



Observatoire ARGA

МЕЖДУНАРОДНЫЙ АНАЛИТИЧЕСКИЙ ДОКЛАД

D-04. Удалённое уведомление INTERPOL

и коммерческие screening databases

Автор:

Сергей Храбрых - президент ARGA, PhD

Организация: Observatoire ARGA

Адрес для корреспонденции: 21 rue de l'Aviation, 64600 Anglet, France

Контакты: info@argaobservatory.org, +33 7 58 49 62 27

Сайт: www.argaobservatory.org

23 сентября 2026 года

Содержание

1. Резюме и основные выводы	3
2. Предмет, метод и границы исследования	4
3. Что доказывает удаление данных INTERPOL	5
4. Цепочка данных и распределение ответственности	6
5. Точность, полнота и исторический контекст	7
6. Исправление по статье 16 GDPR	8
7. Удаление по статье 17: основания и пределы	9
8. Ограничение обработки и возражение	10
9. Доступ и установление получателей	11
10. World-Check: публичная процедура и вопросы проверки	12
11. WorldCompliance: источник, профиль и самостоятельная обязанность	13
12. Судебные ориентиры и пределы аналогии	14
13. Великобритания: отдельный правовой маршрут	15
14. Подготовка доказательств и последовательность обращения	16
15. Клиентская копия и решение банка	17
16. Контраргументы и проверка устойчивости позиции	18
17. Условные сценарии и рекомендации	19
18. Заключение: что считать восстановлением информации	20
19. Источники и справочный аппарат	21

Срез источников: 23 сентября 2026 года. Ключевые слова: INTERPOL; CCF; коммерческие базы; World-Check; WorldCompliance; GDPR; исправление; удаление; получатели данных; банковская проверка.

1. Резюме и основные выводы

Удаление данных из информационной системы INTERPOL и исправление коммерческого профиля относятся к разным правовым процессам. Решение Комиссии по контролю за файлами INTERPOL (CCF) имеет значение для обработки данных в системе Организации. Коммерческий поставщик проверочной информации и использующий её банк должны отдельно оценивать собственную обработку. Поэтому положительный результат в INTERPOL следует рассматривать как существенное доказательство изменения информационной ситуации, но не как универсальное распоряжение всем участникам рынка удалить любые сведения о человеке. [1-3]

Основная проблема возникает при смешении прошлого и настоящего. Утверждение «уведомление было опубликовано» может оставаться исторически точным после удаления. Утверждение «лицо находится в действующем розыске INTERPOL» требует самостоятельного подтверждения на дату использования. Даже достоверная историческая запись может оказаться неполной для цели текущей проверки, если из профиля невозможно понять, что уведомление удалено. Юридическая оценка должна учитывать не только буквальную правильность отдельного предложения, но также назначение обработки, используемую категорию и контекст представления сведений.

Для субъектов данных центральное значение имеют статьи 16 и 17 Общего регламента ЕС о защите данных (GDPR). Первая позволяет требовать исправления неточности и дополнения неполных данных с учётом целей обработки. Вторая предусматривает удаление при установленных основаниях и сохраняет исключения. Дополнительные инструменты - доступ к данным, ограничение обработки на время проверки точности, возражение против определённых видов обработки и уведомление получателей об исправлении. Требование «удалить всё» часто менее убедительно, чем последовательное объяснение того, какое поле неверно, почему оно больше не нужно и какой способ устранения нарушения необходим. [3]

Две коммерческие системы рассматриваются через их собственные публичные документы: World-Check и WorldCompliance. Эти документы позволяют установить заявленные каналы обращения и некоторые принципы обращения с информацией, но не доказывают фактическую скорость исправления, полноту обновления клиентских копий или качество конкретных профилей. В докладе отсутствуют сведения из закрытых баз и статистика успешности жалоб. Выводы о незаконности отдельной записи возможны только после исследования самой записи и обстоятельств её использования. [4-6]

Предлагаемый подход состоит из трёх связанных задач: установить точный статус исходных данных; добиться соразмерного изменения коммерческой записи; проверить, какие получатели получили обновление и требуется ли отдельное исправление у них. Завершение первой задачи не подтверждает выполнение двух остальных. Аналогично, исправление базы не равнозначно восстановлению банковского обслуживания: решение клиента поставщика может опираться на другие сведения и правовые основания. Практический результат нужно описывать отдельно на каждом уровне, не подменяя юридически проверяемое изменение обещанием полного восстановления репутации.

2. Предмет, метод и границы исследования

Доклад D-04 - третий в согласованной последовательности ARGAs Observatory. Он развивает тему последствий удаления данных INTERPOL, но сосредоточен на коммерческом распространении информации и правах субъекта перед частными организациями. Национальные полицейские файлы, SIS и самостоятельные основания задержания не рассматриваются повторно. Предметом анализа являются персональные данные физического лица в коммерческом профиле, их использование при проверке клиента и механизмы исправления после документально подтверждённого изменения статуса INTERPOL.

Под screening database здесь понимается коммерческая информационная система, позволяющая проверять имена и связанные сведения по категориям риска. Это рабочее обозначение, а не отдельная законодательная категория. Нельзя выводить правовой режим только из названия продукта: один сервис может предоставлять санкционные сведения, сообщения о расследованиях, информацию о публичных функциях и иные данные, для которых различаются источники, цели и условия обработки. Также не следует приравнивать включение в коммерческую базу к включению в официальный санкционный список.

Используется правовой анализ первичных источников: нормативного текста GDPR, официальных документов INTERPOL, судебных решений в указанном объёме и разъяснений британского надзорного органа. Публичные политики поставщиков исследуются как заявления соответствующих организаций. Дата среза - 23 сентября 2026 года. Содержание решения, норма права, позиция поставщика и авторское предложение отделены друг от друга; условные сценарии не представляются реальными клиентскими делами.

