Дата поступления рукописи в редакцию: 07.05.2026 г.
Дата принятия рукописи в печать: 27.05.2026 г.

DOI: 10.24412/2782-3849-2026-5-38-43

ДОРСКАЯ Александра Андреевна,

доктор юридических наук, профессор,
заведующая кафедрой общетеоретических
правовых дисциплин Северо-Западного филиала
ФГБОУ ВО «Российский государственный
университет правосудия имени В.М. Лебедева»,
профессор кафедры международного права
ФГБОУ ВО «Российский государственный
педагогический университет им. А.И. Герцена»,
SPIN-код: 9965-3211, AuthorID: 314268,
e-mail: adorskaya@yandex.ru

ВОРОПАЕВА Мария Николаевна,

студентка 4 курса бакалавриата
факультета подготовки специалистов
для судебной системы (юридического факультета)
Северо-Западного филиала ФГБОУ ВО «Российский государственный
университет правосудия имени В.М. Лебедева»,
e-mail: masavoropaeva71083@gmail.com

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЕС И ЕАЭС: ПРАВОВОЙ АНАЛИЗ ОСНОВ РЕГУЛИРОВАНИЯ

Аннотация. *В статье проводится сравнительное исследование основ правового регулирования персональных данных в двух крупнейший региональных интеграционных объединения Евразии: ЕС и ЕАЭС. Целью исследования является заложение фундамента для дальнейшей работы над единым законодательным актом о защите персональных данных на уровне ЕАЭС, путем сопоставления норм уже существующего акта европейского регулирования (GDPR) и национальных норм государств-участников ЕАЭС, выявления как наиболее подходящих для дальнейшего заимствования институтов, так и институтов, нуждающихся в доработке или полном отказе от них. В рамках исследования авторы выводят схожие черты в регулировании, а также уделяют особое внимание фундаментальным различиям: целям правового регулирования и конституционно-правовой природе института персональных данных. Отмечая положительные и спорные моменты в регулировании обоих интеграционных объединений, авторы приходят к выводу о том, что национальное законодательство государств-участниц ЕАЭС должно лечь в основу разрабатываемого единого акта, при этом любые заимствования из европейского системы должны происходить с учетом национальных интересов государств евразийского пространства, а также экономических, политических и исторических особенностей развития ЕАЭС.*

Ключевые слова: *персональные данные, защита персональных данных, GDPR, Европейский союз, Евразийский экономический союз, трансграничная передача данных, унификация законодательства, цифровая экономика, конституционно-правовые основы регулирования.*

DORSKAYA Aleksandra Andreevna,

Doctor in Law, Professor, Head of the Department of Theoretical Legal Disciplines
of North-West branch of the Russian State University
of Justice named after V.M. Lebedev,
Professor at the Department of International Law
of Herzen University

VOROPAEVA Mariia Nicolaevna,

4th year bachelor's student
of the faculty of training specialists
for the judicial system (law faculty)
of the North-West branch of the Russian State
University of Justice named after V.M. Lebedev

PERSONAL DATA PROTECTION IN THE EU AND THE EAEU: A LEGAL ANALYSIS OF THE REGULATORY FRAMEWORK

Annotation. *This article conducts a comparative study of the foundations of legal regulation of personal data in the two largest regional integration associations of Eurasia: the EU and the EAEU. The aim of the research is to lay the groundwork for further work on a unified legislative act on personal data protection at the EAEU level by comparing the provisions of the existing European regulatory act (GDPR) with the national legislation of the EAEU member states, identifying both the institutions most suitable for further borrowing and those that require modification or should be abandoned entirely. Within the framework of the study, the authors identify similarities in regulatory approaches and pay particular attention to fundamental differences, including the objectives of legal regulation and the constitutional and legal nature of the institution of personal data. Noting both the strengths and the controversial aspects of regulation in the two integration associations, the authors conclude that the national legislation of the EAEU member states should form the basis of the future unified act. At the same time, any borrowing from the European regulatory system should take place with due regard to the national interests of the states of the Eurasian region, as well as to the economic, political, and historical particularities of the development of the EAEU.*

Key words: *personal data; personal data protection; GDPR; European Union; Eurasian Economic Union; cross-border data transfer; harmonization of legislation; digital economy; constitutional and legal foundations of regulation.*

