

Regulatory update Data protection, AI, IT and IP

No. 16/2026

DATA PROTECTION

24 August 2026 – Challenges to decisions of the Italian Data Protection Authority: the Supreme Court clarifies the rules on mandatory joinder of parties.

14 August 2026 – China: CAC clarifies the use of publicly available personal information and measures to prevent data breaches.

ARTIFICIAL INTELLIGENCE

21 August 2026 – WikiHow sues OpenAI for copyright infringement: ChatGPT training, RAG and outputs under scrutiny.

20 August 2026 – China: SAMR clarifies when AI prompts and related materials may qualify as trade secrets.

17 August 2026 – AI Act after the Digital Omnibus: CNIL updates its FAQs on the revised application timeline and relationship with the GDPR.

10 August 2026 – Council of Ministers: legislative decrees on the AI Act and measures on national cybersecurity and strategic investments in data centres have been adopted.

CYBERSECURITY

14 August 2026 – ETSI launches the approval process for 17 draft standards supporting the Cyber Resilience Act.

14 August 2026 – National Cybersecurity Agency (ACN): new FAQs on monitoring, supervision and enforcement activities in relation to NIS entities.

INFORMATION TECHNOLOGY

19 August 2026 – European Digital Identity: new rules on electronic attestations of attributes become applicable.

18 August 2026 – The EU e-Evidence Regulation becomes applicable: new cross-border European Production and Preservation Orders.

DIGITAL MARKETS

26 August 2026 – Data Act: from 12 September 2026, data access becomes a design requirement.

25 August 2026 – France: law protecting minors online published without the under-15 social media ban.

INTELLECTUAL AND INDUSTRIAL PROPERTY

19 August 2026 – UPC Milan Central Division adopts a broad approach to standing in patent revocation actions.

17 August 2026 – Round Hill Music v Anthropic and Suno: copyright liability across the AI supply chain comes under scrutiny.

DATA PROTECTION

24 August 2026 – Challenges to decisions of the Italian Data Protection Authority: the Supreme Court clarifies the rules on mandatory joinder of parties.

In Order No. 23755/2026, the Italian Supreme Court of Cassation addressed the proper commencement of proceedings challenging decisions of the Italian Data Protection Authority under Article 10 of Legislative Decree No. 150/2011. The Court clarified the Authority's procedural status and the consequences of failing to join other parties whose participation in the proceedings is mandatory.

According to the Supreme Court, Article 10(6) of Legislative Decree No. 150/2011 – which requires the challenge to be served on both the parties and the Italian Data Protection Authority – establishes a case of mandatory joinder of defendants under Article 102 of the Italian Code of Civil Procedure.

The ruling is also particularly important from a procedural perspective: if the challenge has been brought in time against at least one necessary party, failure initially to join another necessary party does not automatically render the proceedings inadmissible. In that situation, the court must order the joinder of the omitted party.

The case arose from a challenge brought before the Court of Rome against a decision by which the Authority had closed a complaint concerning the processing of personal data in connection with the acquisition of a criminal-record certificate by officials of the office of the Justice of the Peace.

The Ministry of Justice, identified as the controller of the processing at issue, was not initially joined to the proceedings.

The Court of Rome considered this omission to prevent the proceedings from continuing and declared the challenge inadmissible. It held that subsequently joining the Ministry would effectively circumvent the mandatory thirty-day time limit laid down in Article 10(3) of Legislative Decree No. 150/2011 for bringing the challenge.

The Supreme Court, by contrast, allowed the appeal, set aside the decision and remitted the case.

The Court began by considering the particular institutional position of the Italian Data Protection Authority. In exercising the powers conferred on it by the GDPR and the Italian Privacy Code, the Authority may adopt preventive, prohibitory and corrective measures, intervene in relation to unlawful processing and impose administrative sanctions. Although it must exercise its powers impartially and fairly, it does not occupy a position comparable to that of a court in the subsequent judicial proceedings.

From a procedural perspective, Article 10 of Legislative Decree No. 150/2011, as amended by Legislative Decree No. 101/2018, expressly requires the challenge to be served on both the parties and the Italian Data Protection Authority. The Supreme Court inferred from that provision that the Authority and any other parties whose legal positions are directly affected by the dispute are subject to mandatory joinder.

The consequence is significant. Where the challenge has been brought within the applicable time limit and validly commenced against at least one necessary party, the absence of another necessary party does not in itself make the proceedings inadmissible: the court must order the joinder of the omitted party under Article 102 of the Italian Code of Civil Procedure.