Применимость GDPR не предполагается по факту европейского гражданства, наличия европейского банковского счёта или доступности сайта из ЕС. Необходимо установить территориальную связь, предусмотренную статьёй 3: например, обработку в контексте деятельности учреждения контролёра в Союзе либо соответствующее предложение товаров или услуг или наблюдение за поведением лиц в Союзе при установленных условиях. Последующее изложение прав по GDPR предполагает, что эта связь подтверждена. Для Великобритании выделены отдельные замечания; европейские нормы не выдаются за полный текст британского права. [3]

Ограничения исследования существенны для оценки выводов. Не исследованы подписные интерфейсы, внутренние инструкции банков, соглашения о поставке данных и журналы рассылки обновлений. Нет репрезентативной выборки отказов или решений по жалобам. Поэтому доклад устанавливает юридически обоснованные направления проверки, но не измеряет распространённость проблемы и не оценивает эффективность конкретного коммерческого продукта. Более сильные эмпирические утверждения потребовали бы иной исследовательской базы и отдельной методологии сбора данных.

3. Что доказывает удаление данных INTERPOL

Первый документ для коммерческого спора - подтверждение того, какое именно изменение произошло в INTERPOL. Следует различать решение ССФ, сообщение о его исполнении и исчезновение открытой интернет-страницы. Отсутствие страницы в публичном поиске само по себе не устанавливает содержание закрытой информационной системы, основания удаления и дату прекращения обработки. Убедительная позиция требует документа, позволяющего связать изменение с конкретным лицом и конкретными данными. По официальному описанию INTERPOL, при удалении страны уведомляются для обновления национальных сведений; в соответствующих случаях может выдаваться подтверждающий сертификат. Это описание не устанавливает автоматического исполнения коммерческими поставщиками. [1-2]

Не менее важно правильно изложить предмет решения. Удаление может отражать несоответствие обработки правилам INTERPOL, а не разрешение уголовного обвинения по существу. Из него нельзя без дополнительных оснований выводить оправдание, прекращение национального дела или ложность каждого сообщения о расследовании. Если доступная мотивировка ограничена, отсутствие подробностей нельзя заполнять благоприятной догадкой. В обращении допустимо сообщить установленный результат и отдельно отметить, что более широкие обстоятельства документом не подтверждаются.

Для исправления текущего статуса полная публичная реконструкция уголовного дела может и не понадобиться. Если коммерческий профиль продолжает прямо обозначать уведомление как действующее, ключевой вопрос состоит в подтверждении его удаления и в совпадении личности. Требование исправить это конкретное утверждение не тождественно требованию признать заявителя невиновным. Такая постановка позволяет избежать ненужного спора о событиях, которые ССФ не рассматривала и которые поставщик не уполномочен разрешать как уголовный суд.

В то же время удаление одной записи не исключает существования другой. Необходимо сопоставлять номера, даты, категории и юрисдикции, а не только фамилию. В условном случае старое уведомление может быть удалено, тогда как профиль дополнительно ссылается на независимое судебное решение. Исправление первого основания не устраняет автоматически второе. Контролёр, однако, должен объяснить, какое утверждение он сохраняет и почему подтверждение удаления не меняет его содержания или актуальности. Общая ссылка на «негативную информацию» недостаточна для предметной проверки заявителем.

Практически целесообразно составить краткую хронологию: исходное событие, дата документа ССФ, дата подтверждённого исполнения, дата спорной версии профиля и дата последующего использования. Такая хронология не превращается в доказательство сама по себе; каждое существенное звено должно иметь источник. Её назначение - выявить, какая версия существовала в момент решения банка и мог ли поставщик уже располагать обновлением. Это особенно важно, когда профиль впоследствии исправлен: нынешнее состояние базы не отвечает на вопрос о точности ранее переданной информации.

4. Цепочка данных и распределение ответственности

Один информационный эпизод может породить несколько самостоятельных записей: официальный источник, публикацию средства массовой информации, коммерческий профиль, результат проверки и внутреннее банковское досье. Исправление на одном уровне не гарантирует технической синхронизации остальных. Для юридической работы полезнее установить каждую операцию и её участника, чем использовать обобщённое выражение «данные остались в интернете». У каждого звена могут различаться цель, срок хранения и роль в отношении персональных данных.

По статье 4 GDPR контролёр определяет цели и средства обработки, а обработчик действует от его имени. Название стороны в договоре важно, но не заменяет оценки фактических функций. Поставщик, самостоятельно отбирающий источники и формирующий категории профиля, и банк, определяющий порядок проверки клиентов, могут быть самостоятельными контролёрами. Возможность иной конструкции не исключена, однако нельзя автоматически объявлять их совместными контролёрами только потому, что между ними передаются данные. Для такой квалификации необходимо исследовать участие в определении конкретной обработки. [3]

Это разграничение влияет на содержание требований. К поставщику обращаются по поводу профиля, его категорий, источников, распространения и обновления. К банку - по поводу имеющихся у него персональных данных, их актуальности и использования при принятии решения. Издателю направляют отдельное обращение, если неточность содержится в публикации. Пересылка одного общего письма всем адресатам может оставить без ответа существенные вопросы: каждый сочтёт, что оспаривается чужое действие. Лучше описывать общую хронологию одинаково, но формулировать предмет требования с учётом роли получателя.

Следует различать содержание и передачу. Поставщик может исправить действующий профиль, но необходимо выяснить, было ли изменение доведено до получателей в случаях, охватываемых статьёй 19. Банк может получить обновление, но продолжить хранить прежний отчёт как документ ранее проведённой проверки. Само архивное сохранение и использование старого статуса для новой оценки - разные операции. Возможность законного хранения истории не отвечает автоматически на вопрос о допустимости её дальнейшего предъявления как текущей информации.

В доказательственной модели отдельное место занимает происхождение копии. Скриншот без даты и идентификатора продукта может не позволить определить контролёра или версию. Нужны доступные метаданные: название сервиса, дата выгрузки, идентификатор профиля, используемая организация и содержание спорного поля. Эти сведения следует получать законным путём, не нарушая ограничения доступа. Наличие лицензии у банка не даёт заявителю права самостоятельно входить в чужую подписную систему, но не устраняет его права запрашивать собственные персональные данные у соответствующего контролёра.

5. Точность, полнота и исторический контекст

Принцип точности статьи 5(1)(d) GDPR требует принимать разумные меры для исправления или удаления неточных данных с учётом целей обработки. Он действует вместе с ограничением цели, минимизацией и ограничением хранения. Поэтому проверка коммерческого профиля не сводится к вопросу, существовал ли когда-либо процитированный источник. Нужно выяснить, какое сообщение получает пользователь базы сегодня и насколько оно соответствует установленному положению лица. [3]

Предлагается различать пять элементов записи: идентификацию человека; описание события; его процессуальный статус; коммерческую категорию; дату актуальности. Ошибка в любом из них может изменить смысл остальных. Верная фамилия не компенсирует неверную дату рождения. Достоверное сообщение о предъявлении обвинения не подтверждает осуждение. Исторически точное упоминание INTERPOL не оправдывает активную отметку о действующем уведомлении. Эта типология является авторским инструментом анализа, а не классификацией, обязательной для всех поставщиков.

