УДК 342.7:004.738.5

ПРАВОВЫЕ ПРЕДЕЛЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦИФРОВЫХ СЕРВИСАХ

Автор: _____

Организация: _____

Аннотация: В статье рассматриваются правовые пределы обработки персональных данных в цифровых сервисах. На основе Конституции Российской Федерации, Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", положений КоАП РФ и разъяснений уполномоченного органа анализируются ключевые условия законной обработки данных: наличие правового основания, соответствие цели обработки, ограничение объема данных, информирование субъекта и организационная ответственность оператора. Особое внимание уделено проблеме формального согласия пользователя, которое в цифровой среде часто превращается в техническую отметку, а не в осознанное волеизъявление. Сделан вывод о необходимости перехода от модели накопления данных к модели минимизации, доказуемой правомерности и понятной коммуникации с субъектом персональных данных.

Ключевые слова: персональные данные, цифровые сервисы, согласие субъекта, оператор персональных данных, неприкосновенность частной жизни, административная ответственность, Роскомнадзор.

LEGAL LIMITS OF PERSONAL DATA PROCESSING IN DIGITAL SERVICES

Abstract: The article examines the legal limits of personal data processing in digital services. The analysis is based on the Constitution of the Russian Federation, Federal Law No. 152-FZ "On Personal Data", administrative liability rules and explanations of the competent authority. The paper focuses on lawful grounds for processing, purpose limitation, data minimization, transparency for the data subject

and organizational responsibility of the operator. The author concludes that digital services should move from excessive data accumulation to a model of demonstrable legality and clear interaction with users.

Keywords: personal data, digital services, consent, data controller, privacy, administrative liability, data protection.

Введение

Цифровой сервис получает от пользователя не только имя, номер телефона или адрес электронной почты. В момент регистрации, оплаты, авторизации через социальную сеть или использования мобильного приложения он собирает технические идентификаторы, историю действий, данные устройства, сведения о местоположении, платежные признаки и поведенческие параметры. Юридическая проблема состоит в том, что такой массив сведений почти всегда связан с конкретным человеком прямо или косвенно. Поэтому обработка данных в цифровой среде не может рассматриваться как чисто технический процесс.

Конституционная основа защиты частной жизни закреплена в статьях 23 и 24 Конституции Российской Федерации. Эти положения задают общий предел для любой деятельности по сбору, хранению, использованию и распространению сведений о лице. Федеральный закон N 152-ФЗ конкретизирует данный предел через понятие персональных данных, правовые основания обработки, обязанности оператора и права субъекта данных. В юридическом смысле оператор цифрового сервиса действует не свободно, а в рамках специального режима, где каждое действие с данными должно иметь цель, основание и разумный объем.

Актуальность темы связана с тем, что в повседневной цифровой практике согласие пользователя часто используется как универсальное объяснение любой обработки. Пользователь ставит отметку в форме, продолжает пользоваться

сайтом или нажимает кнопку регистрации, но не всегда понимает, какие именно сведения собираются, кому передаются и сколько времени хранятся. В результате формальное согласие не всегда обеспечивает реальную защиту права на частную жизнь.

Цель статьи - определить правовые пределы обработки персональных данных в цифровых сервисах и показать, какие условия позволяют считать такую обработку правомерной. Для достижения цели используются формально-юридический метод, анализ нормативных актов и сравнительное сопоставление типовых обязанностей оператора с практикой цифровых сервисов.

1. Нормативная основа обработки персональных данных

Российская модель защиты персональных данных строится на сочетании конституционных гарантий и специального законодательства. Статья 23 Конституции Российской Федерации закрепляет право каждого на неприкосновенность частной жизни, личную и семейную тайну, а также тайну сообщений. Статья 24 запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Эти нормы важны не только как декларация, но и как критерий оценки любой цифровой обработки данных.

Федеральный закон N 152-ФЗ определяет персональные данные как любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу. Для цифровых сервисов это означает широкий охват: персональными данными становятся не только сведения из анкеты, но и наборы цифровых признаков, если они позволяют выделить конкретного пользователя. Сервис не вправе уходить от закона только потому, что не хранит паспортные данные или домашний адрес.

