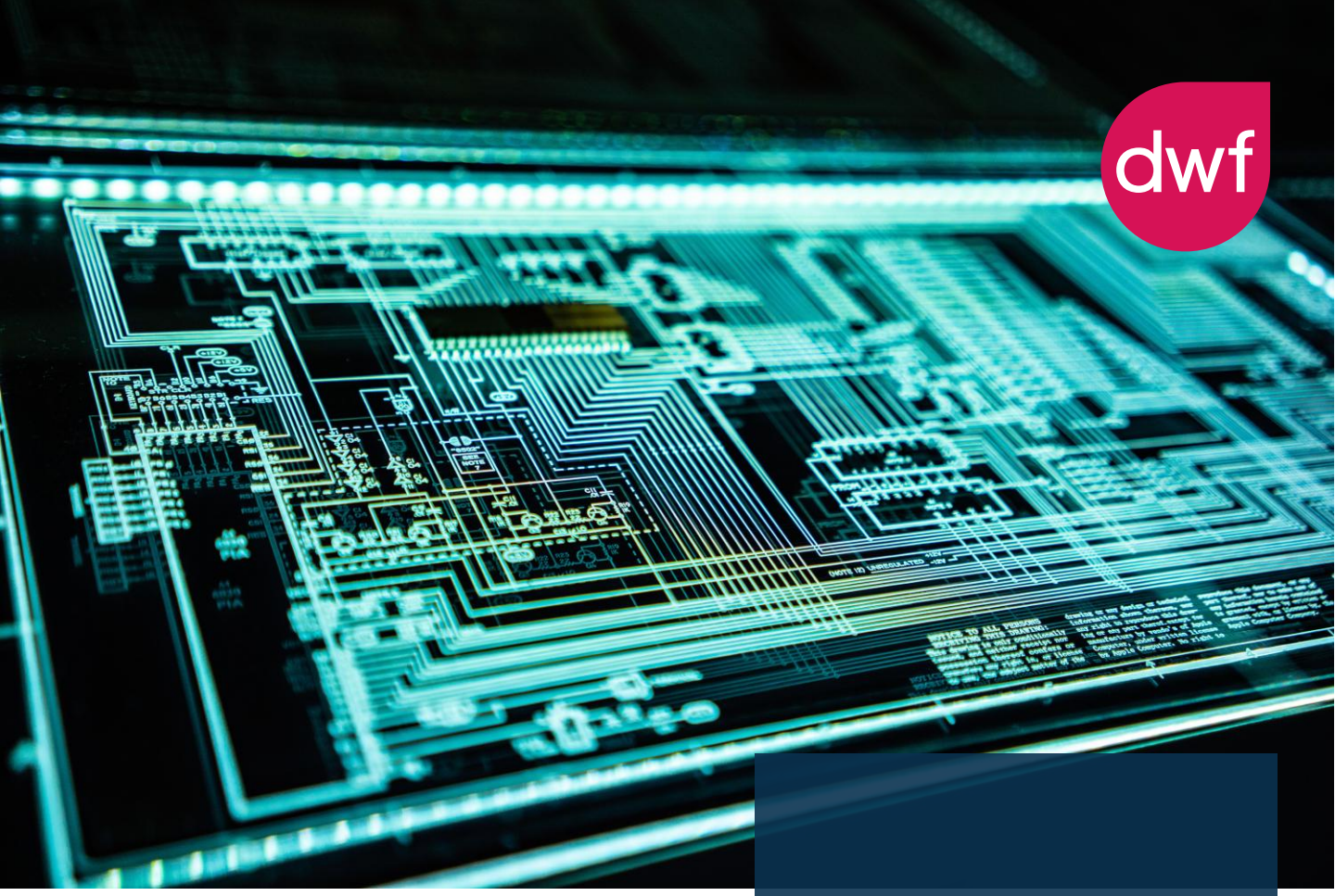


Newsletter

Tech / Data

First Quarter of 2026

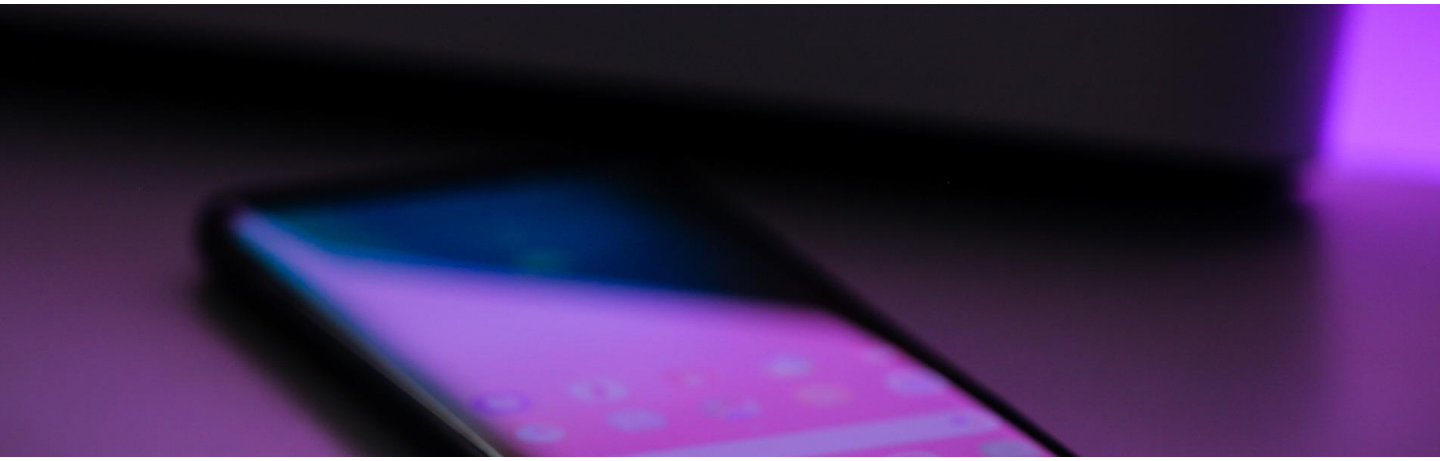
dwfgroup.com

Airbnb denied host status

The Court of Cassation has ruled that Airbnb plays an active role in managing listings and is therefore not eligible for the limited liability regime applicable to hosts.

In this issue

LATEST NEWS - TECHNOLOGIES



META ordered to pay damages for failure to filter advertisements

Paris Court of Appeal, Division 5, Chamber 1, META PLATFORMS IRELAND LIMITED v GROUPE LUCIEN BARRIERE, 28 January 2026, No. 24/12568

In a judgment of 28 January 2026, the Paris Court of Appeal upheld the injunctions issued against Meta Platforms Ireland Limited following the repeated dissemination, in the form of sponsored advertisements, of content that exactly replicated the Lucien Barrière Group's trademark in order to promote illegal online gambling.

Deeming these advertisements unlawful, the Lucien Barrière Group had obtained an emergency order requiring Meta to implement filtering measures and retain data relating to the advertisers concerned. The obligations imposed on Meta included, in particular, implementing, within eight days, preventive measures targeting advertisements promoting online gambling that exactly replicated the European Union trade marks 'BARRIERE' published by unauthenticated advertisers, and ensuring the retention of identification data associated with the accounts in question for a period of twelve months.

Meta lodged an appeal for annulment, which was dismissed by an order dated 24 April 2024. In a judgment of 28 January 2026, the Paris Court of Appeal held that the disputed advertisements infringed the essential and economic functions of the Lucien Barrière Group's European Union trade marks and that their widespread, repeated and reported nature constituted a manifestly unlawful disturbance justifying the intervention of the judge hearing the application for interim relief.

The trial judges held that Meta acted as an intermediary by permitting the publication of advertisements that were likely to be infringing. Consequently, they held that Meta could be ordered to take interim measures designed to put an end to any infringement or to prevent an imminent infringement of the Barrière Group's intellectual property rights, without it being necessary to establish liability orit is necessary to establish whether Meta played an active role in the events in question and whether it should be regarded as acting as a hosting provider or a publisher within the meaning of the LCEN and the E-Commerce Directive.

