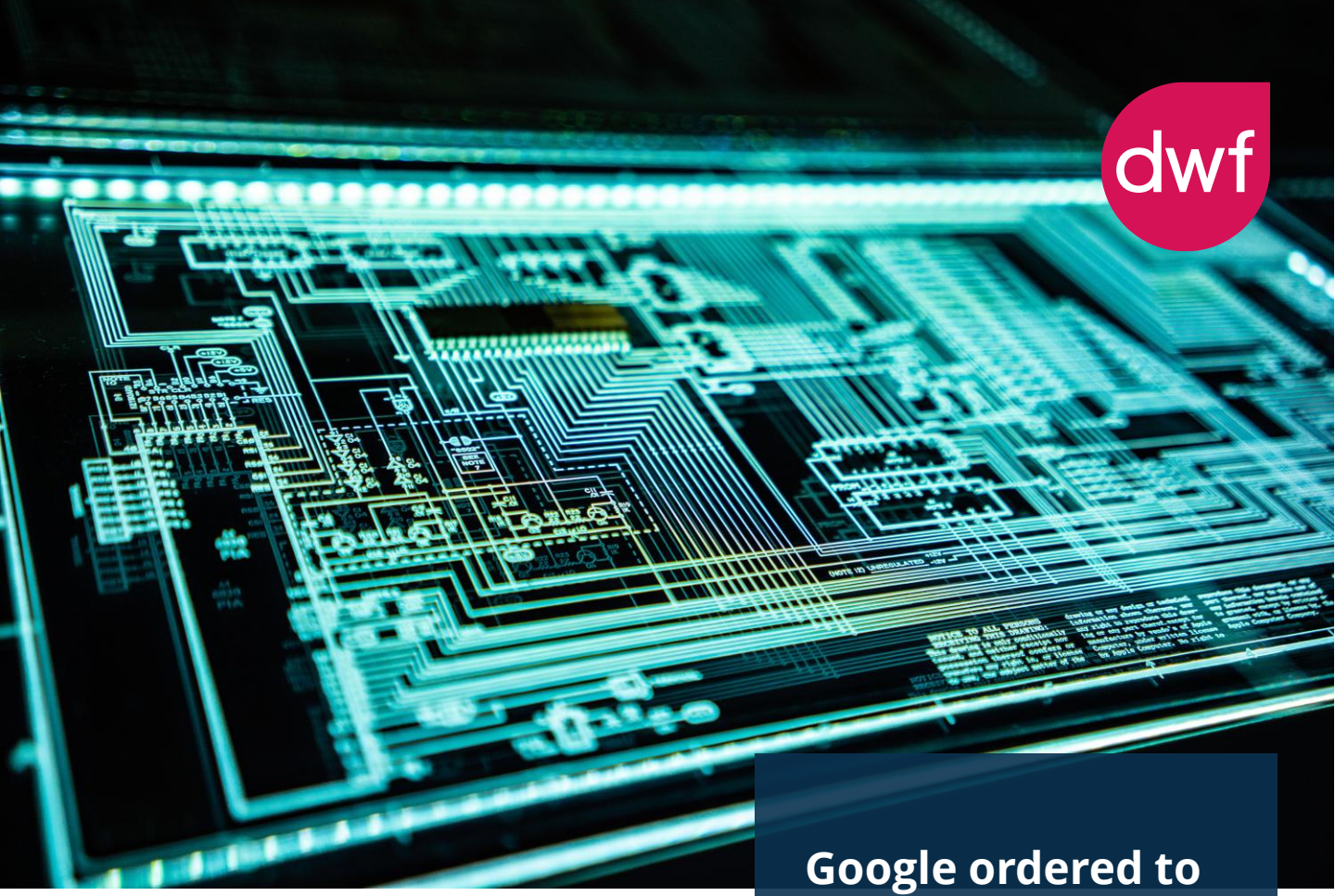


Newsletter

Tech / Data

2nd QUARTER - 2026

dwfgroup.com

Google ordered to pay €22.69 million in damages to M6 for abuse of dominant position

On 10 March 2026, the Paris Economic Activities Court sanctioned Google for favouring its advertising platform AdX, finding that these practices had harmed publishers, including M6. As a result, Google was ordered to pay €22.69 million in damages to M6 for abuse of its dominant position.