Закон устанавливает принципы обработки: законность и справедливость, ограничение обработки конкретными и законными целями, недопустимость

избыточности, точность данных, хранение не дольше необходимого срока. Эти принципы имеют самостоятельное значение. Даже при наличии согласия нельзя собирать сведения, которые не нужны для заявленной цели, хранить их бессрочно или использовать для целей, о которых субъект не был надлежащим образом проинформирован.

Отдельное значение имеет статус оператора. Оператором признается лицо, которое организует или осуществляет обработку персональных данных и определяет цели, состав данных и действия с ними. Для сайта, мобильного приложения, образовательной платформы, маркетплейса или CRM-системы этот статус возникает не из названия организации, а из фактического контроля над данными. Если сервис сам определяет, какие сведения собирать и зачем, он несет обязанности оператора.

2. Согласие субъекта и другие правовые основания

На практике согласие субъекта персональных данных остается самым заметным основанием обработки, но не единственным. Закон допускает обработку данных и в иных случаях: для исполнения договора, выполнения предусмотренных законом обязанностей, защиты жизни и здоровья, осуществления прав и законных интересов оператора или третьих лиц при условии, что не нарушаются права субъекта. Поэтому юридически корректная модель начинается не с автоматического запроса согласия, а с определения конкретного основания для каждой цели обработки.

В цифровом сервисе одна регистрационная форма часто прикрывает разные процессы: создание аккаунта, рассылку, аналитику поведения, персонализацию интерфейса, передачу данных платежному провайдеру, хранение логов безопасности. Эти процессы отличаются по цели и правовому основанию. Например, обработка данных для исполнения пользовательского

договора не равна обработке данных для рекламной рассылки. Их нельзя безоговорочно объединять одним общим согласием.

Согласие должно быть конкретным, информированным и сознательным. Из этого следует, что длинный текст политики, спрятанный за ссылкой внизу страницы, сам по себе не гарантирует законность. Пользователь должен понимать, какие категории данных обрабатываются, для какой цели, кем, в течение какого срока и какие действия он вправе совершить. Чем чувствительнее данные и чем шире передача третьим лицам, тем выше требования к ясности коммуникации.

Особую проблему создает практика связанности согласия с доступом к сервису. Если пользователь вынужден согласиться на необязательную рекламную обработку, иначе он не получает основную услугу, такое согласие может потерять признак свободного волеизъявления. Для оператора безопаснее разделять обязательную обработку, без которой сервис не работает, и дополнительную обработку, например маркетинговую рассылку или профилирование.

3. Пределы допустимой обработки в цифровой среде

Правовые пределы обработки персональных данных определяются не только наличием формального основания. Их задает совокупность критериев: цель, объем, срок, безопасность, прозрачность и возможность субъекта реализовать свои права. Если хотя бы один из этих элементов отсутствует, обработка становится уязвимой с точки зрения закона и контроля.

Первый предел - целевой. Данные собираются для конкретной, заранее определенной и законной цели. Цифровой сервис не вправе сначала накопить максимум сведений, а затем искать им полезное применение. Такая логика противоречит принципу ограничения цели. Для оператора это означает

необходимость описывать процессы обработки до запуска формы, приложения или интеграции с внешним сервисом.

Второй предел - количественный. Сервис должен собирать только те сведения, которые необходимы для заявленной цели. Например, для отправки электронного чека нужен адрес электронной почты, но не всегда нужен день рождения. Для доставки товара требуется адрес, но не обязательно постоянное хранение всех прежних адресов после завершения отношений. Избыточность данных повышает риск нарушения закона и увеличивает последствия утечки.

Третий предел - временной. Персональные данные не должны храниться дольше, чем требуется для цели обработки, если иной срок не предусмотрен законом или договором. В цифровой практике этот принцип часто нарушается из-за отсутствия регламентов удаления, архивирования и обезличивания. У оператора должна быть не только политика конфиденциальности, но и внутренняя процедура прекращения обработки после достижения цели.