The Court further notes that the measure ordered has proved effective in reducing the disputed content and that it has not been demonstrated that it would be disproportionate in view of Meta's capabilities. It also notes that the dynamic injunction complies with European guidelines on combating infringements of intellectual property rights.

The Court thus confirms the order of 24 April 2024 in its entirety, dismisses the application brought by Meta under Article 700 of the Code of Civil Procedure, and orders it to pay the Lucien Barrière Group the sum of €15,000 in this regard, as well as the costs of the appeal.

LATEST NEWS - TECHNOLOGIES

Refusal to grant host status to the Airbnb platform

Court of Cassation, Commercial Chamber, 7 January 2026, No. 23-22.723 and No. 24-13.163

In two judgments of 7 January 2026, the Court of Cassation ruled on the liability of the online rental platform Airbnb in connection with the unlawful subletting of social housing.
A tenant of a property owned by the company Famille et Provence had sublet the property on the Airbnb platform, in breach of her tenancy agreement which prohibited any subletting. The landlord then brought proceedings against the tenant and the companies operating the platform to recover the sums received from these lettings.
The Court of Appeal of Aix-en-Provence had dismissed the claim against Airbnb Ireland, considering that the latter did not act as a publisher but as a hosting provider, which limited its liability.
The Court of Cassation points out that the reduced liability regime provided for hosting providers under the E-Commerce Directive applies only if the service provider plays a purely technical and neutral role in the storage of content. Conversely, where an operator plays an active role conferring upon them knowledge of or control over the content, they can no longer benefit from this status.
However, according to the High Court, the Court of Appeal had not sufficiently examined whether certain features of the platform, such as the rules imposed on users, the promotion of listings or the awarding of 'Superhost' status, could indicate an active role on the part of Airbnb in the management of published listings.
Thus, in its statement, the Court of Cassation specifies that Airbnb does not qualify as an internet hosting provider because it does not play a neutral role vis-à-vis users, but rather interferes in the relationship between hosts and travellers by requiring them to follow a set of rules and by promoting certain listings that influence user behaviour.
By playing this active role, Airbnb does not benefit from the exemption from liability that the law grants to hosting providers.

