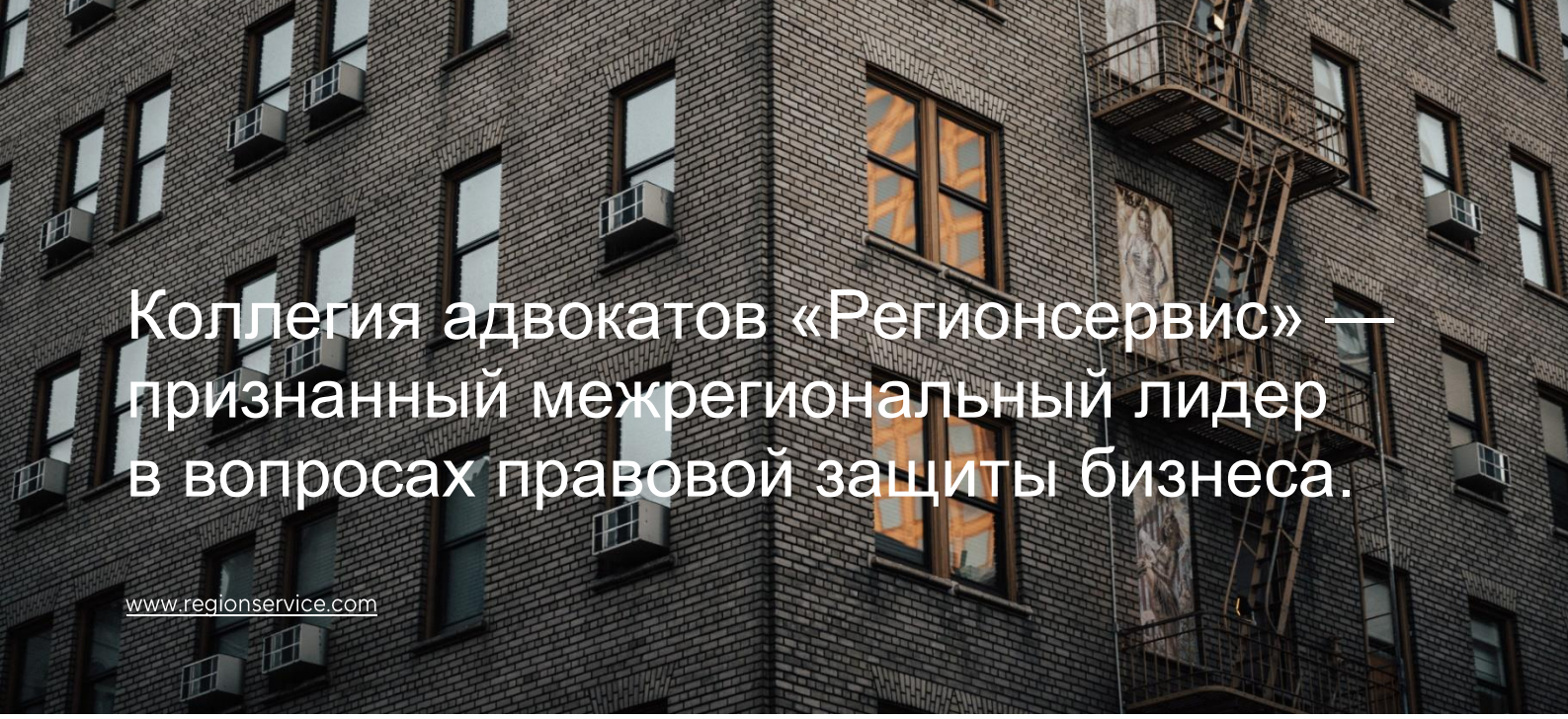

# Коллегия адвокатов «Регионсервис» — признанный межрегиональный лидер в вопросах правовой защиты бизнеса.

www.regionservice.com

**Legal Alert**[1]

**3 декабря 2024 года**

## ОБЛАЧНЫЕ СЕРВИСЫ И ЗАОБЛАЧНЫЕ СРОКИ: НОВЫЕ ПРАВИЛА В ЦИФРОВОЙ СФЕРЕ

30 ноября 2024 года принят Федеральный закон № 421-ФЗ, вводящий изменения в Уголовный кодекс Российской Федерации. В рамках нового закона добавлена статья 272.1, которая устанавливает уголовную ответственность за незаконный оборот персональных данных. Рассмотрим ключевые положения этой статьи, связанные риски и рекомендации для юридической практики.

### ОБЩИЕ ПОЛОЖЕНИЯ

Статья 272.1 УК РФ вводит ответственность за незаконное использование, передачу, сбор, хранение или предоставление доступа к персональным данным (ПД), если такие данные были получены:

- в результате неправомерного доступа к компьютерной информации;
- иным незаконным путём.