Особую сложность представляет формально верный, но неполный текст. Например, в условной записи сохранено сообщение о публикации уведомления с правильной датой, но профиль предназначен для текущей проверки и не содержит известного поставщику последующего удаления. Возможное требование здесь - дополнить данные и изменить текущую категорию. Следует показать, почему пропуск влияет на цель обработки, а не ограничиваться общим заявлением о репутационном ущербе. При этом содержание дополнения должно соответствовать документу: «удалено из системы» не заменяется формулировкой «обвинение признано необоснованным», если такого вывода нет.

Другой случай - точный исторический архив, где дата и последующее изменение ясно обозначены, а данные не предлагаются как подтверждение действующего розыска. Требование удаления такой записи нуждается в отдельном обосновании по статье 17: например, утрата необходимости, незаконность обработки или результат возражения. Одного несогласия с неблагоприятным историческим фактом недостаточно. Но и слово «архив» не создаёт универсального освобождения от GDPR: сохраняются вопросы о цели, объёме, сроке и доступе.

Наконец, нужно учитывать различие между фактами и оценками. Категория риска может отражать аналитическое суждение поставщика, однако это не делает лежащие в её основе персональные данные неподконтрольными проверке. Заявитель может оспаривать неверную фактическую предпосылку, смешение статусов или отсутствие существенного обновления. Требование раскрыть и проверить такую предпосылку точнее, чем требование присвоить «нулевой риск»: законодательство о данных не гарантирует желаемую коммерческую оценку при любых обстоятельствах.

6. Исправление по статье 16 GDPR

Статья 16 предоставляет право без неоправданной задержки исправить неточные персональные данные и дополнить неполные, включая дополнительное заявление, с учётом целей обработки. Для рассматриваемой темы это часто наиболее прямой инструмент: он позволяет требовать замены неверного действующего статуса, уточнения события или добавления подтверждённого результата ССФ без необходимости отрицать весь исторический материал. Исправление не следует описывать как менее значимую альтернативу удалению: иногда именно оно точнее устраняет нарушение. [3]

Предмет обращения нужно сделать воспроизводимым. Полезно привести спорную формулировку, указать её местоположение или поле, назвать дату версии и предложить корректное содержание. Затем объяснить, какой документ подтверждает изменение. Если профиль недоступен, следует обозначить источник сведений о предполагаемой ошибке и одновременно запросить доступ. Нельзя приписывать базе конкретную запись только на основании отказа банка или предположения посредника: сначала устанавливается факт обработки либо прямо указывается, что он пока не подтверждён.

Предлагаемое исправление должно различать минимум два вопроса: что удалить как неверное и что добавить как необходимый контекст. Например, документально подтверждённое прекращение обработки уведомления может требовать снятия активной отметки и отражения даты удаления. Если заявитель просит также удалить связанные сообщения о национальном расследовании, это отдельная часть обращения с собственным основанием. Разделение требований позволяет оценить частичное удовлетворение и оспорить отказ по конкретному пункту, не теряя уже достигнутого результата.

Дополнительное заявление субъекта имеет практическую ценность, но не должно использоваться как универсальная замена исправлению установленной ошибки. Когда текущий статус объективно неверен, размещение рядом фразы «заявитель не согласен» может оставить основную неточность без изменения. Напротив, при неполноте или действительно спорном обстоятельстве согласованное пояснение способно уточнить смысл. Правовая оценка зависит от того, устранена ли проблема для цели обработки, а не от самого факта добавления текста.

Ответ контролёра следует проверять по содержанию. Сообщение «профиль обновлён» ещё не показывает, какие поля изменены, когда это произошло и осталась ли прежняя категория. Разумно запросить подтверждение результата в отношении собственных данных и информацию об уведомлении получателей. Это не означает безусловного права на внутренний программный код или полный коммерческий журнал: необходимо отделять сведения, нужные для осуществления прав, от неопределённого требования раскрыть всю инфраструктуру поставщика.

7. Удаление по статье 17: основания и пределы

Статья 17 GDPR предусматривает несколько самостоятельных оснований удаления. В контексте коммерческого профиля наиболее значимы утрата необходимости для цели обработки, незаконность обработки и успешное возражение при отсутствии преобладающих законных оснований. Если обработка основана на согласии, его отзыв также может иметь значение при отсутствии другого основания, но нельзя предполагать, что профессиональная проверочная база всегда использует согласие. Требование должно соотноситься с реально заявленным основанием обработки. [3]

Утрата необходимости требует анализа конкретной цели. Если единственным содержанием записи было действующее уведомление и этот статус прекращён, возникает вопрос, для чего сохраняется профиль или соответствующая категория. Однако сам по себе возраст информации не устанавливает ненужность, а коммерческий интерес к историческим сведениям не доказывает необходимость. Контролёру следует объяснить, почему требуются именно эти данные, в таком объёме и на такой срок. Заявитель, в свою очередь, может показать, что менее обременительное представление сведений позволяет достичь заявленной цели.

Незаконность обработки нельзя выводить исключительно из решения CCF. Возможные самостоятельные вопросы - отсутствие применимого основания статьи 6, нарушение дополнительных условий статьи 10, несоблюдение принципов точности или минимизации. Каждый из них нуждается в фактическом и правовом обосновании. Если определённые сведения подпадают под режим данных об уголовных осуждениях и правонарушениях, одного заявления о законном интересе по статье 6 недостаточно для завершения анализа: статья 10 устанавливает дополнительные условия. Их национальная конкретизация не исследуется здесь для всех государств ЕС. [3]

Исключения статьи 17(3) также требуют предметной оценки. Среди них - свобода выражения мнения и информации, соответствующая правовая обязанность, выполнение публичной задачи, определённые общественные и исследовательские цели, а также установление, осуществление или защита правовых требований. Нельзя автоматически переносить исключение для одной операции на весь профиль и всех получателей. Ссылка на потенциальный спор не объясняет бессрочное распространение любых сведений среди неопределённого круга клиентов.