Joint Opinion of the EDPS and the EDPB on the OMNIBUS Regulation proposal

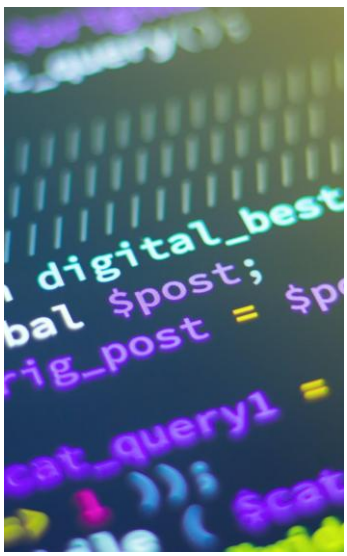
Press release on the opinion of the EDPB and the EDPS on simplifying the rules on artificial intelligence, 13 March 2026

The EDPB (European Data Protection Board) and the EDPS (European Data Protection Supervisor) have published a joint opinion on the proposed Omnibus Regulation.

They support several advances, such as the simplification of data breach notifications, the harmonisation of the concept of 'scientific research', and the new derogation for the processing of special categories of data for the purposes of biometric authentication.

They also support the aim of providing a regulatory solution to address consent fatigue and the proliferation of cookie banners, but at the same time highlight the legal and technical difficulties arising from the coexistence of two different regimes for personal data and non-personal data.

They also express major concerns, in particular regarding the redefinition of personal data, which is deemed too broad and risks weakening the protection of individuals, and certain AI-related exemptions that require further safeguards and clarity.



LATEST NEWS - TECHNOLOGIES

Opinion of the Council of the European Union on the proposal to simplify and adjust certain rules of the AI Act as part of the Omnibus simplification package

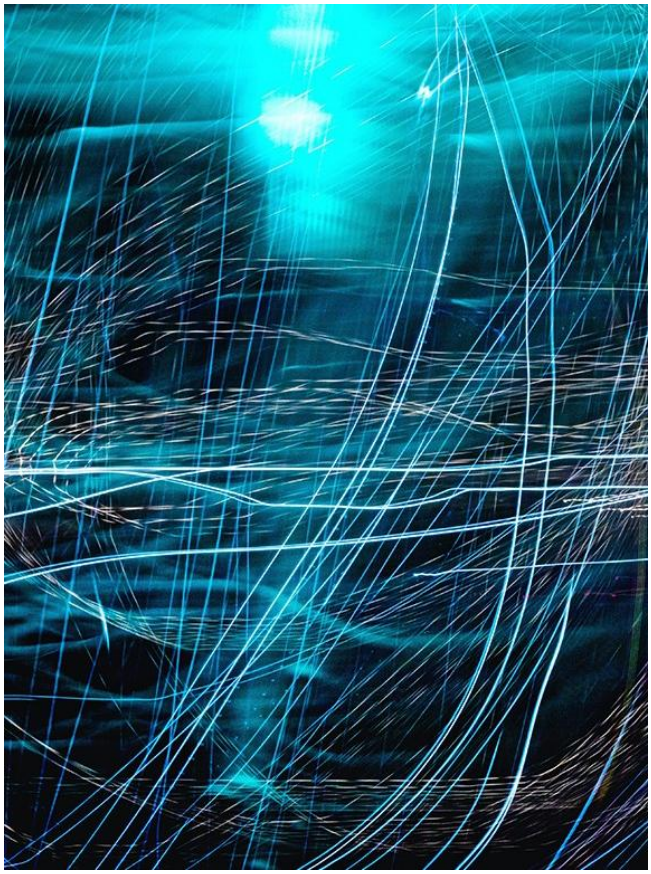
The Council adopts a position aimed at simplifying the rules on artificial intelligence, 13 March 2026

The Commission had initially proposed postponing the entry into force of certain obligations relating to high-risk AI systems by up to sixteen months, in particular to allow time for harmonised technical standards to be developed. It also recommended extending the provisions already in place for SMEs to small and mid-cap companies, reducing certain requirements in limited cases, and allowing for a broader use of sensitive data for the purposes of detecting and mitigating bias. It also intended to strengthen the powers of the AI Office and reduce fragmentation within the governance system.

The Council broadly followed these guidelines, whilst making several significant additions. In particular, it introduced an explicit ban on AI practices that generate non-consensual sexual or intimate content or child sexual abuse material, thereby strengthening protection against particularly harmful uses. It also set specific dates for the deferred application of the rules applicable to high-risk systems: **2 December 2027** for **autonomous systems** and **2 August 2028** for **those integrated into products**. Furthermore, it reinstated the obligation for providers to register in the European database those systems they consider exempt from 'high-risk' status, as well as the 'strict necessity' condition for the processing of sensitive data used in the detection and correction of bias.

