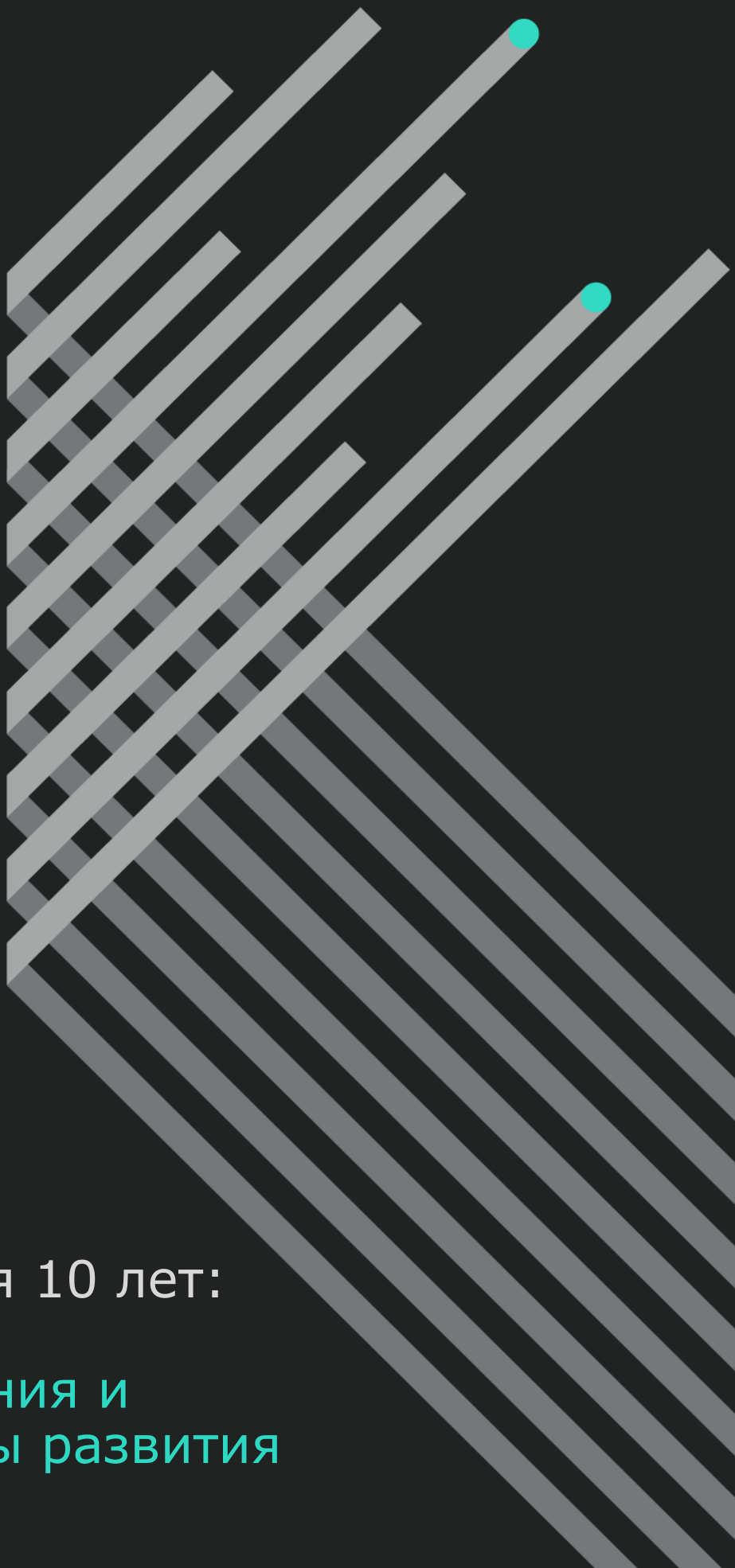
BGP LITIGATION

комплексная
правовая
поддержка

bgplaw.com



GDPR спустя 10 лет: эволюция регулирования и перспективы развития

27 апреля 2016 г. в Европейском союзе был принят Регламент 2016/679[1] (далее - «GDPR» или «Регламент»), что стало отправной точкой для формирования современной модели регулирования персональных данных.

Влияние Регламента при этом вышло далеко за пределы Европейского союза (далее – «ЕС») и оказало существенный вклад в развитие законодательства и правоприменительной практики в сфере защиты персональных данных во многих государствах, включая Россию, США, ОАЭ, Бразилию, Китай и ЮАР.