Стремительное развитие мировой экономики и ее цифрового сектора сопровождается экспоненциальным ростом трансграничных потоков данных, в том числе персональных. Так к 2022 году объёмы трансграничных передач данных выросли примерно в 80 раз в сравнении с 2007 годом [4]. Естественно, что такие крупные интеграционные объединения как Европейский союз и Евразийский экономический союз не являются исключением. Уже в 2023 году 45,2% компаний ЕС использовали облачные сервисы [5], что в подавляющем большинстве случаев означает трансграничную передачу, обработку и хранение персональных данных, поскольку сервера таких облачных хранилищ находятся в других государствах. К 2025 году данный показатель достиг уже 52.74% [6]. Такое кратное увеличение объема данных неизбежно приводит и к росту ответственности субъектов их обработки, причем на всех уровнях. В частности, за четыре года действия Общего регламента ЕС по защите данных (General Data Protection Regulation - GDPR) (далее - GDPR, Регламент) надзорные органы вынесли 1132 штрафных санкций на общую сумму около 1,64 млрд евро [7]. Схожие тенденции прослеживаются и в государствах-членах ЕАЭС: в Российской Федерации только за 2022 год регулятор рассмотрел свыше 44 тыс. обращений граждан о нарушениях при обработке персональных данных [8], в Республике Беларусь количество схожих жалоб с 2022 по 2024 увеличилось более чем в 5 раз [9]. Описанная динамика явно указывает, что вопрос персональных данных давно вышел за рамки внутринационального регулирования и требует унификации на более высоком уровне. Однако подходы, избранные в рамках ЕС и ЕАЭС в вопросе персональных данных, существенно различаются. На территории ЕС окончательная унификация произошла ещё в 2018 года, когда начал применяться Общий регламент ЕС по защите персональных данных. В рамках ЕАЭС на сегодняшний день создана лишь Интегрированная информационная система (ИИС ЕАЭС), которая обеспечивает трансграничный обмен данными между государствами-членами Союза [1]. К сожалению, при наличии развитой цифровой инфраструктуры общее наднациональное законодательство о защите персональных данных отсутствует. Обработка и защита персональных данных продолжают регулироваться исключительно на национальном уровне. Это порождает множество проблем, начиная от постоянной необходимости разрешения коллизионного вопроса, заканчивая сложностями с обеспечением надлежащего

уровня безопасности информационного пространства в рамках ЕАЭС. Вопрос унификации законодательства ЕАЭС остро стоит уже несколько лет [2], однако единого акта или проекта документа за это время выработать так и не удалось. Таким образом, проведение сравнительного анализа основ законодательства о персональных данных в ЕС и ЕАЭС является крайне актуальным на сегодняшний день. Такое исследование позволит создать основу для формирования согласованного подхода к защите персональных данных и в перспективе — разработки единого правового акта в рамках ЕАЭС, направленного на сближение национальных правовых систем и повышение эффективности правового регулирования в условиях трансграничной обработки персональных данных.