The text adopted by the Council also extends the deadline for establishing **national regulatory sandboxes** to **2 December 2027**, thereby giving national authorities more leeway to organise these supervised testing environments. At the same time, it further clarifies the scope of the AI Office's remit regarding the supervision of systems based on general-purpose AI models, notably by listing the areas where national authorities retain an exclusive role, such as law enforcement, border management, judicial authorities and certain financial sectors.

Overall, the Council's position aims to accelerate the effective implementation of the European framework on artificial intelligence whilst ensuring greater proportionality of obligations, better harmonisation between Member States and increased support for businesses. It marks an important step towards the coherent and operational implementation of the AI Act, at a time when the EU wishes to strengthen its competitiveness and establish a clear regulatory environment whilst protecting citizens from the riskiest uses of AI.



LATEST NEWS - TECHNOLOGIES

Streaming platforms and violent content

Paris Judicial Court, French State v. Kick Streaming, 19 December 2025, No. 25/57054

The judgment of the Paris Judicial Court of 19 December 2025 comes in a specific context marked by the live streaming of extremely violent content on the Kick platform, culminating in the death of streamer Jean Pormanove.

Referred to by the French State on the basis of the Law on Confidence in the Digital Economy (LCEN), the judge had to determine to what extent he could intervene to put a stop to these infringements whilst respecting freedom of expression.

The Court first recognised the jurisdiction of the judicial judge to order measures aimed at preventing serious harm linked to online content. It therefore accepted that judicial intervention is legitimate in response to the dissemination of violent content accessible to the French public. This recognition forms part of the interplay between national law (LCEN) and European law, in particular the Digital Services Act (DSA), which governs the liability of platforms.

However, the Court refuses to grant the State's main request to block the entire platform. It considers that such a measure would be disproportionate, in the absence of evidence of systemic misconduct on the part of Kick as a whole. A block would constitute an excessive infringement of the freedom of expression and communication protected, in particular, by the European Convention on Human Rights.

On the other hand, the judges noted the particular seriousness of the content broadcast on the 'Jean Pormanove' channel, characterised by violence, humiliation and endangerment. As such, they ordered targeted measures: maintaining the inaccessibility of this channel, removing the associated violent content, and imposing financial penalties in the event of non-compliance. Judicial intervention is therefore permitted but limited to what is deemed strictly necessary. No appeal appears to have been lodged.

New National Cybersecurity Strategy 2026–2030

ANSSI, National Cybersecurity Strategy 2026–2030

On 29 January 2026, the National Cybersecurity Agency published its new National Cybersecurity Strategy 2026–2030. This strategy, commissioned by the President of the Republic, sets out the ambition to make France a leading cyber nation in response to the growing digital threat affecting the entire economic and social fabric.

It places the large-scale development of cyber skills at the heart of public policy, with the aim of building Europe's largest pool of cyber talent by strengthening all training pathways and guiding young people towards these careers of the future. To strengthen national resilience, it raises the level of cybersecurity for critical infrastructure and government services, improves crisis preparedness and enhances support for victims via a streamlined national portal.

France also intends to curb the spread of the threat by mobilising all its resources (judicial, diplomatic, military, economic and technical) and by stepping up information sharing with the private sector. Finally, the strategy aims to preserve technological sovereignty by investing in critical technologies (encryption, cloud computing, security assessment), supporting a competitive European market and strengthening international cooperation for a secure, open and stable cyberspace within the European Union, NATO and with its partners.

