023). *Sobranie*

zakonodatel'stva RF. St. 9388 [Collected Legislation of the Russian Federation. Art. 9388], 51..
7. Ob osobennostyakh organizatsii i osushchestvleniya gosudarstvennogo kontrolya (nadzora), munitsipal'nogo kontrol»: postanovlenie Pravitel'stva RF ot 10.03.2022 № 336 (red. ot 11.09.2024) [On the specifics of organizing and implementing state control (supervision), municipal control: RF Government Resolution No. 336 of March 10., 2022 (as amended on September 11, 2024)] (2022). *Sobranie zakonodatel'stva RF. St. 1715* [Collected Legislation of the Russian Federation. Art. 1715], 11.