In this issue

LATEST NEWS - TECHNOLOGIES

DNS providers may be subject to blocking measures

Paris Court of Appeal, 13 May 2026, No. 24/19156

In a judgment dated 13 May 2026, the Paris Court of Appeal confirmed that blocking measures may be imposed on technical intermediaries other than internet service providers, in particular domain name system (DNS) service providers, as part of the fight against sports piracy.

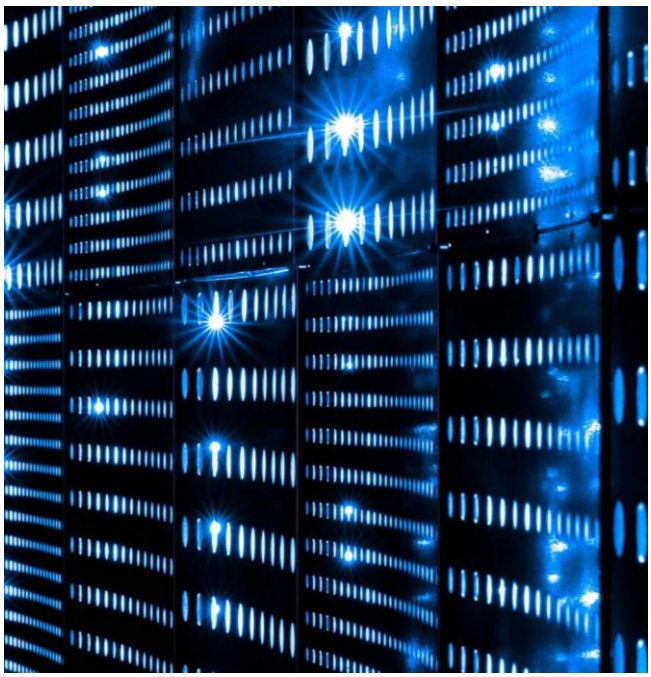
In this case, the Canal+ group sought, on the basis of Article L.333-10 of the Sports Code, the imple-mentation of measures designed to prevent access, from within France, to websites broadcasting the 2024/2025 Champions League matches without authorisation. The Paris Judicial Court had granted these requests by ordering several technical intermediaries, including DNS providers, to implement blocking measures.

On appeal, the Court first confirmed the standing of the Canal+ group companies to bring proceedings, holding that they hold exclusive audiovisual exploitation rights as well as neighbouring rights in the pro-grammes broadcast.

The main significance of the judgment lies in the classification of the parties targeted by the injunctions. Indeed, the Court adopts a broad interpretation of the concept of a 'person capable of helping to remedy the infringement' and rules that DNS service providers constitute technical intermediaries within the meaning of EU law. It notes that, even though their role is neutral and automated, these services enable users to access the disputed websites by translating domain names into IP addresses. They thus indi-rectly contribute to the transmission of unlawful content and may, as such, be subject to blocking in-junctions. The Court also confirms the existence of serious and repeated infringements of the rights holder's rights, characterised by the systematic broadcasting of matches via streaming websites and IPTV services accessible from France.

As regards the measures ordered, the Court upheld their proportionality. It considered that DNS block-ing, although imperfect and subject to circumvention, constitutes an effective means of making access to unlawful content more difficult and of deterring users.

Arguments relating to the technical complexity and cost of these measures were also dismissed, as the Court found that the operators concerned had not demonstrated that implementing these measures would entail disproportionate changes to their technical architecture.