The position is different where the proceedings have been brought exclusively against a person who is not a proper defendant. In that case, the proceedings were not validly commenced against any party required to participate, and the mechanism for joining an omitted necessary party does not apply.

The Supreme Court also clarified that the application of the procedural rules governing employment disputes to proceedings under Article 10 of Legislative Decree No. 150/2011 is compatible with a court order for joinder under Article 102 of the Italian Code of Civil Procedure, provided that the action was brought in time against at least one necessary party.

In the case before it, the challenge had been brought in time against the Italian Data Protection Authority. The Court of Rome should therefore not have declared it inadmissible because the Ministry of Justice had not initially been joined, but should instead have ordered the joinder of the Ministry.

On that basis, the Court of Cassation set aside Court of Rome Judgment No. 13820/2025, filed on 8 October 2025, and remitted the case.

The decision provides important clarification for personal data protection litigation. When bringing a challenge under Article 10 of Legislative Decree No. 150/2011, the claimant must identify not only the Italian Data Protection Authority, whose participation is expressly required by law, but also any other parties whose legal positions are directly affected by the relief sought.

At the same time, failure initially to serve the challenge on one of those parties does not necessarily result in dismissal: where the proceedings were brought in time against at least one necessary party, the court can and must order the joinder of the omitted party.

14 August 2026 – China: CAC clarifies the use of publicly available personal information and measures to prevent data breaches.

The Cyberspace Administration of China (CAC) has published a new Q&A document on policies and obligations concerning personal information protection, providing operational guidance for organisations processing personal information under the Personal Information Protection Law (PIPL).

Among the most significant points, CAC addresses the processing of publicly available personal information, clarifying that it may be processed within a reasonable scope consistent with the purposes and circumstances in which it was disclosed. This is not, however, an unlimited permission: the personal information processor must respect any express objection by the individual and, where the processing may have a significant impact on the individual's rights and interests, the separate consent required by the PIPL must be obtained.

The document also addresses the prevention of security incidents and data breaches, identifying the absence or inadequacy of encryption and, more generally, insufficient security measures among the main operational weaknesses. Recommended measures include encryption, strong passwords and regular staff training on risks and security safeguards.

For companies operating in China or processing personal information subject to the PIPL, CAC's guidance highlights the need to review the collection and reuse of data from public sources rather than automatically treating such data as freely available for unrestricted use. Companies should also review the technical and organisational measures adopted to prevent unauthorised access, disclosure or loss of data, and document the criteria used to assess whether the processing of publicly available information is reasonable and when separate consent from the individual is required.

ARTIFICIAL INTELLIGENCE

21 August 2026 – WikiHow sues OpenAI for copyright infringement: ChatGPT training, RAG and outputs under scrutiny.

WikiHow sued OpenAI in the U.S. District Court for the Southern District of New York, alleging the unauthorised use of its content in connection with ChatGPT. The lawsuit, filed on 21 August 2026, concerns 1,211 copyright registrations covering a total of 11,211 articles.

The case is particularly significant because it expands the traditional litigation concerning the relationship between copyright and the training of generative models. According to wikiHow's allegations, OpenAI not only reproduced the articles to train its LLMs, but also uses them through *Retrieval-Augmented Generation* (RAG) systems to provide the model with external content when generating responses; ChatGPT would also, in certain cases, be capable of reproducing all or part of the wording and structure of the original articles.

wikiHow also challenges the alleged removal of copyright management information (CMI) – including titles, author names and publication information – under Section 1202 of the Digital Millennium Copyright Act. At present, these are allegations that have yet to be judicially determined. The case is significant because it shifts the debate beyond the lawfulness of training alone to a more complex chain involving content acquisition, training, *retrieval*, output generation and the handling of copyright management information.

20 August 2026 – China: SAMR clarifies when AI prompts and related materials may qualify as trade secrets.

On 20 August 2026, China's State Administration for Market Regulation (SAMR) published six exemplary cases of trade secret infringement. They include what the authority describes as the first national case concerning the protection, as trade secrets, of elements of a specialised large language model.

The case concerns an algorithm expert who, while working for a company active in the artificial intelligence sector, allegedly transferred materials relating to a specialised model to a company under his control. These included proprietary prompt templates, review rules and data-annotation specifications, which were subsequently used to develop a competing system.

According to the technical assessment relied on by SAMR, those elements, taken together, formed an integrated solution meeting the requirements of secrecy, economic value and adequate protection and could therefore qualify as trade secrets. The individual responsible had already been fined RMB 350,000 by the Hangzhou authority on 28 May 2026. What is new as of 20 August is the inclusion of the case among SAMR's nationally designated exemplary cases.