Корректное требование может быть построено последовательно: удалить конкретные данные по указанному основанию; если контролёр считает удаление неприменимым, объяснить исключение и его объём; независимо от этого исправить неверный текущий статус и рассмотреть ограничение обработки на время проверки. Такая структура сохраняет юридическую определённость. Она не предполагает, что все альтернативы обязательно будут удовлетворены, но не позволяет отказу в полном удалении скрыть самостоятельный вопрос о точности.

8. Ограничение обработки и возражение

Спор о точности может продолжаться, пока запись используется для новых проверок. Статья 18(1)(a) GDPR предусматривает ограничение обработки на период, необходимый контролёру для проверки точности оспариваемых данных. Поэтому обращение целесообразно сопровождать самостоятельным требованием рассмотреть ограничение, указав конкретную неточность и доказательства. Это не автоматическое удаление и не универсальный запрет любых операций: режим ограниченной обработки имеет собственные условия. [3]

По статье 18(2), кроме хранения, дальнейшая обработка ограниченных данных допускается в предусмотренных случаях, в том числе с согласия субъекта, для правовых требований, защиты прав другого лица или по важным основаниям публичного интереса. До снятия ограничения субъект должен быть уведомлён. В коммерческом споре полезно выяснить, как ограничение отражено в отношении спорной записи и её передачи. Но без доступа к продукту нельзя заранее утверждать, что определённая отметка интерфейса обеспечивает соблюдение закона или, напротив, что отсутствие известной отметки доказывает нарушение.

Статья 21(1) относится к обработке на основаниях статьи 6(1)(e) или (f) и требует учитывать конкретную ситуацию субъекта. Аргументация может включать подтверждённое удаление уведомления, отсутствие актуального основания для прежней категории, несоразмерные последствия и возможность менее обременительного представления истории. Контролёр должен оценить наличие убедительных законных оснований, преобладающих над интересами, правами и свободами лица, либо оснований для правовых требований. Абсолютный режим возражения против прямого маркетинга нельзя переносить на AML-проверку. [3]

Ограничение и возражение решают разные задачи. Первое может сохранять положение на время проверки, второе направлено на прекращение определённой обработки с учётом её основания и индивидуальной ситуации. Смешение терминов способно привести к ответу не на тот вопрос. В письме лучше отдельно обозначить предмет каждого требования и указать, какие данные оно охватывает. Если речь идёт только об удалённом уведомлении, не следует без объяснения расширять требование на сведения, не связанные с ним.

Практическое значение имеет сохранение доказательств до изменения профиля. Заявителю может быть необходима прежняя версия для обоснования жалобы или убытков; контролёру - ограниченное хранение для защиты правовых требований. Поэтому требование немедленно уничтожить все следы обработки иногда противоречит интересу самого заявителя установить прошлое нарушение. Возможный выход - разграничить прекращение обычного распространения и обоснованное, ограниченное по цели сохранение доказательственного материала. Допустимость такого решения зависит от конкретного основания и не презюмируется.

9. Доступ и установление получателей

Доступ по статье 15 GDPR помогает перейти от предположений к проверяемой записи. Запрос может охватывать подтверждение обработки, собственные персональные данные, цели, категории, получателей, предполагаемый срок хранения или критерии его определения и доступную информацию об источнике, если данные получены не от субъекта. Это позволяет выяснить, спорит ли человек с устаревшим официальным статусом, пересказом публикации или самостоятельной категорией. Право получить копию персональных данных не следует без оговорок описывать как право получить весь коммерческий продукт. [3]

В деле C-154/21 Суд ЕС разъяснил значение сведений о получателях. Когда данные переданы или будут переданы, субъект в принципе имеет право знать конкретных получателей. Предоставление одних категорий допускается, если получателей невозможно установить либо контролёр докажет явную необоснованность или чрезмерность запроса. Этот вывод помогает адресовать последующие требования организациям, действительно получившим данные, но не гарантирует существование конкретного технического журнала или определённый формат выгрузки. Дело не касалось исправления профиля World-Check. [7]

Статья 19 связывает исправление, удаление и ограничение с уведомлением получателей, которым данные были раскрыты, кроме случаев невозможности или несоразмерных усилий. По запросу субъекту сообщают об этих получателях. Существенно различать фактического получателя спорных данных и любую организацию, имеющую подписку на продукт. Норма не должна пересказываться как обязанность разослать персональную историю всем клиентам поставщика независимо от передачи им информации. [3]

В обращении полезно разделить три вопроса: кому раскрывались данные; кому направлено сообщение об изменении; какие исключения применены и почему. Это авторская структура запроса, а не установленная форма. Она позволяет заметить неполный ответ: например, список категорий клиентов без объяснения невозможности назвать конкретных получателей либо подтверждение исправления без рассмотрения уведомления. При оценке ответа учитываются права других лиц и применимые ограничения; сами по себе коммерческая чувствительность и объём системы не заменяют юридическое обоснование.

Уведомление получателя не равнозначно доказанному изменению всех его систем. Получивший сообщение банк может иметь несколько связанных записей и собственные обязанности хранения. Если имеется основание полагать, что он продолжает использовать прежний статус, требуется самостоятельное обращение. На этом этапе сведения о дате уведомления особенно полезны: они позволяют поставить конкретный вопрос о том, какие данные использовались после получения обновления, не приписывая банку заранее установленную ошибку.

10. World-Check: публичная процедура и вопросы проверки

Публичное уведомление World-Check определяет Refinitiv Limited как контролёра в описанном контексте и предусматривает обращение за доступом, исправлением и рассмотрением удаления через contact@world-check.com с проверкой личности. Оно признаёт возможность ошибок и устаревания, одновременно связывая результат обращения с точностью, релевантностью и основаниями дальнейшей обработки. Включение в систему не предлагается считать само по себе неблагоприятным выводом; пользователям указывается на необходимость собственной проверки. Это изложение позиции поставщика, а не вывод о соблюдении требований в каждом деле. [4]

Для заявителя важнее не общее описание продукта, а ответ применительно к спорному полю. Если документ CCF относится к тому же лицу и той же записи, следует выяснить, какая категория останется после обновления, какое утверждение она выражает и на каком источнике основана. Возможны разные результаты: изменение текущего статуса, уточнение исторического описания, исключение отдельного основания или удаление профиля. Доклад не утверждает, что политика предусматривает обязательный одинаковый результат при любом удалении данных INTERPOL.