Особенность нормы заключается в том, что наказуемым является даже хранение персональных данных, полученных незаконным путём, вне зависимости от наличия цели распространения. Это вызывает вопросы относительно возможного широкого толкования понятия «иным незаконным путём», что может привести к презумпции незаконности данных при отсутствии доказательств их законного происхождения.

### КВАЛИФИЦИРУЮЩИЕ ПРИЗНАКИ

Статья предусматривает повышенную ответственность за деяния, совершённые с отягчающими обстоятельствами, включая:

- использование служебного положения;
- действия, совершённые группой лиц;

[1] Данный материал подготовлен исключительно в информационных целях и не является юридической консультацией или заключением.

- причинение значительного ущерба.

Особое внимание привлекает часть 4 статьи, устанавливающая уголовную ответственность за трансграничную передачу персональных данных. Это создаёт дополнительные риски для использования облачных сервисов и серверов, расположенных за границей. Максимальное наказание за такие деяния достигает 8 лет лишения свободы.

## ИСКЛЮЧЕНИЯ

Закон предусматривает, что норма статьи 272.1 не распространяется на обработку персональных данных физическими лицами для личных и семейных нужд. Однако остаётся вопрос, как трактовать ситуации, когда обработка данных осуществляется для иных целей, например, в рамках профессиональной деятельности юристов.

## ВТОРОЙ СОСТАВ ПРЕСТУПЛЕНИЯ

Дополнительно статья вводит уголовную ответственность за создание или обеспечение функционирования программ, заведомо предназначенных для незаконного хранения, передачи или распространения персональных данных. Это касается, в частности, программ и ботов, работающих в мессенджерах, таких как Telegram.

## ПОТЕНЦИАЛЬНЫЕ РИСКИ

1. Широта формулировок

Включение фразы «иной незаконный путь» позволяет трактовать статью достаточно широко. На практике это может привести к презумпции незаконного происхождения данных, если законный источник их получения не установлен.

2. Трансграничная передача данных

Компании, использующие иностранные облачные сервисы или передающие данные за границу, могут столкнуться с серьёзными рисками, если такие действия будут признаны нарушающими закон.

3. Практика юридической работы

Юристы и адвокаты, собирающие персональные данные для подачи исков или представления интересов клиентов, должны быть особенно осторожны. Использование сомнительных источников данных, например сервисов автоматического поиска информации, теперь может привести к уголовной ответственности.

4. Конкуренция с другими статьями УК РФ

Вопрос остаётся открытым: как статья 272.1 будет соотноситься со статьёй 137 УК РФ, регулирующей нарушение неприкосновенности частной жизни? На практике статья 137 может утратить своё значение, учитывая более широкий охват новой нормы.

## РЕКОМЕНДАЦИИ

1. Провести аудит процессов обработки данных

Проанализируйте внутренние процедуры сбора, хранения и обработки персональных данных. Убедитесь, что все данные получены законным способом, и задокументируйте их происхождение.

2. Пересмотреть использование сервисов

Откажитесь от использования сомнительных источников данных, таких как Telegram-боты, даже если ранее они применялись для профессиональных нужд.

3. Внедрить контроль за трансграничной передачей данных

Если компания использует облачные сервисы за границей, важно проанализировать их соответствие российскому законодательству и предусмотреть альтернативные решения.

4. Обучить сотрудников

Организуйте тренинги для персонала, включая юристов и ИТ-специалистов, чтобы они знали новые правила обработки данных и могли минимизировать риски.

5. Обновить соглашения и внутренние документы

Проверьте, соответствуют ли ваши соглашения с клиентами и партнёрами новым требованиям. Добавьте положения о документации законного источника персональных данных.

## ЗАКЛЮЧЕНИЕ

Принятие Федерального закона № 421-ФЗ значительно усложняет правила работы с персональными данными, вводя новые требования и ограничения. Адвокатам и юридическим лицам важно пересмотреть свои подходы к обработке данных, чтобы избежать рисков уголовной ответственности. Мы рекомендуем активно следить за практикой применения статьи 272.1 УК РФ и своевременно адаптировать внутренние процессы.

## КЛЮЧЕВЫЕ КОНТАКТЫ


**Владимир Агапов**

Советник Председателя Коллегии,
руководитель практики «Уголовно-правовая защита бизнеса»
v.agapov@regionservice.com
Тел.: +7 (495) 260-06-50

**Иван Ларионов**

Адвокат, старший юрист
i.larionov@regionservice.com
Тел.: +7 (343) 272 45 07