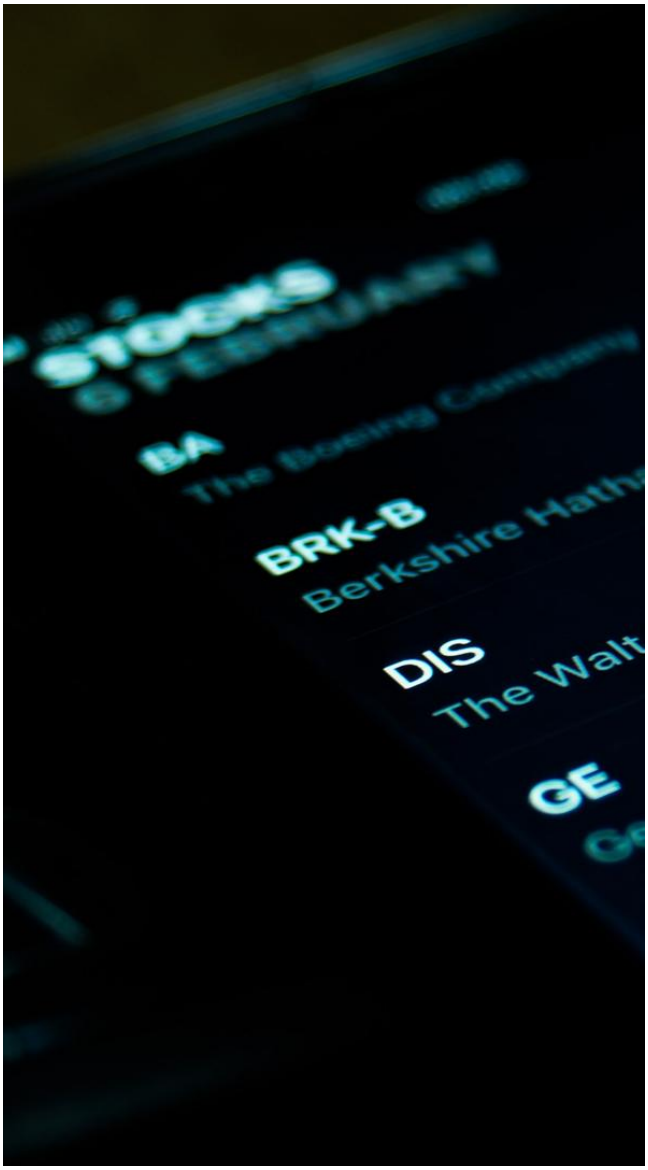
Furthermore, the Court of Appeal upheld the use of so-called 'dynamic' injunctions, which allow blocking measures to be extended to sites not yet identified, under the supervision of ARCOM, in order to adapt to the evolving nature of piracy practices.

Finally, the Court rejected the requests for a preliminary ruling from the CJEU as well as the challenges based on EU law, considering in particular that the measures in question do not constitute general res-trictions on the freedom to provide services but are targeted and proportionate measures.

LATEST NEWS - TECHNOLOGIES

€200 million fine imposed on TEMU under the DSA

DSA: Commission imposes a €200 million fine on Temu, 28 May 2026



On 28 May 2026, the European Commission imposed a fine of €200 million on Temu under the Digital Services Act (DSA) for failing to fulfil its obligations to assess systemic risks.

The Commission criticises Temu for failing to diligently identify, analyse and assess the risks associated with the presence of illegal and dangerous products on its platform (baby toys, chargers, etc.), or the resulting harm to consumers in the European Union.

The evidence gathered by the Commission, notably from Temu's 2024 risk assessment report and 2025 interim report, responses to formal requests for information, and a mystery shopper exercise carried out by an independent testing body, demonstrates that European consumers are highly likely to encounter illegal items on the platform.