Несмотря на то, что Европейский союз и Евразийский экономический союз представляют собой разные по своей правовой природе интеграционные объединения, в сфере регулирования персональных данных прослеживаются определённые сходства. В частности, совпадают базовые принципы обработки персональных данных (законность, ограничение цели, минимизация, точность, ограничение срока хранения и обеспечение безопасности), закрепляется правовой статус субъекта данных как носителя самостоятельных прав, а также предусматривается обязанность оператора (контролёра) принимать меры по защите информации и обеспечению её конфиденциальности. Вместе с тем при внешнем сходстве нормативных конструкций глубинное содержание значительно различается. Одно из ключевых различий заключается в целях регулирования. Так, основными целям принятия GDPR, исходя из статьи 1 Регламента, принято считать: а) укрепление гарантий защиты прав физических лиц 2) правовая определенность в вопросах ответственности субъектов обработки 3) обеспечение надлежащего уровня регулирования вопроса защиты персональных данных в условиях цифрового суверенитета [3]. Такая постановка целей имеет практические последствия. Так, реализуя цели, закрепленные в 1 статье, европейский законодатель вводит модель подотчетности контролера (статья 5 GDPR) - он обязан доказывать контролирующему органу соблюдение действующего законодательства, в том числе на нем лежит обязанность выстроить систему сбора, обработки и хранения данных таким образом, чтобы контролирующий орган мог в любой момент получать доступ к любому участку системы и провести аудит. Кроме того, у физического лица также есть право на получение информации о процессе обработки его данных, в том числе о сроках, целях, вопросах трансграничности и так далее (статья 15 Регламента). Очевидно, что многоуровневые цели GDPR реализуются на практике через «проактивную» модели - законность обработки контролируется не столько посредством внешнего надзора, сколько через институционализацию внутреннего контроля, причем соответствующие обязанности контролёра могут возникать ещё до фактического начала обработки персональных данных, в частности на стадии предварительной оценки рисков [10]. Комплексный анализ законодательства государств-членов ЕАЭС позволяет выявить общую цель регулирования: обеспечение защиты прав и свобод человека и гражданина при сборе и обработке персональных данных. Такая цель представляется более узкой в сравнении с европейской моделью. С одной стороны, таким образом законодатели выстраивают регулирование вокруг гарантий прав более «слабых» участников отношений - физических лиц, ставя их защиту в приоритет над интересами бизнеса или государства. В условиях цифровой экономики, где физическое лицо всегда находится в уязвимом положении, такая расстановка приоритетов как нельзя лучше демонстрирует социальную направленность государства. Однако избранный подход также порождает некоторые риски. В частности, защита прав человека представляется затруднительной в отсутствии выстроенных механизмов ответственности операторов. На практике сведение цели регулирования исключительно к защите прав человека без дополнительных элементов приводит к формированию «реактивной» модели: операторы стремятся лишь к формальному соблюдению законодательства, а превентивные механизмы внутреннего контроля и управления рисками развиты ограниченно. В результате риск человеческого фактора значительно увеличивается, что в том числе приводит к регулярным утечкам данных [11].

Представляется, что необходимо сохранить приоритет защиты прав и свобод человека и гражданина, созданный в анализируемых законодательствах, однако добавить в цели регулирования иные элементы, которые позволят обеспечить более стабильную реализацию главной цели на практике, а также создадут условия для дальнейшей интеграции и развития.

Кроме того, законодательство ЕС и ЕАЭС также значительно различается с точки зрения конституционно-правовой природы института персональных данных. В ЕС право на защиту персональных данных воспринимается законодателем как самостоятельное, фундаментальное право гражданина,

закреплённое в Хартии Европейского союза об основных правах (далее - Хартия) (ссылка, статья 8). При этом государства-члены ЕАЭС, как правило, не выделяют такое право отдельно, оно выводится из более общих конституционных гарантий: неприкосновенность частной жизни, право на личную и семейную тайну и тд (это следует, в частности, из Постановления Конституционного Суда РФ от 25.05.2021 N 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона «О персональных данных» в связи с жалобой общества с ограниченной ответственностью «МедРейтинг» + Решения Конституционного Суда Республики Беларусь «О соответствии Конституции Республики Беларусь Закона Республики Беларусь «О защите персональных данных» от 29 апреля 2021 г. № Р-1261/2021). Такая разница в оценках самой природы права на защиту персональных данных неизбежно оказывает влияние на практический аспект. В рамках ЕС законодатель, регуляторы и суды в случае даже незначительных нарушений GDPR будут оценивать такое деяние через призму посягательства на самостоятельное фундаментальное право, а в государствах ЕАЭС - как частный аспект нарушения режима информации о личной жизни. Различие в правовой оценке в первую очередь сказывается на размере ответственности за нарушения. Если в ЕС статья 83 GDPR устанавливает штраф до 10 млн евро или 2% годового оборота компании при незначительных нарушениях и до 20 млн евро и 4% годового оборота компании при более крупных, то в государствах-членах ЕАЭС размер штрафов значительно меньше: в РФ штраф для юридических лиц варьируется от 50 тысяч до 1,5 млн рублей, то есть примерно от 555 до 16 655 евро (статья 13.11 КоАП РФ), в Республике Беларусь - до 200 базовых величин - около 2 500 евро (23.7 КоАП Республики Беларусь), в Республике Казахстан - до 2000 МРП для крупного бизнеса - около 14 900 евро (статья 79 КоАП Республики Казахстан). Кроме того, жесткость предъявляемых регуляторами требований также значительно различается: проактивная европейская модель вынуждает компании не только формально соблюдать действующие ограничения, но и постоянно доказывать факт их соблюдения, тратить огромные ресурсы на создание внутренней системы контроля и анализа рисков. Такой жесткий способ регулирования представляется не в полной мере целесообразным. Согласно данным Центра европейских экономических исследований имени Лейбница (ZEW) [12] в результате расширенного опроса 1350 немецких компаний около половины считает, что негативные последствия внедрения GDPR превышают положительный эффект. Компании жалуются на значительное усложнение бизнес-процессов, резкий рост расходов на создание и поддержание внутренней системы контроля и анализа рисков. Кроме того, внедрение новых технологий, в том числе искусственного интеллекта, значительно затруднено, что неизбежно ведет к упущенной выгоде для предпринимателей. Таким образом, с учетом особой роли малого и среднего бизнеса в экономиках государств-членов ЕАЭС, создание аналогичной ресурсоёмкой системы регулирования может привести к значительному увеличению затрат бизнеса и многократному росту потенциальных рисков для субъектов предпринимательской деятельности.