При этом за десять лет текст Регламента не подвергался законодательным изменениям.

Ввиду этого закономерно возникает вопрос о том, насколько его положения сохраняют актуальность в условиях стремительного развития технологий.

Чтобы ответить на этот вопрос мы рассмотрим предпосылки принятия Регламента, ключевые изменения, которые он внес в европейскую систему защиты персональных данных, основные тенденции его применения, а также развитие регулирования с учетом новых технологических вызовов.

Предпосылки появления GDPR

Формирование предпосылок для принятия регулирования о защите персональных данных началось задолго до принятия Регламента и проходило в несколько этапов.

1. Защита частной жизни как фундаментальное право

Одной из правовых основ стало закрепленное в ст. 8 Европейской конвенции о защите прав человека и основных свобод 1950 г. право на уважение частной и семейной жизни, жилища и корреспонденции.

Защита персональных данных рассматривалась прежде всего как элемент защиты фундаментальных прав человека.

2. Конвенция № 108: первые специальные положения

Следующим важным этапом в развитии регулирования стало подписание «Конвенции о защите физических лиц при автоматизированной обработке персональных данных» в 1981 г., известной как Конвенция № 108.

Конвенция стала первым юридически обязательным международным документом в Европе, непосредственно посвященным защите персональных данных и закрепившим основные принципы их обработки и права субъектов персональных данных.

3. Директива 95/46/ЕС: формирование общеевропейских правил

[1] Регламент (ЕС) 2016/679 Европейского парламента и Совета о защите физических лиц в отношении обработки персональных данных и о свободном обращении таких данных, а также об отмене директивы 95/46/ЕС.

В 1995 г. была принята Директива 95/46/ЕС[2], которая сформировала общеевропейские правила обработки персональных данных и заложила ряд принципов, позднее развитых в Регламенте.

Вместе с тем Директива требовала имплементации в национальное законодательство государств-членов ЕС. В результате сохранялись различия в национальных правилах, что создавало сложности для компаний, работающих одновременно в нескольких странах ЕС.

4. Развитие цифровой среды: необходимость нового регулирования

Одновременно стремительное развитие цифровых технологий, Интернета и трансграничных сервисов привело к резкому росту объемов обрабатываемых данных. Правовое регулирование, сформированное в 1990-е годы, перестало в полной мере соответствовать новым технологическим и экономическим реалиям.

Таким образом, к началу 2010-х годов сформировалась совокупность предпосылок для пересмотра европейской системы защиты данных: необходимость усилить защиту прав физических лиц, адаптировать регулирование к цифровой среде и одновременно обеспечить единообразие правил в ЕС.

Решение этих задач стало одной из ключевых целей для принятия Регламента в 2016 г.

Что изменил GDPR

1. Экстерриториальное действие

Одним из наиболее значимых нововведений Регламента стало его экстерриториальное действие (ст. 3):

Директива 1995 г.	**GDPR**
Каждое государство-член ЕС применяет к обработке персональных данных национальные нормы, которые принимает в соответствии с настоящей Директивой, когда **обработка осуществляется** в контексте деятельности учреждения оператора **на территории государства-члена ЕС.**	Регламент применяется в отношении обработки персональных данных в контексте деятельности учреждения контролера или обрабатывающего данные лица в Союзе, **вне зависимости от того, проводится обработка в Союзе или нет**.

Положения Регламента распространяются на лиц за пределами ЕС, если они обрабатывают персональные данные лиц, находящихся в ЕС, или осуществляют мониторинг их поведения.

2. Детализация прав и обязанностей

[2] Директива 95/46/ЕС Европейского парламента и Совета от 24 октября 1995 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных.

Положения Регламента также уточнили регулирование вопросов обработки данных, которые уже были освещены в Директиве:

Директива 1995 г.	**GDPR**
Основная ответственность возлагалась на контролера, тогда как обязанности процессора регулировались менее подробно.	Для процессора установлены подробные самостоятельные обязанности и ответственность за их нарушение. Обязанности контролера расширены и систематизированы.
Контролер обязан уведомлять надзорный орган о проведении операций обработки персональных данных.	Контролер и процессор в предусмотренных Регламентом случаях обязаны вести внутренние записи операций обработки, которые предоставляются надзорному органу по его запросу.