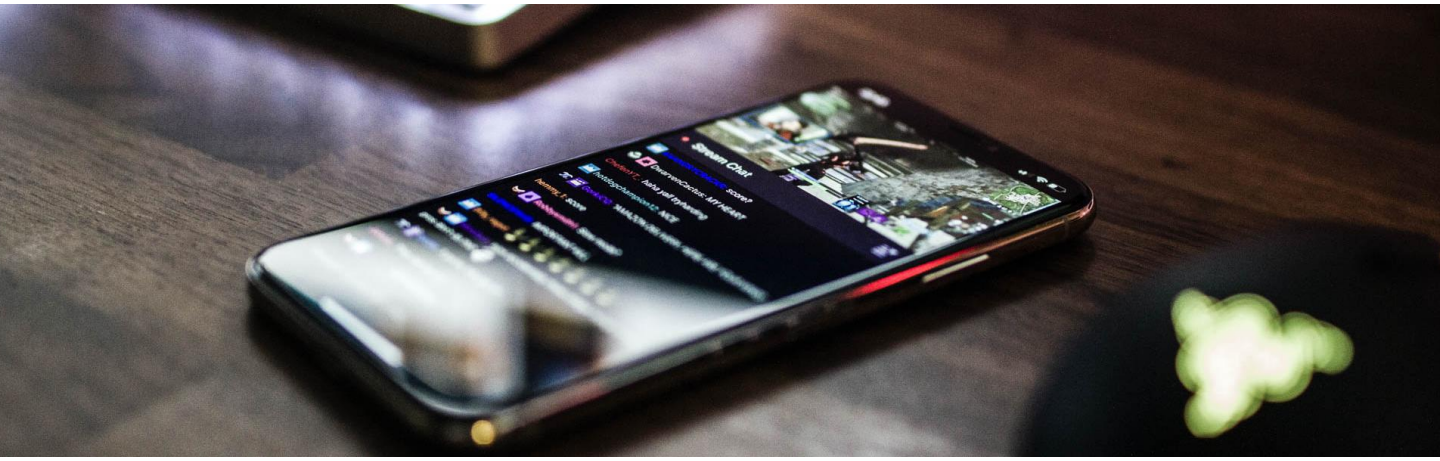
Furthermore, the risk assessment carried out by Temu in 2024 did not comply with the standards set out in the DSA, in particular because it was based on general data relating to the e-commerce sector rather than on evidence specific to its own service.

This procedure, which was launched on 31 October 2024 and was the subject of preliminary findings in July 2025, has therefore concluded with a decision of non-compliance. The amount of the fine was determined by taking into account the nature of the infringement, its seriousness in view of the number of European users affected and its duration; the Commission considers that the failure to carry out an adequate risk assessment constitutes a particularly serious breach of one of the cornerstones of the DSA.

In accordance with Article 75 of the Regulation, Temu has until 28 August 2026 to submit an action plan setting out the proposed remedial measures. This plan will be submitted to the European Digital Services Board for its opinion; the Board will have one month to give its view, before the Commission adopts its final decision within a further month and sets a timetable for compliance. Failure to comply with this decision could result in further periodic penalty payments.

This action forms part of a wider drive by the European authorities against major low-cost e-commerce platforms such as Shein and AliExpress, which are also under investigation for potential breaches of the DSA rules, particularly regarding product safety, consumer protection and the management of systemic risks.

LATEST NEWS - TECHNOLOGIES



Partial annulment of Meta's designation as an access controller

General Court of the European Union, 8th Chamber, Meta Platforms, Inc. v European Commission, 3 June 2026, T-1078/23

In a judgment of 3 June 2026, the General Court of the European Union partially annulled the European Commission's decision of 5 September 2023 designating Meta as an access controller under the Digital Markets Act (DMA).

The General Court thus annulled the designation of Meta as an access controller in respect of Marketplace, whilst upholding that of Messenger.

With regard to Messenger, the General Court confirmed that it constitutes a person-to-person communications service that is not based on the distinct numbering of the Facebook social network. It emphasised that this service is offered via standalone applications, can be used independently of Facebook and is subject to specific tools enabling businesses to interact with users. The arguments relating to the integration of services were not deemed sufficient to call this classification into question. The General Court also upholds the Commission's assessment that Messenger, on its own, constitutes a major access point. As such, the Commission was not required to exclude from the calculation of end-users those who also use Facebook, nor to launch a market in nquiry in the absence of sufficiently substantiated evidence provided by Meta to rebut the presumptions laid down in the DMA.

As regards Marketplace, however, the General Court criticises the Commission's analysis. It points out that the legality of a Union act must be assessed in the light of all the factual and legal elements existing at the date of its adoption. However, the Commission committed an error of law by limiting its examination to data from the preceding three years without taking into account the changes introduced on 31 July 2023. These changes consisted of a limit on the number of listings that could be published per user and had the effect of removing the criterion used by the Commission to identify user undertakings.