The most significant principle stated by the authority is that the protection of artificial intelligence technologies is not limited to source code. Information expressed in natural language and non-standardised operational components may also constitute trade secrets, provided that the statutory requirements are met.

SAMR notes, in particular, that companies are increasingly relying on trade secret law to protect prompt-engineering techniques, AI agent skill packages and other emerging categories of technical information. The case therefore illustrates the growing importance of trade secret protection for AI-related technological assets, extending well beyond traditional source-code protection.

17 August 2026 – AI Act after the Digital Omnibus: CNIL updates its FAQs on the revised application timeline and relationship with the GDPR.

On 17 August 2026, the French CNIL updated its FAQs on the AI Act to reflect the changes introduced by the Digital Omnibus, which entered into force on 27 July 2026. The update provides a particularly useful overview of the revised application timeline for the EU Artificial Intelligence Act and further clarifies the relationship between the AI Act and the GDPR.

According to the timeline updated by CNIL, transparency obligations relating to certain AI systems apply from 2 August 2026. From 2 December 2026, the ban on AI systems that generate child sexual abuse material and deepfakes will also apply, as will, for affected systems placed on the market before 2 August 2026, the specific transparency obligations relating to the labelling of AI-generated content. The rules on high-risk systems listed in Annex III will apply from 2 December 2027, while those concerning high-risk systems related to products listed in Annex I will apply from 2 August 2028.

CNIL also points out that the GDPR continues to apply to the processing of personal data during both the development and use of AI systems. In many cases, the provider of an AI system or model may act as controller under the GDPR during the development phase, while a deployer processing personal data through the system will often act as controller for the processing carried out during use.

Particularly significant is CNIL's reminder that the two regulatory frameworks should be read together. The transparency, documentation, risk-assessment and accountability obligations under the AI Act can contribute to GDPR compliance. CNIL refers, for example, to the relationship between the fundamental rights impact assessment under the AI Act (FRIA) and the data protection impact assessment (DPIA), highlighting the possibility of coordinating the two assessments to avoid duplicating documentation.

Finally, CNIL confirms that it retains its full powers under the GDPR in relation to the processing of personal data involving AI systems and models, even where those systems and models are also subject to the AI Act.

10 August 2026 – Council of Ministers: legislative decrees on the AI Act and measures on national cybersecurity and strategic investments in data centres have been adopted.

The Council of Ministers approved a package of measures covering three increasingly interconnected areas of Italy's digital strategy: implementation of the European AI Act, strengthening national cybersecurity and developing digital infrastructure, with particular focus on data centres.

On artificial intelligence, legislative decrees were approved to align Italian law with Regulation (EU) 2024/1689 – the AI Act. The measures highlighted include strengthening the principle of human oversight in the use of AI systems and introducing limits on the use of real-time remote biometric identification systems.

The measures form part of the broader process of adapting the Italian legal system to the new European AI framework and are particularly relevant to organisations that develop, provide or use artificial intelligence systems, especially where those systems may fall within categories subject to enhanced requirements. Companies should therefore verify that their AI-governance frameworks ensure effective human oversight, a clear allocation of responsibilities and, for high-risk systems, security and control measures consistent with the European and national regulatory framework.

At the same time, the Council of Ministers approved a bill aimed at strengthening the national cybersecurity and cyberspace defence system. The announced measures include defining the concept of “national cyberspace” and establishing a Cybersecurity Incentive Fund to support the strengthening of national capabilities in this area.

The initiative confirms the growing importance of cybersecurity as a structural component of national security and corporate business continuity. For economic operators, especially those already subject to the NIS2 framework or included in critical supply chains, the evolving regulatory framework requires the progressive consolidation of cyber governance, risk management, incident response and supply-chain security safeguards, also in anticipation of possible further obligations and implementing measures.

The Government has also acted on digital infrastructure, recognising two major data-centre projects as investments of national strategic interest, with a total value of approximately EUR 6.8 billion.

The figure is particularly significant because it confirms the growing role of data centres in Italian industrial and digital policy and, more generally, in building the infrastructure needed to support cloud services, artificial intelligence applications and high-performance computing capabilities.

Taken together, these measures show increasing convergence between AI regulation, cybersecurity and infrastructure policy. Companies should therefore address these areas not as separate compliance silos but through integrated digital-governance frameworks connecting AI governance, data protection, cybersecurity, operational resilience and technology-supplier management.