Проверка личности имеет понятную цель - не передать данные постороннему и не изменить профиль по ложному обращению. Однако объём дополнительно запрашиваемой информации также нуждается в обосновании. Разумно уточнить безопасный канал передачи и направлять только необходимое для идентификации и подтверждения полномочий представителя. Полный массив материалов уголовного дела не должен автоматически становиться первым вложением, если спор касается одного подтверждаемого статуса. Избыточная передача создаёт новые риски и затрудняет выделение доказательства, действительно относящегося к требованию.

Если поставщик указывает на независимый источник, нужно проверить, действительно ли он подтверждает сохраняемое утверждение. Сообщение о прежнем задержании не обязательно подтверждает действующее уведомление; публикация о расследовании не равнозначна приговору. Вопрос следует формулировать содержательно: какое именно положение профиля опирается на этот источник и почему обновление не меняет его точности или необходимости. Такой подход допускает сохранение правомерной исторической информации, одновременно не позволяя подменить одно событие другим.

После получения ответа целесообразно сопоставить результат с первоначальным запросом по каждому пункту. Подтверждены ли новые данные, рассмотрено ли требование об ограничении, решён ли вопрос уведомления получателей? Наличие официального канала обращения облегчает запуск процедуры, но не подтверждает её завершение. В отсутствие индивидуального ответа нельзя заявлять ни об отказе поставщика соблюдать закон, ни о фактическом восстановлении информации во всех клиентских копиях.

11. WorldCompliance: источник, профиль и самостоятельная обязанность

В уведомлении LexisNexis Financial Crime Compliance Solutions, обновлённом в декабре 2025 года, описываются обработка сведений для проверок, возможные права на доступ, исправление, удаление и ограничение с учётом применимого права. Указаны отдельные маршруты обращения для США и других юрисдикций. Поставщик заявляет, что не принимает решения за клиентов и что его данные не должны служить их единственным основанием. Эти положения характеризуют заявленную организацию сервиса; фактическое выполнение договорных требований клиентами в исследовании не проверялось. [5]

В разделе WorldCompliance на странице Consumer and Data Access Policies говорится о доступе и оспаривании ошибок; также отмечается, что из-за происхождения сведений у третьих лиц может потребоваться обращение к первоначальному источнику. Такой ответ необходимо анализировать отдельно от обязанности контролёра по применимому законодательству. Публичная политика не создаёт самостоятельного исключения из статьи 16 GDPR. Но её наличие также не доказывает, что поставщик откажется исправлять подтверждённую неточность в конкретном случае. [6]

Здесь возникают два разных предмета спора. Первый - содержание исходной публикации: например, неверно указанное лицо или сообщение о событии, которого не было. Второй - собственная обработка поставщика: неверная категория, отсутствие обновления или представление старого сообщения как текущего статуса. Исправление публикации способно помочь в обоих случаях, но ожидание решения издателя не всегда отвечает на самостоятельный вопрос о точности коммерческой записи. В обращении полезно прямо указать, какая часть требования относится к каждому уровню.

Если источник исторически точен, требование переписать его как никогда не существовавший материал может быть необоснованным. При этом коммерческий профиль может нуждаться в дополнении сведениями о последующем удалении уведомления. Отсутствие ошибки у издателя не исключает неполноты у агрегатора, использующего информацию для иной цели. Это аналитический вывод из разграничения операций и требований точности, а не судебное установление неправомерности рассматриваемого продукта.

Сопоставление двух поставщиков имеет ограниченную задачу: показать необходимость читать актуальную политику конкретного контролёра и не переносить процедуру одного сервиса на другой. Оно не является рейтингом качества. Для оценки реальной работы потребовались бы сопоставимые индивидуальные обращения, документы ответов и проверка последующих версий профилей. У ARGА в настоящем докладе не заявляется такая выборка; рекомендации основаны на нормах и документированных публичных маршрутах.

12. Судебные ориентиры и пределы аналогии

Судебная практика полезна, когда её правовой вывод соотнесён с предметом конкретного спора. Решение о поисковой выдаче не становится решением о подписной базе, а разъяснение права на получателей не доказывает причинную связь между записью и банковским отказом. В настоящем исследовании выделены три узких ориентира: доступ к получателям, оценка требования при заявленной неточности и условия компенсации. Каждый используется в пределах проверенного текста. [7-9]

C-154/21 непосредственно толкует общее право доступа и помогает установить адресатов дальнейших требований. Авторское применение к коммерческому screening состоит в том, что субъект может выяснять конкретных получателей, чтобы осуществить права на исправление и защиту. Из решения не следует обязанность поставщика угадать всех косвенных пользователей или назвать организации, никогда не получавшие данные. Требование должно оставаться связано с реальной обработкой, а исключения - оцениваться по установленному Судом стандарту. [7]

В C-460/20 рассматривалась поисковая деиндексация. Проверенные пункты 72-73 связывают результат с представленными релевантными и достаточными доказательствами явной неточности всего содержания либо его существенной части; когда неточность не очевидна из доказательств и отсутствует соответствующее судебное решение, обязанность удовлетворить требование не возникает на этом основании. Полный текст решения в ходе текущей проверки непосредственно получить не удалось; использование ограничено указанными официальными фрагментами. Специальный подход к поисковику не переносится на статью 16 как дополнительное универсальное условие исправления профиля. [8]

В C-300/21 Суд ЕС установил, что само нарушение GDPR недостаточно для компенсации, а возмещение нематериального вреда не может зависеть от достижения минимального порога серьёзности. Для требования по статье 82 остаются значимыми вред и причинная связь. Здесь использована официально опубликованная резолютивная часть; доклад не сообщает о присуждении конкретной суммы заявителю и не представляет дело как спор об INTERPOL. [3, 9]

Практический вывод состоит в необходимости разделять способы защиты. Для исправления неточного поля не требуется сначала доказать денежный убыток в размере закрытого контракта. Для компенсации, напротив, одного факта исправления после жалобы недостаточно: нужно установить нарушение, вред и связь между ними. Для пересмотра банковского решения необходимо понять, какие данные реально использовались. Объединение этих задач в одно недифференцированное требование ослабляет доказательственную позицию и создаёт ожидание результата, который соответствующая процедура не гарантирует.