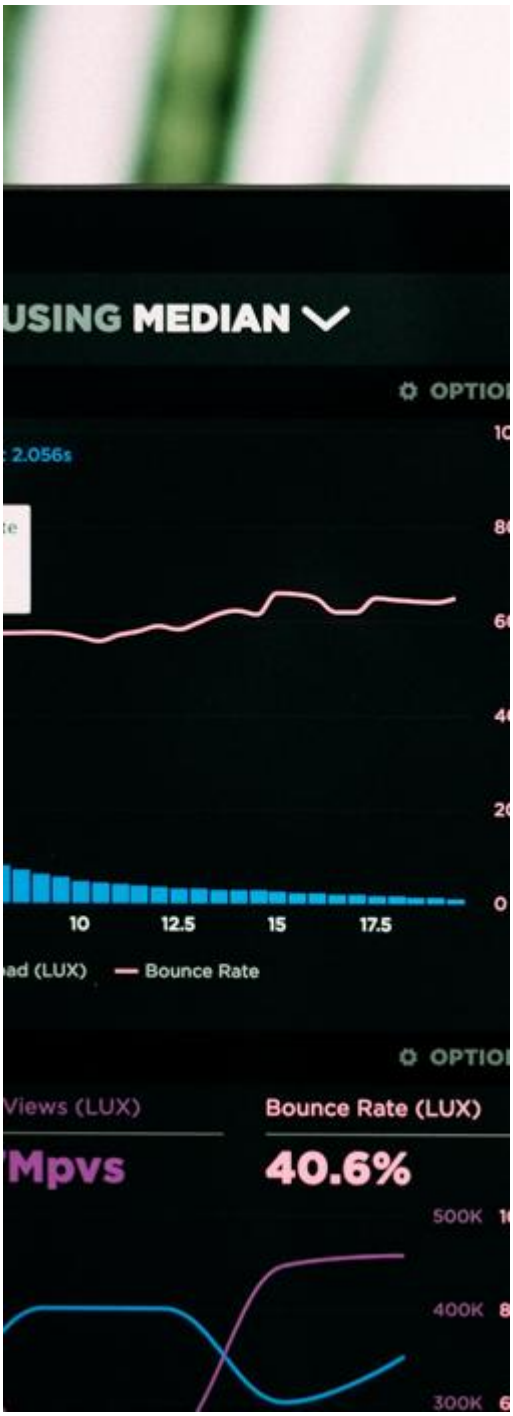
Furthermore, the General Court notes a failure to state reasons, finding that the Commission provided no concrete analysis of the impact of those changes on the classification of Marketplace as an online intermediation service, relying instead on hypothetical and incomplete evidence. In those circumstances, the decision did not enable Meta to understand the reasons for classifying the service as an essential online intermediation service, nor did it enable the EU court to carry out its review.

PERSONAL DATA NEWS

Non-compliance with the GDPR renders the contract void on the grounds of a mistake regarding the essential characteristics of the website

Douai Court of Appeal, Chamber 2, Section 2, 7 May 2026, No. 22/05075

Lyon Court of Appeal, 6th Chamber, 5 March 2026, No. 24/02311



In a judgment of 7 May 2026, the Douai Court of Appeal declared a contract for the creation and hosting of a website null and void on the grounds that the website delivered did not comply with the mandatory rules relating to the protection of personal data.