Четвертый предел - организационный. Законная обработка требует распределения ответственности внутри компании: кто отвечает за согласия, кто контролирует доступы, кто ведет учет поручений обработчикам, кто реагирует на запрос субъекта, кто фиксирует инциденты. Без такой системы даже правильно написанная политика остается внешним документом, который не подтверждает реальное соблюдение закона.

Таблица 1. Основные правовые пределы обработки данных в цифровом сервисе

Предел обработки	Юридическое содержание	Практическое действие оператора
Цель	Данные используются только для заранее определенной цели.	Разделить цели: регистрация, договор, рассылка, аналитика, безопасность.
Объем	Нельзя собирать больше данных, чем нужно для цели.	Убрать лишние поля из форм, сократить обязательные данные.

Предел обработки	Юридическое содержание	Практическое действие оператора
Срок	Хранение допустимо только до достижения цели или окончания законного срока.	Установить сроки удаления, архивирования или обезличивания.
Прозрачность	Субъект должен понимать, кто и зачем обрабатывает его данные.	Сделать понятную политику и отдельные согласия для разных целей.
Ответственность	Оператор обязан доказать законность и безопасность обработки.	Вести внутренние регламенты, журналы доступов, учет поручений и запросов.

4. Ответственность оператора и контрольные риски

Административная ответственность за нарушение законодательства о персональных данных предусмотрена статьей 13.11 КоАП РФ. Норма охватывает разные составы: обработку без законного основания, нарушение правил согласия, невыполнение обязанности по опубликованию или обеспечению доступа к политике обработки данных, нарушение требований к локализации, невыполнение обязанности по уточнению, блокированию или уничтожению данных. Для цифрового сервиса это означает, что риск возникает не только при утечке, но и при ошибках в документах, форме согласия или внутреннем порядке обработки.

Контрольный риск усиливается тем, что цифровой сервис обычно взаимодействует с несколькими участниками: хостингом, платежным сервисом, рассыльщиком, системой аналитики, CRM, подрядчиком технической поддержки. Передача данных таким лицам требует правового оформления. Оператор должен понимать, действует ли внешний участник как самостоятельный оператор, как лицо, осуществляющее обработку по поручению, или как технический посредник с доступом к данным.

Отдельного внимания требует уведомление Роскомнадзора о намерении обрабатывать персональные данные. Уполномоченный орган разъясняет, что оператор до начала обработки обязан уведомить его о такой обработке, если нет

предусмотренного законом исключения. Следовательно, запуск сайта с формами сбора данных, личного кабинета или приложения должен сопровождаться не только публикацией политики, но и проверкой обязанности по уведомлению.

Практическая ошибка многих сервисов состоит в том, что документы готовятся после запуска обработки. Сначала создается форма регистрации, подключается аналитика, запускается рассылка, а затем появляется политика. Юридически правильный порядок обратный: сначала определяется карта данных, цели и основания, затем готовятся документы, настраиваются технические ограничения, и только после этого начинается обработка.

5. Права субъекта персональных данных

Правовые пределы обработки раскрываются также через права субъекта. Пользователь вправе получать информацию об обработке своих данных, требовать уточнения, блокирования или уничтожения данных при наличии оснований, отзывать согласие, обращаться к оператору и в уполномоченный орган. Эти права должны быть реализуемыми не только на бумаге. Если политика содержит адрес для обращений, но компания фактически не обрабатывает запросы, соблюдение закона становится формальным.

Для цифрового сервиса удобным решением является отдельный канал для запросов по персональным данным: электронная почта, форма в личном кабинете или иной фиксируемый способ обращения. Внутри организации должен быть определен срок реакции и лицо, ответственное за проверку основания запроса. Особенно важно отличать удаление аккаунта от прекращения всех операций с данными: отдельные сведения могут сохраняться по закону, договору или для защиты прав оператора, но это должно быть объяснимо и документально подтверждено.

Субъект не обязан разбираться в архитектуре сервиса, сторонних интеграциях и технических логах. Поэтому обязанность оператора состоит в переводе сложной обработки на понятный юридический язык. Чем проще пользователю найти сведения о целях, сроках, получателях и способах отзыва согласия, тем ниже риск конфликта и претензий со стороны контролирующих органов.