Проведенный анализ позволяет сделать следующие выводы:

- В виду значительных различий в условиях формирования исследованных интеграционных объединений, правовые модели регулирования персональных данных значительно различаются, несмотря на наличие некоторых общих черт. - Основными целями регулирования персональных данных в рамках GDPR европейский законодатель определил баланс интересов личности, бизнеса и цифровой экономики. При этом уклон был сделан в проактивную модель с возложением на контролера ответственности за создание многоступенчатой системы отчетности и контроля за соблюдением всех требований. Такой подход в значительной степени защитил право европейских граждан на защиту персональных данных, гарантированное Хартией. Однако создание столь жесткого механизма регулирования неизбежно повлекло за собой множественные проблемы для предпринимателей и бизнеса, создав для них дополнительных расходы и риски.

- В государствах-членах ЕАЭС главной целью регулирования персональных данных является защита прав человека и гражданина. Такой исключительный приоритет прав личности ярко демонстрирует социальную ориентацию государств-участников Союза, однако в отсутствии дополнительных целей (в частности, стабильное развитие бизнеса, создание благоприятных условий для экономического роста и тд) может приводить к излишне формалистскому подходу в ущерб результативности регулирования.

- Особые исторические, экономические и политические условия развития ЕАЭС как интеграционного объединения не позволяют механически заимствовать созданные в ЕС правовые институты. При выработке единого акта по вопросу защиты персональных данных на уровне ЕАЭС безусловно необходимо

учитывать удачный опыт иных интеграционных объединений, в том числе европейский. Однако в первую очередь необходимо учитывать интересы государств-участников, а также особые цели евразийской интеграции. Представляется, что в основу будущего акта должно лечь уже существующего нормативное регулирование государств Союза с незначительными изменениями некоторых институтов.

Список литературы:

[1] Бороздин А.Н., Коварда В.В. Анализ системы обеспечения защиты информации в процессе цифровизации ее оборота в рамках ЕАЭС в аспекте повышения экономической безопасности // Вестник Евразийской науки, 2020 №4. URL: https://esj.today/PDF/41ECVN420.pdf (дата обращения: 10.02.2026).

[2] Гаджиева К. А. Гармонизация правового поля стран ЕАЭС в области защиты персональных данных // Бизнес. Образование. Право. 2021. № 2 (55). С. 258–262.

[3] Удовиченко Ю. Г., Ногаева В. У. General Data Protection Regulation // Актуальные проблемы российского права. – 2018. – No 8 (93). – С. 222.

[4] Boston Consulting Group; United Nations Capital Development Fund. Cross-Border Data Flows: A Pathway to Inclusive Growth: аналитический отчёт. - 2022. URL: https://web-assets.bcg.com/7a/2b/9a0cb4b545ad87cf7e901301ad27| en-uncdf-brief-cross-border-data-flows-2022.pdf (дата обращения: 10.02.2026).

[5] European Commission. Cloud computing. URL: https://digital-strategy.ec.europa.eu/en/policies/cloud-computing (дата обращения: 10.02.2026).

[6] Eurostat. Cloud computing – statistics on the use by enterprises: аналитический материал. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises (дата обращения: 10.02.2026).