CYBERSECURITY

14 August 2026 – ETSI launches the approval process for 17 draft standards supporting the Cyber Resilience Act.

The European Telecommunications Standards Institute (ETSI) has launched the approval process for 17 draft standards developed under the *Cyber Resilience Act* (CRA), intended to support implementation of the European cybersecurity requirements applicable to products with digital elements.

The objective is for these specifications eventually to be adopted as harmonised standards, giving manufacturers technical references for demonstrating compliance with the relevant CRA requirements. The initiative is particularly important for products with digital elements where compromise may pose greater risks, including, for example, password managers and wearable devices.

The 17 drafts now enter the public inquiry phase, during which ETSI member organisations and participating partner organisations may submit comments and proposed amendments. The consultation will remain open until mid-November 2026.

The start of the process is an important step towards building the technical framework for implementing the Cyber Resilience Act: once harmonised, the standards will be among the main operational tools available to manufacturers to demonstrate that products with digital elements comply with the cybersecurity requirements laid down by EU law.

14 August 2026 – National Cybersecurity Agency (ACN): new FAQs on monitoring, supervision and enforcement activities in relation to NIS entities.

The National Cybersecurity Agency has updated its FAQs [on the NIS framework](#), introducing new FAQs MVE.1, MVE.2, MVE.3, MVE.4 and MVE.5 on monitoring, supervision and enforcement activities.

FAQ MVE.1 explains that supervision and enforcement are organised into four areas – monitoring, analysis and support; checks and inspections; enforcement measures; administrative fines and ancillary penalties – through which the Agency monitors and assesses compliance by NIS entities. The same FAQ confirms that these activities follow a gradual, risk-based approach, in accordance with the principles of effectiveness, proportionality and dissuasiveness and taking account of the specific circumstances of each case.

With regard to monitoring, analysis and support, FAQ MVE.2 highlights the systematic and continuous nature of these activities and their role in assisting NIS entities with implementation. Through monitoring, the Agency gathers the information needed to assess implementation; through analysis, it evaluates the results; and through support activities, it assists NIS entities by means of recommendations, guidelines and awareness-raising initiatives.

With regard to checks and inspections, FAQ MVE.3 clarifies that *ex ante* inspections may be carried out only in respect of essential entities.

FAQ MVE.4 explains that, through enforcement measures, the Agency may require NIS entities to comply with their obligations, remedy identified deficiencies or cease conduct found to be in breach, including by means of formal orders and warnings.

Finally, FAQ MVE.5 clarifies that the amount of administrative fines and the scope of ancillary measures vary depending on whether the entity is classified as essential, important or a public administration.

INFORMATION TECHNOLOGY

19 August 2026 – European Digital Identity: new rules on electronic attestations of attributes become applicable.

From 19 August 2026, Articles 6–9 of Implementing Regulation (EU) 2025/1569, one of the technical acts completing the new European Digital Identity Framework introduced by the revision of the eIDAS Regulation, become applicable. The provisions concern qualified electronic attestations of attributes and attestations issued by, or on behalf of, public-sector bodies responsible for authentic sources.

Electronic attestations of attributes make it possible for natural and legal persons to prove specific characteristics or qualifications digitally, without necessarily disclosing their full identification data on each occasion, and are a central element of the European Digital Identity Wallet ecosystem.

From 19 August, the provisions requiring the Commission to establish and maintain a list of public-sector bodies issuing attestations of attributes on the basis of authentic sources, and to create a European catalogue of attributes in both human-readable and *machine-readable formats*, also apply.

The catalogue of attribute-attestation schemes, designed to ensure interoperability, integrity and common trust models, also becomes operational, together with the system through which qualified trust service providers can verify attributes directly against authentic sources or intermediaries designated by Member States.

The Regulation expressly provides safeguards for integrity, authenticity, confidentiality and personal data protection, confirming the role of data minimisation and selective disclosure in the architecture of the new European digital identity.

The application of these provisions marks another step towards the deployment of the European Digital Identity Wallet, intended to enable European citizens and businesses to identify themselves and digitally prove their identity, qualifications and other attributes when interacting with public and private services throughout the Union.

18 August 2026 – The EU e-Evidence Regulation becomes applicable: new cross-border European Production and Preservation Orders.

From 18 August 2026, Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings becomes applicable. The new framework significantly changes how judicial authorities in Member States can obtain data held by service providers established or represented in another Member State.