13. Великобритания: отдельный правовой маршрут

Британский аспект нельзя оформлять простой заменой названия европейского надзорного органа на ICO. После реформ 2025-2026 годов необходимо проверять применимый UK GDPR, Data Protection Act 2018 и вступившие в силу изменения. Настоящий раздел ограничен двумя подтверждёнными вопросами: обработкой сведений об уголовных правонарушениях и процедурой жалоб контролёру. Он не является исчерпывающим обзором британского режима или всех его исключений. [10-12]

ICO разъясняет, что для обработки уголовных данных требуется не только общее основание, но также официальное полномочие либо соответствующая правовая авторизация с предусмотренными гарантиями. При отсутствии официального полномочия существенны условия DPA 2018. Страница ICO помечена как пересматриваемая в связи с Data (Use and Access) Act 2025; поэтому она используется для этого ограниченного разграничения, а не как подтверждение полной актуальности каждого элемента руководства. Для индивидуального дела конкретное условие должно быть проверено по действующей норме. [10]

По официальному сообщению ICO, новые требования к рассмотрению жалоб начали действовать 19 июня 2026 года. Организация должна обеспечить возможность подать жалобу о защите данных, подтвердить её получение в течение 30 дней, без неоправданной задержки предпринять надлежащие действия по рассмотрению, информировать заявителя и сообщить результат. Тридцатидневный срок относится к подтверждению получения, а не является обещанием окончательного разрешения спора или удаления профиля за этот период. [11-12]

Это различие следует отражать в календаре обращения. Запрос об осуществлении права и жалоба на его нарушение могут иметь разные процессуальные функции. Получение автоматического подтверждения не означает рассмотрения требования по существу; одновременно отсутствие окончательного решения на тридцатый день не позволяет без дополнительного анализа утверждать нарушение именно срока окончательного ответа. Для британского обращения сроки и возможные особенности соответствующего запроса необходимо сверять отдельно; правила статьи 12 EU GDPR ниже не заявляются как полное описание UK GDPR после реформы.

При трансграничном профиле нужно установить юридическое лицо, роль в обработке и применимый режим, а не выбирать юрисдикцию только по удобству формы на сайте. Один фактический эпизод может затрагивать несколько организаций, но это не даёт основания обещать одинаковую процедуру и результат в каждой стране. В докладе британский маршрут служит предупреждением о необходимости отдельной квалификации, сохраняя общий практический принцип: сначала конкретизировать запись и контролёра, затем выбрать право и средство защиты.

14. Подготовка доказательств и последовательность обращения

Первый этап - сохранить доступные документы в их исходном виде и составить перечень того, что каждый из них подтверждает. Решение ССФ подтверждает свой предмет; письмо банка - сообщённую банком причину или сам факт отказа; профиль - содержание определённой версии. Ни один документ не следует использовать вместо другого. Если источник сведений неясен, это фиксируется как пробел, который нужно закрыть запросом доступа, а не как доказанный факт использования определённой базы.

Второй этап - установить идентичность. Сопоставляются доступные идентификаторы лица, записи INTERPOL и коммерческого профиля. При совпадении распространённого имени дополнительное значение имеют дата рождения, гражданство, связанные организации и обстоятельства события. Используются только необходимые данные; сведения о родственниках или третьих лицах не включаются автоматически. Если спор вызван ложным совпадением, предметом требования становится неверная связь с человеком, а не только статус уведомления. Удаление правильной записи о другом лице не является необходимым результатом такого спора.

Третий этап - сформулировать требования по отдельным основаниям. Для EU GDPR это могут быть доступ по статье 15, исправление по статье 16, удаление конкретных данных по статье 17, ограничение по статье 18, уведомление получателей по статье 19 и возражение по статье 21 при применимом основании. Не требуется механически перечислять все статьи: каждое требование должно иметь свой предмет и объяснение. Избыточный набор несвязанных претензий затрудняет проверку ответа и может скрыть наиболее сильный довод.

Четвёртый этап - вести процессуальную хронологию. По статье 12 EU GDPR информация о действиях по запросу предоставляется без неоправданной задержки и, как правило, в течение месяца; при необходимости срок может быть продлён ещё на два месяца с уведомлением и объяснением в первый месяц. Это не гарантия успешного удаления или полного восстановления обслуживания за месяц. Если действий не принимают, существенны причины и информация о возможности жалобы и судебной защиты. При разумных сомнениях относительно личности контролёр может запросить дополнительную информацию для её подтверждения. [3]

Пятый этап - проверить результат, а не только факт переписки. Сопоставляются заявленные изменения и ответ по каждому спорному элементу; отдельно оцениваются уведомление получателей и положение у известного пользователя данных. Нерешённые вопросы переносятся в жалобу с хронологией, документами и конкретным предметом. Авторская рекомендация состоит в том, чтобы формировать короткое основное объяснение и упорядоченный доказательственный комплект, избегая эмоциональных обвинений и обещаний будущего судебного исхода.

Если ответ не устраняет предполагаемое нарушение, статья 77 GDPR предусматривает жалобу надзорному органу, в частности по месту обычного проживания, работы или предполагаемого нарушения. Статья 79 предусматривает судебную защиту против контролёра или обработчика без ущерба для административных и внесудебных средств. Выбор компетентного органа и суда требует оценки обстоятельств; наличие жалобы не

означает заранее установленной обязанности восстановить банковское обслуживание. Предмет обращения должен различать неточность, отказ в осуществлении права и требование компенсации, для которого отдельно оцениваются условия статьи 82. [3]

15. Клиентская копия и решение банка

Коммерческий профиль является информационным входом, а банковское решение - самостоятельным действием. Даже доказанное исправление поставщиком не показывает, что банк использовал именно эту запись или что она была единственным основанием отказа. Анализ должен начинаться с доступного объяснения банка и правомерно полученных собственных данных. Если банк не раскрывает подробности, нельзя автоматически заполнять пробел предположением о конкретном продукте или мотиве. Возможные законные ограничения раскрытия оцениваются отдельно по применимому праву.