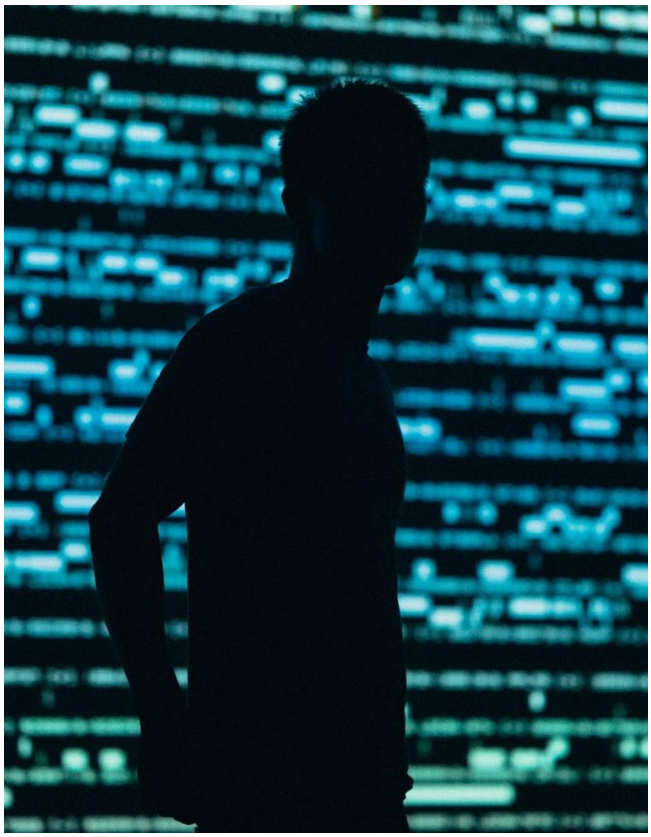
PERSONAL DATA NEWS

Abusive request for access rights under the GDPR

CJEU, C-526/24, Brillen Rottler GmbH & Co. KG v TC, 19 March 2026

On 19 March 2026, the CJEU clarified that a request for access to one's personal data may be deemed abusive and refused if it is made for the sole purpose of subsequently seeking compensation for an alleged breach of the GDPR.

In this case, an individual residing in Austria subscribed to the newsletter of the family-run opticians Brillen Rottler by entering his personal data into the registration form available on the company's website. Thirteen days later, he sent Brillen Rottler a request for access under the General Data Protection Regulation (GDPR).



Brillen Rottler rejected the request, considering it to be abusive. The company noted, through various news reports, blog posts and legal bulletins, that this individual systematically subscribes to newsletters from various companies before submitting a request for access, followed by a claim for compensation. The individual, for his part, considered his request for access to be legitimate and sought compensation of at least €1,000 from Brillen Rottler for the non-pecuniary damage he claimed to have suffered as a result of the rejection of his request.

The Arnsberg District Court, to which the case was referred, asked the Court of Justice of the European Union (CJEU) whether an initial request for access to personal data could be considered 'excessive' and whether the data subject was entitled to compensation for the damage resulting from a breach of the right of access.

The CJEU replied that an initial request for access may, in certain circumstances, be considered 'excessive' within the meaning of the GDPR and therefore be abusive. This is the case where the controller demonstrates that, despite formal compliance with the conditions laid down in the GDPR, the request was made not to ascertain the processing of data and verify its lawfulness, but with the abusive intention of artificially creating the conditions necessary to obtain compensation under the GDPR. The fact that the individual has, according to publicly available information, submitted several requests for access followed by claims for compensation to various controllers may be taken into account in establishing the existence of such an abusive intention.

Furthermore, the Court reiterated that a person who has suffered material or non-material damage as a result of a breach of the GDPR, including a breach of the right of access, is entitled to compensation. However, in order to obtain such compensation, the person must demonstrate that they have actually suffered damage. They cannot obtain compensation if their own conduct constitutes the decisive cause of the damage.

It is now for the Arnsberg District Court to rule on the dispute, taking into account these clarifications provided by the CJEU.

PERSONAL DATA NEWS

The Council of State rules on algorithmic video surveillance

Council of State, Municipality of Nice v CNIL, 30 January 2026, No. 506370

Following an inspection carried out in 2023, the CNIL had served formal notice on the Municipality of Nice to produce a data protection impact assessment concerning several algorithmic processing operations applied to CCTV footage.

In its opinion of 15 May 2025, the CNIL considered that the 'school entrance intrusion zone' system, designed to automatically detect, in real time, vehicles parked illegally outside schools in order to alert the municipal police, could not be implemented under the current applicable law.

The municipality of Nice brought an action before the Council of State seeking the annulment of the CNIL's decision of 15 May 2025 on the grounds of misuse of powers. The municipality also sought an order for the CNIL to pay the costs of the proceedings.

With regard to external legality, the Council of State ruled that the decision had been adopted in accordance with the proper procedures, both in terms of quorum rules and the requirements for stating reasons. The grounds of appeal based on a procedural irregularity and insufficient reasoning were therefore dismissed.

On the merits, the Council of State considered that whilst the Internal Security Code authorises the deployment of video surveillance systems on public roads, these provisions do not, in the absence of specific legislation, permit the systematic and automated algorithmic analysis of the images collected. As there is no other legal basis authorising such processing, the CNIL neither erred in law nor exceeded its powers in concluding that the system could not be deployed within the current legislative framework.

The application by the municipality of Nice and its claims regarding legal costs are therefore dismissed.

Implementation of pseudonymisation

Council of State, GERS v CNIL, 13 February 2026, No. 498628

In a decision of 13 February 2026, the Council of State reiterated that the processing of pseudonymised health data remains subject to the GDPR as long as the risk of re-identification is not zero.

A company challenged two decisions of the CNIL's restricted chamber taken on 28 August 2024, imposing fines of €800,000 and €200,000 respectively. These sanctions related to data processing carried out using databases sourced in particular from medical practices and pharmacies, in which the health data had only been pseudonymised. The company, however, argued that this data was anonymised and therefore did not fall within the scope of the GDPR, and sought, in the alternative, a review of the penalty or a preliminary ruling from the CJEU.