[7] Four years under the EU GDPR: How to fix its enforcement: аналитический отчёт. – 2022. URL: https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-4-year-report-2022.pdf (дата обращения: 10.02.2026).

[8] С Днем Защиты персональных данных. Официальный Telegram-канал Роскомнадзора: публикации. URL: https://web.telegram.org/k/#@rkn_tg (дата обращения: 10.02.2026).

[9] Незаконная обработка персональных данных: число жалоб с 2022 года выросло в 5 раз // NEG.BY. URL: https://neg.by/novosti/otkrytj/nezakonnaya-obrabotka-personalnykh-dannykh-chislo-zhalob-s-2022-goda-vyroslo-v-5-raz/ (дата обращения: 10.02.2026).

[10] Мунтян А. Структурное описание принципа подотчётности в GDPR на основе ICO Accountability Framework. Версия 1.0 от 10.01.2022. RPPA (Russian Privacy Professionals Association). URL: https://rppa.pro (дата обращения: 26.02.2026)

[11] Роскомнадзор сообщил об утечке 500 млн данных о россиянах за один раз // РБК. – 2024. URL: https://www.rbc.ru/rbcfreenews/65d7ef3d9a7947d8608dbbb3 (дата обращения: 10.02.2026).

[12] Six years of GDPR: Companies remain critical // ZEW – Leibniz Centre for European Economic Research. – 2024. URL: https://www.zew.de/en/press/latest-press-releases/six-years-of-gdpr-companies-remain-critical (дата обращения: 10.02.2026).

References:

[1] Borozdin A.N., Kovarda V.V. Analysis of the Information Security System in the Process of Digitalization of Its Circulation within the EAEU in Terms of Improving Economic Security // Bulletin of Eurasian Science, 2020, No. 4. URL: https://esj.today/PDF/41ECVN420.pdf (accessed: 10.02.2026).

[2] Gadzhieva K.A. Harmonization of the Legal Field of the EAEU Countries in the Field of Personal Data Protection // Business. Education. Law. 2021. No. 2 (55). P. 258–262.

[3] Udovichenko Yu.G., Nogaeva V.U. General Data Protection Regulation // Actual Problems of Russian Law. – 2018. – No. 8 (93). – P. 222.

[4] Boston Consulting Group; United Nations Capital Development Fund. Cross-Border Data Flows: A Pathway to Inclusive Growth: Analytical Report. - 2022. URL: https://web-assets.bcg.com/7a/2b/9a0cb4b545ad87cf7e901301ad27| en-uncdf-brief-cross-border-data-flows-2022.pdf (accessed: 10.02.2026).

[5] European Commission. Cloud computing. URL: https://digital-strategy.ec.europa.eu/en/policies/cloud-computing (accessed: 10.02.2026).

[6] Eurostat. Cloud computing – statistics on the use by enterprises: analytical material. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises (accessed: 10.02.2026).

[7] Four years under the EU GDPR: How to fix its enforcement: analytical report. – 2022. URL: https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-4-year-report-2022.pdf (accessed: 10.02.2026).

[8] Happy Personal Data Protection Day. Official Telegram channel of Roskomnadzor: publications. URL: https://web.telegram.org/k/#@rkn_tg (accessed: 10.02.2026).

[9] Illegal processing of personal data: the number of complaints has increased 5-fold since 2022 // NEG.BY. URL: https://neg.by/novosti/otkrytj/nezakonnaya-obrabotka-personalnykh-dannykh-

chislo-zhalob-s-2022-goda-vyroslo-v-5-raz/ (accessed: 10.02.2026).

[10] Muntyan A. Structural description of the accountability principle in the GDPR based on the ICO Accountability Framework. Version 1.0 from 10.01.2022. RPPA (Russian Privacy Professionals Association). URL: https://rppa.pro (accessed: 26.02.2026)

[11] Roskomnadzor reported a leak of 500 million pieces of data on Russians in one go // RBC. – 2024. URL: https://www.rbc.ru/rbcfreenews/65d7ef3d9a7947d8608dbbb3 (date accessed: 10.02.2026).

[12] Six years of GDPR: Companies remain critical // ZEW – Leibniz Centre for European Economic Research. – 2024. URL: https://www.zew.de/en/press/latest-press-releases/six-years-of-gdpr-companies-remain-critical (date accessed: 10.02.2026).