После подтверждённого исправления заявитель может направить банку документ о новом статусе и попросить проверить актуальность собственных данных, обновить соответствующее поле и пересмотреть решение в пределах применимой процедуры. Эти просьбы различаются по правовой природе. Исправление персональных данных не создаёт само по себе общего права на любой финансовый продукт. Возможные права на определённый вид счёта, договорные обязанности и правила обжалования банковских действий требуют самостоятельной юрисдикционной оценки, которая не проводится в этом докладе.

Внутренняя копия прежнего отчёта может сохранять доказательство того, что организация проверяла клиента в определённую дату. Вопрос заключается в том, как она обозначена и используется после получения обновления. Если прежняя версия хранится как история, а текущая оценка учитывает исправление, ситуация отличается от повторного использования старого активного статуса. Просьба уничтожить весь архив способна не учитывать законные обязанности хранения; требование отделить историческую версию от действующего статуса может точнее соответствовать спору.

Если отказ сохраняется, полезно выяснить, какие вопросы остались нерешёнными после обновления. Это не обязательно означает право получить весь внутренний анализ рисков. Однако ответ может показать, что оспариваемый статус исправлен, а решение связано с иным обстоятельством. Для последующей защиты важно не смешивать доказанное нарушение данных и неудовлетворённое коммерческое ожидание. Оба могут быть значимы, но требуют разных норм и доказательств.

Причинная связь особенно важна при требовании компенсации. Нужны доступные сведения о времени передачи данных, версии профиля, дате решения и понесённых последствиях. Временная последовательность сама по себе ещё не устанавливает причину: отказ после публикации не доказывает отказ из-за неё. Вместе с тем прямое указание на ошибочный статус, повторение той же формулировки или документированное получение профиля могут быть значимыми элементами совокупной оценки. Их юридическая сила определяется в конкретном производстве, а не заранее в аналитическом докладе.

16. Контраргументы и проверка устойчивости позиции

Первый сильный контраргумент - историческая достоверность. Поставщик вправе указывать, что событие действительно имело место и не исчезает из истории после удаления уведомления. Ответ не должен отрицать очевидное. Следует установить, спорит ли заявитель с существованием события или с его текущим представлением. Если историческая запись точна и ясно дополнена последующим изменением, требование удаления нуждается в других основаниях; если прежний статус выдаётся за действующий, историческая достоверность не устраняет проблему.

Второй контраргумент - необходимость AML-проверки и предотвращения финансовых преступлений. Законная цель может оправдывать определённую обработку, но не доказывает необходимость любого объёма данных, любой категории или бессрочного распространения. Вопрос ставится конкретно: как спорное поле служит цели после обновления и существует ли менее обременительный способ представить релевантную историю? Доклад не устанавливает универсальный срок хранения и не предполагает, что все коммерческие поставщики несут те же обязанности, что и банк.

Третий контраргумент - сохранение независимых источников. Если профиль содержит несколько оснований, исчезновение одного не устраняет остальные. Проверка должна идти по каждому утверждению. При этом нельзя заменять источник, подтверждающий одно событие, ссылкой на любое другое неблагоприятное сообщение. В мотивированном ответе важна связь между фактом, категорией и целью. Согласие заявителя с сохранением одного исторического элемента не означает отказа от права исправить другой.

Четвёртый контраргумент - невозможность полного контроля над копиями. Поставщик не может обещать фактическое уничтожение каждого документа, уже находящегося у самостоятельного контролёра. Именно поэтому статья 19 говорит об уведомлении получателей и предусматривает исключения, а индивидуальная работа продолжается у известных пользователей данных. Нельзя превращать ограниченность технического контроля в полное отсутствие обязанностей, но нельзя и обещать универсальное исчезновение информации после одного письма.

Пятый контраргумент - недостаточность доказательств заявителя. Он требует честной оценки. Нечитаемое письмо, неподтверждённый перевод или документ о другом уведомлении могут не позволить контролёру проверить требование. Следует устранить недостаток, а не объявлять любой дополнительный вопрос злоупотреблением. Одновременно запрос доказательств должен оставаться связанным с проверяемым обстоятельством. Если документ однозначно подтверждает удаление конкретной записи, требование доказать невиновность по всему уголовному делу может относиться к иной задаче и нуждается в отдельном объяснении.

17. Условные сценарии и рекомендации

Все приведённые далее ситуации - авторские модели, а не сведения о клиентах ARGА или установленных нарушениях поставщиков. В первом сценарии профиль после подтверждённого удаления сохраняет действующую отметку INTERPOL. Основной маршрут - исправление конкретного статуса с документом об удалении, рассмотрение ограничения на период проверки и вопрос об уведомлении получателей. Требование признать национальное обвинение ложным в этот спор не включается без самостоятельных доказательств. Успех измеряется содержанием нового статуса и выполнением связанных обязанностей, а не автоматически возобновлённым обслуживанием.

Во втором сценарии запись ясно описывает историческое уведомление и последующее удаление, но остаётся доступной для проверки. Здесь нет оснований заранее объявлять текущую неточность. Анализ переносится на необходимость, объём, основание обработки, дополнительные условия для уголовных данных и применимые исключения из удаления. Возможен спор о соразмерности дальнейшего использования, однако документ CCF не заменяет его аргументацию. Итог может состоять в сохранении части сведений, изменении категории или удалении - в зависимости от установленных обстоятельств.

В третьем сценарии поставщик исправил профиль, но банк использует старую выгрузку. Нужно подтвердить содержание и дату копии, передать обновление банку, запросить исправление его собственных данных и выяснить применимую процедуру пересмотра. Одновременно проверяется вопрос уведомления по статье 19. Нельзя считать, что ответственность автоматически лежит только на поставщике или только на банке: значение имеют роли, фактические действия и то, когда каждый получил сведения об изменении.

В четвёртом сценарии отказ банка известен, а профиль и источник не установлены. Начинать следует с уточнения и доступа, а не с публичного обвинения конкретной базы. Если выясняется ложное совпадение, исправляется связь между лицом и записью; если подтверждается использование исторических данных о том же лице, анализируются точность и цель. Этот сценарий показывает, почему ранняя квалификация без документов способна направить усилия к неверному адресату.