A European Production Order allows a judicial authority in one Member State to require a service provider, or its legal representative in another Member State, to produce electronic evidence such as emails, messages, communications data or information necessary to identify an individual. The standard deadline for compliance is 10 days, reduced to 8 hours in urgent cases.

A European Preservation Order enables a competent authority to require the preservation of specified data so that they are not deleted or altered before a subsequent production request. The system is accompanied by safeguards for fundamental rights and personal data protection, mechanisms for raising objections and specific procedures for conflicts of legal obligations.

The Regulation also provides for a decentralised IT system for secure communications between authorities and service providers and requires providers offering services in the EU, including those based in third countries, to have a designated establishment or legal representative in the EU to receive and execute orders.

The application of the Regulation marks a significant development in the EU framework for cross-border access to data and sits at the intersection of criminal judicial cooperation, digital services, cybersecurity and personal data protection.

DIGITAL MARKETS

26 August 2026 – Data Act: from 12 September 2026, data access becomes a design requirement.

From 12 September 2026, one of the most significant obligations under the Data Act (Regulation (EU) 2023/2854) becomes applicable to manufacturers of connected products and providers of related services. This is not the date on which the Data Act itself becomes applicable – it has applied since 12 September 2025 – but the date on which the specific obligation in Article 3(1) begins to apply to connected products and related services placed on the market after that date.

The provision introduces what is commonly referred to as “*access by design*”: connected products must be designed and manufactured, and related services designed and provided, so that product and related-service data, together with the metadata necessary to interpret and use them, are by default easily and securely accessible to the user, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, directly accessible.

The obligation covers a wide range of connected products, including vehicles, industrial and agricultural machinery, IoT devices, monitoring equipment and smart-home systems. It mainly concerns raw and pre-processed data that are readily available, rather than, in general, information further processed or inferred through processes that produce significantly enriched data.

The change is primarily technological and design-related: for newly covered products, it will no longer be sufficient merely to be able to extract data following a user request. Accessibility will need to be built into the architecture of the product or service, for example through interfaces, applications, portals, export functions or APIs.

The relationship with the GDPR is particularly important. Data generated by connected products may include personal data. Where the user is also the data subject, the Data Act and the GDPR operate in a complementary manner. Where, however, the data concern persons other than the user – for example, an employee using a company vehicle or several people using the same device – the Data Act does not independently provide a legal basis for disclosing those personal data. A legal basis under Article 6 GDPR must therefore be identified and, where special categories of personal data are involved, one of the conditions laid down in Article 9(2) GDPR must also apply.

This creates a need to coordinate “*access by design*” with “*data protection by design and by default*”: making data technically accessible does not mean making them indiscriminately available. Systems must enable the user to be identified and authenticated, limit access to the data that the user is lawfully entitled to access, and protect data relating to third parties.

A similar balancing exercise applies to cybersecurity and trade secrets. The Data Act does not permit companies to invoke trade secrets or know-how as a blanket justification for refusing data sharing, but it does provide specific safeguards and, in certain circumstances, allows access to be limited or refused. For the companies concerned, the deadline therefore requires a concrete assessment of products intended to be placed on the market after 12 September 2026: companies should map the data generated, distinguish personal from non-personal data, identify any third-party data and trade secrets, and design appropriate access, authentication and sharing mechanisms.

Under the Data Act, data accessibility therefore becomes a feature to be incorporated into the design of connected products. Where personal data are involved, however, “access by design” must be implemented from the outset in a manner consistent with the principles and obligations of the GDPR.

25 August 2026 – France: law protecting minors online published without the under-15 social media ban.

On 25 August 2026, Law No. 2026-813 of 24 August 2026, aimed at protecting minors from risks associated with the use of social networks, was published in the French Official Journal. The law, however, entered into force without its main measure: the general ban on access to social networks for children under 15, which had been struck down by the Conseil constitutionnel a few days earlier.

By Decision No. 2026-911 DC of 14 August 2026, the Conseil constitutionnel declared Article 1 of the law unconstitutional. The provision would have prohibited children under 15 from accessing social network services provided by online platforms.

The Conseil constitutionnel recognised that protecting the best interests of the child against risks such as addiction, isolation, pornography, harassment and fraud may legitimately justify restrictions on access to digital services. It nevertheless considered the French ban excessively broad and undifferentiated: it would have applied to very different services even where the risks to minors had not been specifically established, without taking account of the platform’s functionalities, the nature of the content or the protective measures adopted.