Регламент сформировал единый общеевропейский подход к регулированию обработки персональных данных, включая:

- Принципы privacy by design и privacy by default (ст. 25);
- Оценку воздействия на защиту персональных данных (Data Protection Impact Assessment, DPIA) при обработке, способной создать высокий риск для прав и свобод субъектов (ст. 35);
- Уведомление контролером надзорного органа об утечках персональных данных в течение 72 часов (ст. 33);
- Назначение DPO для указанных категорий организаций (ст. 37).

Регламент также закрепил новые права субъектов данных, включая право на переносимость данных (ст. 20) и право на удаление данных («право на забвение») (ст. 17).

3. Установление оборотных штрафов

Помимо этого, Регламентом установлены внушительные санкции за нарушения в сфере персональных данных. За нарушение ключевых требований предусмотрены штрафы до **20 млн евро или 4% мирового годового оборота** и до 10 млн евро или 2% оборота за иные нарушения.

Как следствие, Регламент сделал защиту персональных данных постоянной обязанностью бизнеса с риском получения внушительных штрафов в случае несоблюдения положений регламента. Практика подтверждает этот вывод.

Обзор практики применения GDPR

1. Дело WhatsApp: штраф 225 млн евро и роль Европейского совета по защите данных

Дело WhatsApp Ireland касалось прозрачности обработки данных пользователей, в том числе их передачи другим компаниям группы Facebook, а также обработки данных лиц, не пользовавшихся WhatsApp.

В соответствии с механизмом «единого окна» по трансграничным делам определяется ведущий надзорный орган. Как правило, им является орган государства, где находится основное учреждение компании в ЕС. Ирландия, где расположены европейские штаб-квартиры многих крупных технологических компаний, включая группу Facebook, по этой причине стала одной из ключевых юрисдикций по таким делам.

После направления Ирландской комиссией по защите данных (далее – «DPC») проекта решения по делу WhatsApp Ireland другим европейским регуляторам восемь из них заявили возражения. В связи с этим спор был передан на рассмотрение Европейского совета по защите данных (далее – «EDPB»).

В обязательном решении от 28 июля 2021 г. EDPB указал на необходимость пересмотреть выводы о допущенных нарушениях и увеличить размер штрафа. На основании этого решения DPC 20 августа 2021 г. назначила WhatsApp штраф в размере 225 млн евро.

Дело стало примером практической роли EDPB в обеспечении единообразного применения Регламента.

2. Дело Meta: штраф 1,2 млрд евро и трансграничная передача данных

Одним из наиболее значимых дел о трансграничной передаче данных стало решение DPC от 12 мая 2023 г. в отношении Meta Platforms.

Компания передавала данные пользователей Facebook из ЕС и ЕЭЗ в США на основании стандартных договорных условий (SCC) и дополнительных мер защиты. DPC, основываясь на обязательном решении EDPB, пришла к выводу, что эти меры не обеспечивали необходимого уровня защиты данных с учетом возможного доступа к ним со стороны органов власти США.

Meta была оштрафована на 1,2 млрд евро и обязана приостановить передачу данных и привести обработку в соответствие с GDPR.

Дело стало практическим применением подхода, согласно которому при передаче данных в третью страну необходимо оценивать не только условия договора между компаниями, но и законодательство и практику государства назначения. Если они не обеспечивают уровень защиты, эквивалентный европейскому, передача должна быть приостановлена или прекращена.

3. Дело Amazon: штраф 746 млн евро и поведенческая реклама

Решением Люксембургской комиссии по защите данных (CNPD) от 15 июля 2021 г. Amazon была оштрафована на 746 млн евро за использование персональных данных для поведенческой рекламы, в том числе отсутствие надлежащего правового основания для обработки и недостаточную прозрачность.

Административный суд Люксембурга в марте 2026 г. подтвердил основные выводы CNPD, но отменил штраф с учетом последующего развития практики Суда ЕС. В частности, суд учел сформированный Судом ЕС подход к необходимости установить наличие умысла или небрежности для применения финансовой

санкции. Вопрос о размере и возможности применения штрафа должен быть повторно рассмотрен CNPD.

Дело Amazon в очередной раз показывает, насколько важна судебная практика при применении Регламента. Развитие подходов Суда ЕС может существенно повлиять на возможность и размер последующей санкции.

4. Статистика

Масштаб этой системы также подтверждается отчетами европейских надзорных органов, которые свидетельствуют о стабильном росте количества обращений, проверок и сложных расследований.

Например, Испанское агентство по защите данных (AEPD) в 2025 г. получило 30 931 жалобу, что на 64% больше, чем в 2024 г. Число трансграничных дел также продолжает расти.