6. Предложения по совершенствованию практики

Для повышения уровня правовой определенности цифровым сервисам целесообразно использовать модель документированной обработки. Она включает карту персональных данных, разделение целей обработки, учет правовых оснований, перечень получателей данных, сроки хранения, порядок удаления и перечень технических мер защиты. Такой подход не требует избыточной бюрократии, но позволяет доказать, что оператор действует осознанно и системно.

Первое практическое предложение - отказаться от универсального согласия на все действия с данными. Более корректной является модульная модель: отдельное основание для исполнения договора, отдельное согласие на маркетинговую рассылку, отдельное согласие на передачу данных третьим лицам, отдельное информирование о файлах cookie и аналитике при необходимости. Это повышает качество волеизъявления и снижает риск признания согласия неконкретным.

Второе предложение - включать принцип минимизации в техническое задание на разработку сервиса. Юрист не должен подключаться только на этапе проверки политики. Он должен участвовать в проектировании формы регистрации, личного кабинета, CRM-процессов и интеграций. Тогда требование закона влияет на архитектуру обработки, а не остается приложением к уже работающему продукту.

Третье предложение - регулярно проверять фактическую обработку данных. Политика может устареть после подключения новой аналитики, смены платежного провайдера, запуска партнерской программы или добавления мобильного приложения. Поэтому комплаенс в сфере персональных данных должен быть не разовой подготовкой документов, а периодической проверкой соответствия документов реальным процессам.

Заключение

Обработка персональных данных в цифровых сервисах является правомерной только при наличии совокупности условий: законного основания, конкретной цели, ограниченного объема данных, понятного информирования субъекта, установленного срока хранения и организационной системы ответственности. Формальная отметка о согласии не заменяет эти условия и не освобождает оператора от обязанности соблюдать принципы обработки.

Правовые пределы обработки следует понимать как работающую систему ограничений, а не как набор шаблонных документов. Оператор цифрового сервиса должен заранее определить, какие данные он собирает, зачем, на каком основании, кому передает и когда прекращает обработку. Именно такая модель соответствует конституционной защите частной жизни и специальным требованиям законодательства о персональных данных.

Для правоприменительной практики ключевым становится переход от декларативного согласия к доказуемой правомерности обработки. Чем подробнее оператор может подтвердить цели, основания, объем, сроки и меры защиты, тем устойчивее его позиция при обращении субъекта, проверке или споре. В цифровой среде защита персональных данных становится не только юридической обязанностью, но и условием доверия пользователя к сервису.

Список источников

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993, с изменениями, одобренными в ходе общероссийского голосования 01.07.2020. URL: https://www.constitution.ru/10003000/10003000-4.htm (дата обращения: 02.06.2026).
2. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных". URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 02.06.2026).
3. Кодекс Российской Федерации об административных правонарушениях: статья 13.11 "Нарушение законодательства Российской Федерации в области персональных данных". URL: https://www.consultant.ru/document/cons_doc_LAW_34661/1f421640c6775ff67079ebde06a7d2f6d17b96db/ (дата обращения: 02.06.2026).
4. Роскомнадзор. Часто задаваемые вопросы в сфере персональных данных. URL: https://rkn.gov.ru/activity/personal-data/questions/ (дата обращения: 02.06.2026).
5. ГОСТ Р 7.0.7-2021. Система стандартов по информации, библиотечному и издательскому делу. Статьи в журналах и сборниках. Издательское оформление. URL: https://ifap.ru/library/gost/7072021.pdf (дата обращения: 02.06.2026).
6. Klymenko O., Kosenkov O., Meisenbacher S., Elahidoost P., Mendez D., Matthes F. Understanding the Implementation of Technical Measures in the Process of Data Privacy Compliance: A Qualitative Study. 2022. URL: https://arxiv.org/abs/2208.08671 (дата обращения: 02.06.2026).
7. Amaral O., Azeem M. I., Abualhaija S., Briand L. NLP-based Automated Compliance Checking of Data Processing Agreements against GDPR. 2022. URL: https://arxiv.org/abs/2209.09722 (дата обращения: 02.06.2026).