The ban also applied indiscriminately to all children under 15, without allowing holders of parental responsibility to authorise access to specific services and without any assessment of the child’s age, degree of maturity, individual circumstances or the particular platform concerned. According to the Conseil, the measure therefore imposed an unnecessary, inappropriate and disproportionate restriction on freedom of expression and communication.

The age-verification and data-protection aspects of the decision are also particularly significant. The Conseil noted that preventing access by children under 15 would inevitably require all users, including adults,

to prove their age. The law, however, did not lay down sufficient conditions, limits and safeguards for such verification, resulting in a violation of the right to respect for private life.

The publication of the law on 25 August did not follow a redrafting designed to address those constitutional objections. Rather, pursuant to Article 62 of the French Constitution, the provision declared unconstitutional was simply omitted from the promulgated text. In the official text, Article 1 is replaced by a statement recording its declaration of unconstitutionality. Accordingly, Law No. 2026-813 does not, at present, introduce a general ban on access to social networks for children under 15 in France.

The other provisions of the law remain in force. Article 2 strengthens the measures available to combat online content related to suicide. In particular, it brings the offence under Article 223-14 of the Criminal Code – concerning propaganda or advertising for products, objects or methods presented as means of taking one's own life – within the regime allowing the suspension of accounts used to commit the offence, while also amending the French law on confidence in the digital economy.

Article 3, applicable from the 2026–2027 school year, addresses the use of digital technologies in schools. It extends the ban on the use of mobile phones and other electronic devices to upper-secondary schools (lycées), subject to the procedures and exceptions laid down in internal rules, and requires school projects to include measures on the use of digital technologies and awareness-raising activities for students, staff and parents concerning the risks of excessive screen exposure and the potentially addictive nature of social networks.

Finally, it should be emphasised that the Conseil constitutionnel did not expressly declare all the other provisions to be consistent with the Constitution. The decision states that the Conseil did not examine of its own motion any constitutional issues concerning provisions other than Article 1 and therefore did not rule on their constitutionality.

The decision provides an important reference point for future European rules on age assurance: protecting minors may justify restrictions on access to platforms, but an age-verification system must be narrowly tailored, proportionate and accompanied by precise safeguards for freedom of communication and the privacy of adult users as well.

INTELLECTUAL AND INDUSTRIAL PROPERTY

19 August 2026 – UPC Milan Central Division adopts a broad approach to standing in patent revocation actions.

The Milan Central Division of the Unified Patent Court, in *LS9 GmbH v Bellissa HAAS GmbH* (UPC_CFI_860/2025), issued a decision on 19 August 2026 of particular importance concerning standing to bring an action for revocation of a European patent.

The Court interpreted broadly the requirement that a person be “concerned by a patent” under Article 47(6) of the Agreement on a Unified Patent Court. According to the Division, a legal person must, in principle, be regarded as concerned by the validity of a patent: since a legal person cannot act in a purely private capacity, its activities are commercial in nature, and there is a general interest in ensuring that patents which should not have been granted do not remain in force. This applies even where the claimant is not already active in the industrial sector to which the patent relates.

The ruling therefore significantly reduces the scope for challenging a claimant's standing in central revocation actions on the ground that it has no concrete presence in the relevant market and may also facilitate the use of companies established or used for the purpose of bringing revocation actions.

The Court also clarified that the subject matter of a revocation action is determined not only by the grounds of invalidity relied upon, but also by the specific prior-art documents and arguments on which the action is based. Accordingly, a parallel revocation action based on different prior art is not, as a general rule, barred by *lis pendens*.

17 August 2026 – Round Hill Music v Anthropic and Suno: copyright liability across the AI supply chain comes under scrutiny.

Round Hill Music filed two separate copyright infringement actions against Anthropic and Suno in the U.S. District Court for the Northern District of California on 17 August 2026. Bright Data Ltd. and Bright Data Inc., companies providing web-scraping technologies, are also defendants in the action against Suno.

According to Round Hill, the defendants allegedly reproduced protected musical works without authorisation to develop and train artificial intelligence systems. The action against Suno includes claims of direct copyright infringement, contributory infringement, circumvention of technological protection measures, and removal or alteration of copyright management information. Round Hill also alleges that web-scraping tools were used to circumvent technological protections put in place to protect the content.

The proceedings are significant not only because of the growing conflict between the music industry and generative AI providers, but also because they directly involve a provider of data-acquisition infrastructure. They may therefore help clarify how liability for the collection and use of protected works is allocated across the AI supply chain, including AI system providers, dataset suppliers and web-scraping operators. The allegations remain, of course, subject to judicial determination.