The Council of State, to which the case was referred, had to determine whether the data processed was truly anonymous, which would exclude it from the scope of the GDPR, or whether the risk of re-identification remained. The court noted that pseudonymisation, however extensive, does not constitute anonymisation where the risk of identifying a person is not negligible. The assessment must be concrete, based on all available data and sources, and not solely on the measures announced by the data controller.

In this case, the Council of State confirmed that the databases used contained pseudonymised health data, derived from medical or pharmaceutical software, and that this data remained re-identifiable given the possibility of cross-referencing with other information. Consequently, the court held that the processing did indeed fall within the scope of the GDPR and required a lawful basis, which was lacking. The company's arguments regarding the alleged anonymisation of the data or the absence of a reasonable risk of re-identification are therefore rejected.

Several breaches were therefore found, notably regarding the lawfulness of the processing, the protection of health data and the lack of appropriate consent, thereby confirming the CNIL's sanctions. The Council of State also refused to refer the question for a preliminary ruling to the CJEU, considering that the applicable legal framework is clear.

PERSONAL DATA NEWS

Access to an employee's file in the context of an internal investigation

Court of Cassation, Social Chamber, Saleforce.com v M.[D][I], 14 January 2026, 24-13.234

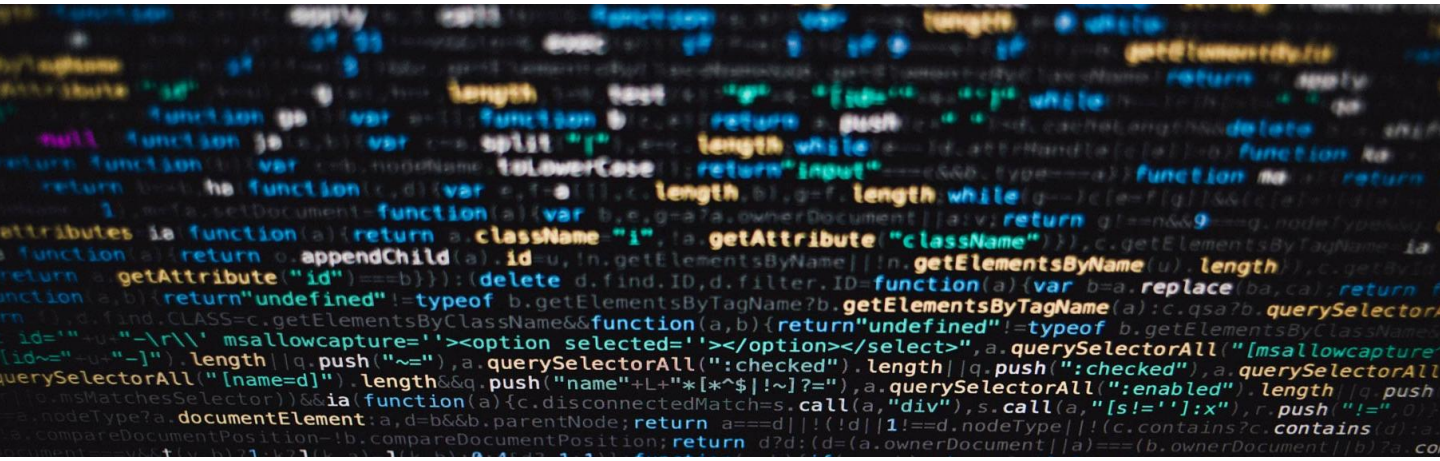
In a judgment of 14 January 2026, the Court of Cassation reiterated the scope of the right of access to the file in the context of an internal investigation prior to dismissal. Seized of the case by a former employee of a company, the judges had to determine whether the lack of full access to the investigation rendered the dismissal unlawful.

A regional vice-president, dismissed for serious misconduct following an internal investigation triggered by a whistleblowing mechanism, contested the validity of the termination. In particular, he argued that the employer had breached the company's code of conduct by failing to provide him with detailed information regarding the alleged facts or the identities of the persons concerned, and by denying him access to the investigation report, thereby rendering his dismissal unlawful.

The Court rejected this argument, noting that the code of conduct governing the whistleblowing procedure does not create a separate disciplinary procedure. It merely sets out the procedure for handling whistleblowing reports but does not require the exhaustive and detailed disclosure of all the facts reported, nor the identity of any victim

The High Court affirmed that, in the context of an internal investigation aimed at verifying reported facts, respect for the rights of the defence and the adversarial principle does not imply a right of full access to the investigation file, the disclosure of all documents gathered, or a confrontation with the employees who had accused the employee.

It is sufficient for the employee to be informed of the existence of the investigation and the nature of the allegations, and to be given the opportunity to explain themselves before the decision to dismiss is taken.



The CNIL sanctions France TRAVAIL for lack of data security

CNIL, France Travail, decision SAN–2026-003, 22 January 2026

Following a breach in 2024, attackers gained access to France Travail's information system using social engineering techniques that exploited people's trust, ignorance or credulity. This enabled them to take control of the accounts of advisers at CAP EMPLOI, an organisation specialising in employment for people with disabilities.