Французский регулятор (CNIL) также сообщил о рекордных показателях в 2025 году: 20 150 жалоб, 323 проверки и 259 корректирующих мер, включая 83 штрафа на общую сумму около 487 млн евро.

Таким образом, Регламент не только сделал защиту персональных данных постоянной обязанностью бизнеса, но и сформировал систему активного правоприменения с существенными финансовыми рисками для нарушителей.

Дальнейшая работа над GDPR

Хотя за десять лет Регламент не подвергался законодательным изменениям, среда, в которой применяется Регламент, существенно изменилась. Получили развитие новые модели цифровых платформ, алгоритмические системы и технологии искусственного интеллекта, что поставило вопрос о введении дополнительных регуляторных механизмов.

Однако и тогда Регламент не подвергся доработкам, а стал частью более масштабной системы цифрового регулирования в ЕС. Принятые в 2022 г. Digital Services Act (DSA) и Digital Markets Act (DMA) дополнили существующее регулирование специальными требованиями к цифровым платформам и крупным технологическим компаниям.

Например, DSA установлены дополнительные ограничения на таргетированную рекламу и использование профилирования, а DMA урегулировано использование и объединение данных крупными цифровыми платформами.

Таким образом, для крупных игроков цифрового рынка соблюдение требований Регламента теперь происходит в рамках более сложной системы взаимосвязанных цифровых правил.

Одновременно с этим в ЕС обсуждается снижение административной нагрузки, связанной с соблюдением требований Регламента, для ряда организаций.

В частности, в мае 2025 г. был представлен пакет Omnibus IV[3], направленный на упрощение регулирования и снижение административной нагрузки для малых и средних предприятий (далее – «МСП»). Предусмотренные изменения пока не приняты и не вступили в силу.

[3] Предложение Европейской комиссии о принятии Регламента в части распространения отдельных мер поддержки МСП на малые предприятия средней капитализации и дальнейшего упрощения регулирования (Omnibus IV) от 21 мая 2025 г., COM(2025) 501 final/3, процедура 2025/0130(COD).

Следующим этапом стал представленный в ноябре 2025 г. пакет Digital Omnibus[4], предусматривающий, в частности, следующие изменения в Регламент:

- Пересмотр определения «персональных данных» с учетом возможности конкретной организации идентифицировать физическое лицо. Предлагается уточнить, что информация не становится персональными данными для одной организации только потому, что другая организация располагает средствами для идентификации лица;
- Закрепление возможности использования данных при разработке и эксплуатации систем искусственного интеллекта, в том числе возможности использования законного интереса в качестве правового основания при соблюдении условий Регламента;
- Перенос в Регламент отдельных правил доступа к пользовательскому оборудованию (в т.ч в отношении cookie-файлов), возможности «единого согласия» и сохранения настроек на уровне браузера;
- Изменение порядка уведомления о нарушениях безопасности персональных данных: повышение порога, при котором возникает обязанность уведомления надзорного органа, увеличение срока уведомления с 72 до 96 часов;
- Уточнение положений об автоматизированном принятии решений и стандартизация подходов к DPIA.

Соответствующие поправки в Регламент пока не приняты. Вместе с тем обсуждение его дальнейшего развития показывает, что адаптация Регламента к новым технологиям должна сочетаться с пропорциональным распределением административной нагрузки с учетом особенностей различных субъектов и сохранением высокого уровня защиты персональных данных и фундаментальных прав.

[4] Предложение Европейской комиссии о принятии Регламента в части упрощения цифрового нормативного регулирования (Digital Omnibus) от 19 ноября 2025 г., COM (2025) 837 final, процедура 2025/0360(COD).

BGP LITIGATION

комплексная
правовая
поддержка

ДЦ «Империя», Пресненская наб., д. 6, стр. 2
г. Москва, Россия 123112

+7 (495) 777 28 20 office@bgplaw.com bgplaw.com

Александра Курдюмова

Партнер, адвокат
MENA Desk, финтех, интеллектуальная собственность и технологии

alexandra.kurdiumova@bgplaw.com

Арсений Топадзе

Советник, адвокат
Защита данных и цифровое регулирование

arseniy.topadze@bgplaw.com

Александра Сокольникова

Юрист
Финтех и международные проекты

aleksandra.sokolnikova@bgplaw.com

Мария Константинова

Младший юрист
Защита данных и цифровое регулирование

mariia.konstantinova@bgplaw.com