Для поставщиков авторская рекомендация - ясно различать действующие и исторические статусы, фиксировать дату подтверждённого изменения и обеспечивать проверяемую процедуру исправления и уведомления. Для пользователей данных - проверять существенные сведения и учитывать обновление в собственной записи. Для субъектов - сохранять доказательства, формулировать требования по конкретным полям и отдельно проверять результат у известного получателя. Эти предложения не представлены как уже внедрённый стандарт ARGА, обязательная спецификация продукта или эмпирически доказанная программа повышения эффективности.

18. Заключение: что считать восстановлением информации

Юридически осмысленное восстановление информации начинается с правильного описания результата INTERPOL. Удаление данных должно быть отражено там, где прежний статус используется как текущий, но не превращается автоматически в опровержение всех исторических фактов. Такая позиция одновременно защищает точность и не требует от коммерческого контролёра подменять уголовное правосудие. Её сила состоит в проверяемости конкретного утверждения и в соответствии выбранного требования его предмету.

Для статьи 16 центральный вопрос - неточность или неполнота с учётом цели. Для статьи 17 - наличие основания удаления и пределы исключений. Статьи 18, 19 и 21 позволяют рассмотреть временную защиту, распространение обновления и дальнейшую допустимость обработки; статья 15 помогает установить содержание записи и получателей. Эти инструменты образуют последовательность, но не гарантируют одинакового исхода во всех юрисдикциях и продуктах. Применимость каждой нормы должна быть подтверждена, а не предположена по названию базы.

Результат следует описывать на четырёх уровнях: изменён исходный статус; исправлен коммерческий профиль; уведомлены соответствующие получатели; проверена собственная запись известного пользователя. Последний уровень не равнозначен желаемому коммерческому решению. Раздельная фиксация позволяет честно сообщить о частичном успехе и определить следующий шаг. Формула «всё удалено» без проверки этих элементов способна скрыть как сохраняющуюся ошибку, так и законно хранимую историю, которая ошибкой не является.

Исследование подтверждает необходимость предметного, документированного подхода, но не устанавливает масштаба нарушений на рынке. Для дальнейшего мониторинга нужны обезличенная методология наблюдений, законный доступ к версиям профилей, сопоставимые обращения и проверка ответов. До появления такой базы нельзя заявлять долю ошибок, среднюю продолжительность исправления или достижения ARGА в восстановлении обслуживания. Настоящий доклад предоставляет правовую и доказательственную основу для индивидуальной проверки, сохраняя эти ограничения открытыми.

19. Источники и справочный аппарат

[1] INTERPOL. Compliance and review. Официальное описание последствий удаления уведомлений и подтверждающих документов. Дата обращения: 23.09.2026.

<https://www.interpol.int/How-we-work/Notices/Compliance-and-review>

[2] INTERPOL. Statute of the Commission for the Control of INTERPOL's Files. Редакция 2025, изменения 27.11.2025. Статьи 33(4), 38–41; пределы компетенции и исполнения.

[https://www.interpol.int/en/content/download/5695/file/Statute%20of%20the%20CCF%20\(E\).pdf?inLanguage=eng-GB&version=17](https://www.interpol.int/en/content/download/5695/file/Statute%20of%20the%20CCF%20(E).pdf?inLanguage=eng-GB&version=17)

[3] Европейский парламент и Совет. Регламент (ЕС) 2016/679 от 27.04.2016 (GDPR), OJ L119, 04.05.2016. Статьи 3–6, 10, 12, 15–19, 21, 77, 79, 82. Прочитан официальный исходный текст ЕС, воспроизведённый на legislation.gov.uk; это не консолидированный UK GDPR. Идентификатор EUR-Lex: CELEX 32016R0679.

https://www.legislation.gov.uk/eur/2016/679/pdfs/eur_20160679_adopted_en.pdf

[4] LSEG. World-Check Privacy Statement. Публичное уведомление контролёра: доступ, исправление, ограничения удаления и роль пользователей. Заявления поставщика, не независимый аудит. Дата обращения: 23.09.2026.

lseg.com/.../world-check-kyc-screening/about/privacy-statement

[5] LexisNexis Risk Solutions. Financial Crime Compliance Solutions Processing Notice. Последнее обновление: декабрь 2025. Публичное уведомление об обработке и маршрутах осуществления прав.

<https://risk.lexisnexis.com/corporate/processing-notices/financial-crime-compliance-services>

[6] LexisNexis Risk Solutions. Consumer and Data Access Policies. Только подраздел WorldCompliance: доступ, спор об ошибках и обращение к первичному источнику. Дата обращения: 23.09.2026.

<https://risk.lexisnexis.com/consumer-and-data-access-policies>

[7] Суд ЕС. RW v Österreichische Post AG, C-154/21, 12.01.2023, ECLI:EU:C:2023:3. Полный официальный текст; особенно пункты 37–51 о конкретных получателях и исключениях.

<https://juris.curia.europa.eu/juris/document/document.jsf?docid=269146&doclang=en>

[8] Суд ЕС. TU, RE v Google LLC, C-460/20, 08.12.2022, ECLI:EU:C:2022:962. Использованы официально индексированные пункты 72–73. Полный текст непосредственно не получен; узкий сравнительный вывод, не правило о коммерческих базах.

<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62020CJ0460>

[9] Суд ЕС. UI v Österreichische Post AG, C-300/21, 04.05.2023. Официальная резолютивная часть: OJ C216, 19.06.2023, с. 6–7, 2023/C 216/07. Нарушение само по себе недостаточно для компенсации; минимальный порог серьёзности нематериального вреда недопустим.

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CA0300>

[10] Information Commissioner's Office. What are the rules on criminal offence data? Страница помечена как пересматриваемая после Data (Use and Access) Act 2025. Использована только для разграничения общего основания и дополнительного условия обработки.

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/criminal-offence-data/what-are-the-rules-on-criminal-offence-data/>

[11] Information Commissioner's Office. How to deal with data protection complaints. Опубликовано 12.02.2026, обновлено 08.05.2026. Официальное руководство по жалобам.

<https://ico.org.uk/for-organisations/how-to-deal-with-data-protection-complaints/>

[12] Information Commissioner's Office. One month to go: what businesses need to know to meet new data law. 19.05.2026. Подтверждает вступление требований к жалобам 19.06.2026 и срок подтверждения получения.

<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/05/one-month-to-go-what-businesses-need-to-know-to-meet-new-data-law/>