This attack gave them access to the data of everyone who had registered over the past 20 years, as well as those who had a candidate account on France Travail, including National Insurance numbers, email and postal addresses, and telephone numbers. The attack did not allow them to access complete files that might contain sensitive data such as health information.

The CNIL's investigation revealed serious shortcomings in the technical and organisational measures implemented by France Travail to ensure the security of the personal data processed, which could have made the breach more difficult.

The CNIL identified the following breaches:

- The authentication methods allowing CAP EMPLOI advisers to access the France Travail information system were not sufficiently robust.
- There were no logging measures in place to detect unusual behaviour on the information system.
- Access permissions for CAP EMPLOI advisers' accounts had been defined too broadly, allowing CAP EMPLOI advisers to access data on individuals they were not supporting, which increased the volume of data accessible to hackers.

These breaches constitute a violation of Article 32 of the GDPR, which requires the data controller and the processor to ensure the security of personal data by implementing security measures appropriate to the risks.

The CNIL's restricted chamber imposed a fine of €5 million on France Travail and ordered the organisation to implement corrective measures according to a specific timetable, subject to a penalty payment of €5,000 per day of delay. The penalty takes into account the fact that most of the impact assessments carried out by France Travail prior to the implementation of the data processing had already identified adequate security measures, but these had not been implemented.

PERSONAL DATA NEWS

CNIL fines a company for transferring data for targeted advertising purposes

CNIL, anonymous, decision SAN-2025-017, 30 December 2025

In January 2023, the CNIL conducted several investigations into a company, during which it discovered that the company had, for several years, been transmitting the email addresses and/or telephone numbers of members of its loyalty programme to a social media platform for the purposes of targeted advertising.

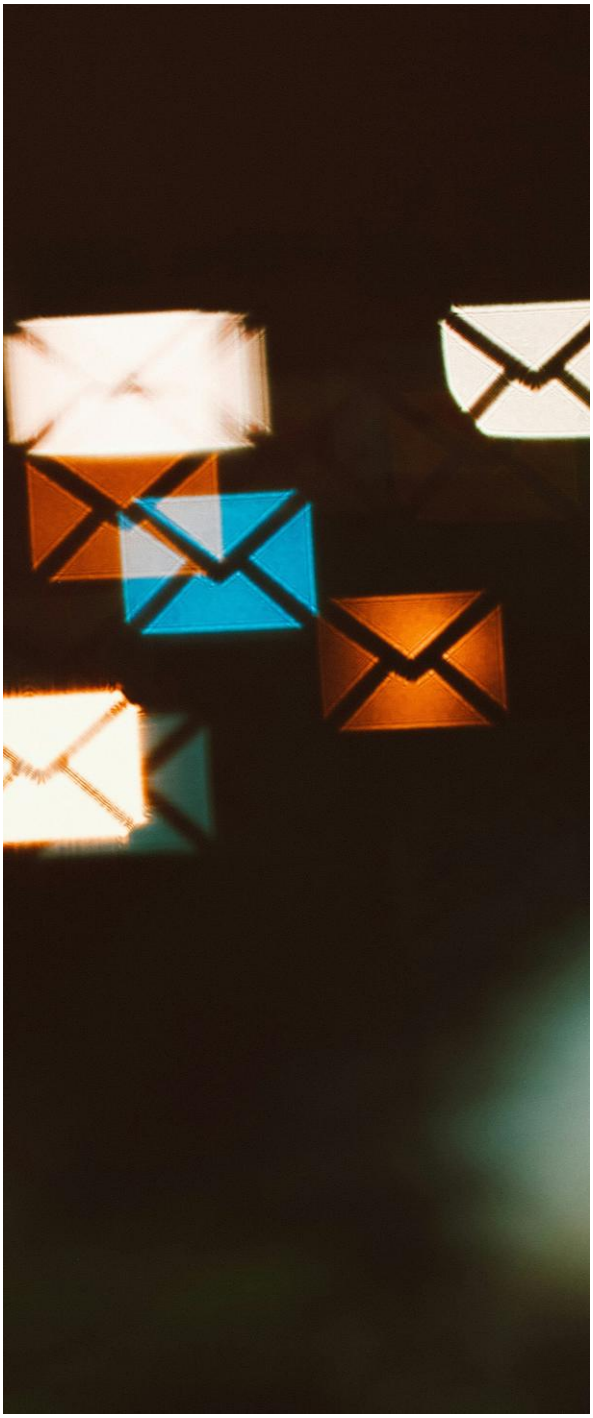
Following these investigations, the CNIL identified several breaches of the requirements of the GDPR and the French Data Protection Act:

- The consent of the data subjects had not been obtained lawfully, as no information had been provided or clearly indicated in the registration form or in the accessible documents concerning the transfer of data for advertising purposes. The consent given by the data subjects was neither explicit nor informed, which constitutes a breach of the obligation to have a legal basis in accordance with Article 6 of the GDPR.
- The purposes of the data processing were provided inaccurately and incompletely, which constitutes a breach of Articles 12 and 13 of the GDPR relating to the obligation to inform data subjects.
- The rules regarding the complexity of user account passwords were not sufficiently robust, which constitutes a breach of the obligation to ensure data security (Article 32 of the GDPR).
- The company had not carried out an impact assessment, even though the processing of targeted advertising posed a high risk to the rights and freedoms of data subjects, which constitutes a breach of Article 35 of the GDPR.
- The CNIL found that eleven consent-based cookies were placed on users' devices as soon as they visited the website, were not deleted and continued to be read even after consent had been refused, in breach of Article 82 of the French Data Protection Act.

The CNIL and its 16 European counterparts imposed a fine of €3.5 million on the company and decided to publish their deliberations in order to highlight the rules applicable to targeted advertising on social media. The amount of the fine takes into account the large number of data subjects involved (over 10.5 million) and the widespread nature of these practices.

PERSONAL DATA NEWS

CNIL sanctions against FREE and FREE MOBILE



CNIL, FREE and FREE MOBILE, decision SAN-2026-001, 8 January 2026

On 13 January 2026, the CNIL issued two penalty decisions against FREE and FREE MOBILE, imposing fines of €27 million and €15 million respectively, given the inadequacy of the measures taken to ensure the security of their subscribers' data.

In October 2024, an attacker managed to breach the companies' IT systems and gain access to personal data relating to 24 million subscriber contracts. Certain sensitive information was compromised, including IBANs for customers using services provided by both companies. This data breach led to more than 2,500 complaints from affected individuals, prompting the CNIL to launch an investigation.

Following the investigation, the CNIL identified several breaches of the GDPR:

- The security measures put in place to protect the data were deemed insufficient: for example, authentication to access the internal VPN was not robust enough and the mechanisms for detecting suspicious activity ( ) were ineffective. These weaknesses facilitated the attack and demonstrated that data protection was not commensurate with the sensitivity and volume of the information processed.
- The CNIL also criticised the companies for failing to properly inform those affected by the data breach: the email sent did not contain all the information required by the GDPR to understand the risks and possible protective measures. Furthermore, FREE MOBILE retained data on former subscribers for an excessive period, without adequate mechanisms for sorting or deletion.

Consequently, the CNIL imposed a fine of €27 million on FREE MOBILE and €15 million on FREE, totalling €42 million. The companies were also ordered to rapidly strengthen their security measures and improve the management and deletion of personal data.

PERSONAL DATA NEWS

The CNIL publishes its final recommendations on multi-device consent

Recommendation proposing practical methods for ensuring compliance with multi-device consent, 18 December 2025

The CNIL has published its final recommendations on multi-device consent for the use of cookies and other trackers, to help data controllers comply with the GDPR and the French Data Protection Act. These recommendations concern web environments and mobile applications, but may also guide other contexts requiring consent, such as smart TVs, games consoles, voice assistants, connected devices or connected vehicles. They apply to users logged into an account as well as to unauthenticated users, even though multi-device consent itself applies only to logged-in users.

Multi-device consent allows a user to set their preferences regarding cookies and trackers on one device and have them automatically applied to all their other devices linked to the same account. This mechanism is optional, but it must comply with the principles of free, informed, specific and unambiguous consent. The user must be informed of the scope of their choices before making them, and must be able to manage their preferences on each device via a control panel or a preferences centre.

The CNIL also recommends establishing clear procedures to manage conflicts between choices made on an unauthenticated device and those recorded in the account. Two approaches are possible: either the most recent choices made on a device override those in the account, or the account's choices take precedence. In all cases, the user must be informed of the situation and of the means to change their choices.

Furthermore, data controllers must minimise the personal data transmitted to external service providers involved in consent management, for example by using a technical identifier rather than the account identifier containing personal information. Finally, when implementing a multi-device mechanism, it is necessary to obtain new consent so that the user is informed of the multi-device scope of their choices.

QUICK FACTS

On 27 January 2026, the European Commission adopted an adequacy decision recognising that Brazil ensures a level of personal data protection that is 'essentially equivalent' to that of the European Union, thereby allowing personal data to flow between the EU and Brazil without additional formalities.

Stéphanie Berland

Partner

T: +33 1 40 69 26 63

E: s.berland@dwf.law

Emmanuel Durand

Partner

T: +33 1 40 69 26 83

E: e.durand@dwf.law

Florence Karila

Partner

T: +33 1 40 69 26 57

E: f.karila@dwf.law

Anne-Sylvie Vassenaix-Paxton

Partner

T: +33 1 40 69 26 51

E: as.vassenaix-paxton@dwf.law

DWF is a leading global provider of integrated legal and business services.

Our Integrated Legal Management approach delivers greater efficiency, price certainty and transparency for our clients.

We deliver integrated legal and business services on a global scale through our three offerings; Legal Services, Legal Operations and Business Services, across our nine key sectors. We seamlessly combine any number of our services to deliver bespoke solutions for our diverse clients.

dwfgroup.com