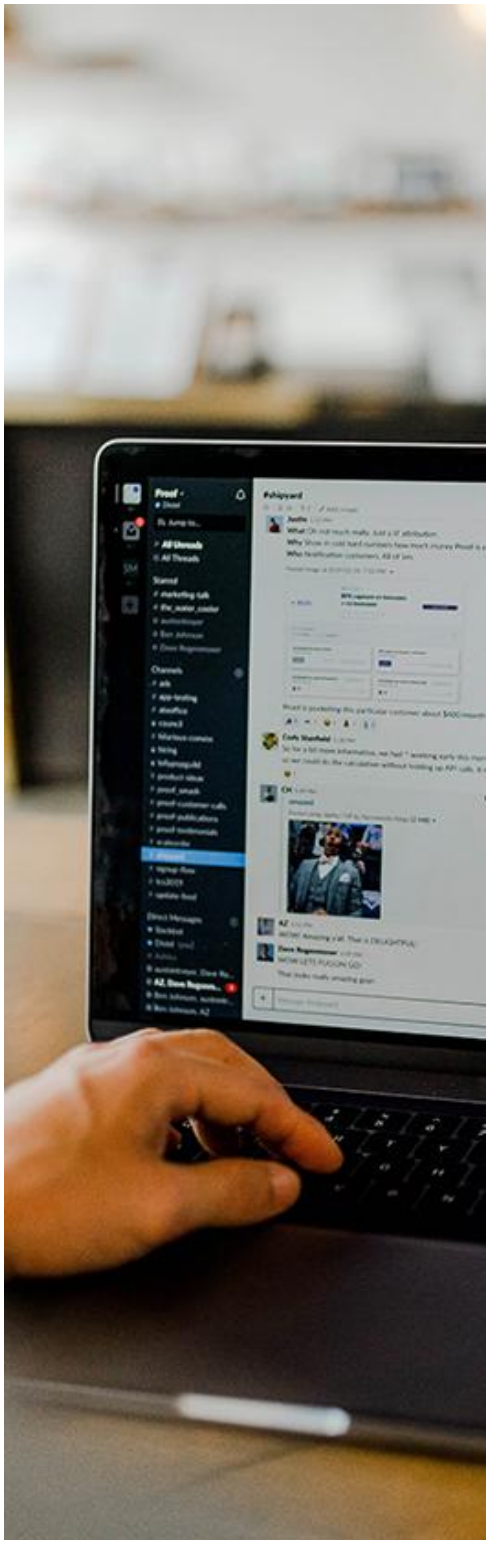
In this case, a company had entered into a subscription contract with a web agency for the creation and operation of a website. After the website went live, the company had a bailiff certify the presence of cookies placed without prior consent, as well as data collection mechanisms (contact form and call-back button) lacking any information compliant with the GDPR.

Having lost its case at first instance, the client company lodged an appeal, arguing in particular that there had been a fundamental defect in the service due to the website's non-compliance with data protection regulations.

Firstly, the Court ruled out the application of consumer law, noting that the client company had failed to provide evidence that it employed no more than five staff members at the time the contract was concluded – a condition required to benefit from the protective provisions applicable to professionals treated as consumers.

However, the trial judges held that a website's compliance with data protection rules constitutes an essential quality tacitly agreed between the parties. They identified several serious breaches, in particular the automatic installation of cookies simply by browsing the site, without first obtaining the consent of internet users, even though some of these cookies were used for advertising purposes. The judges also noted the absence of an effective mechanism allowing users to refuse cookies at the initial information stage or to withdraw consent in a manner as simple as that used to grant it. In addition to these breaches, there was a complete lack of information provided to users regarding the processing of personal data carried out via contact forms and reminder systems, in breach of the requirements of the GDPR.

PERSONAL DATA NEWS



The Court emphasises that the use of a specialist professional justified the expectation that the site would comply with regulations, particularly as such breaches expose the client to significant legal and financial risks. It concludes that these factors vitiated the consent of the client company, which would not have entered into the contract, or would have done so on different terms, had it been informed of these non-compliances. The contract is therefore set aside on the grounds of a mistake regarding an essential quality of the service.

Compliance with the GDPR is thus recognised as an essential quality of the website creation service, and a failure to recognise this may vitiate consent and render the contract void.

This decision forms part of a line of case law already established by the Lyon Court of Appeal on 5 March 2026. In that case, a tradesperson had entered into a contract with Linkeo.com for the creation and launch of a website, together with a maintenance service. Following non-payment, the dispute led the client to seek the nullity of the contract, citing, in particular, the website's non-compliance with the requirements of the GDPR.

Upholding the judgment at first instance, the Lyon Court of Appeal also found that there was a defect in consent resulting from serious breaches of the rules on the protection of personal data. It noted, in particular, that cookies were installed without complying with the requirements of the GDPR, that refusing them did not prevent them from being placed, that withdrawing consent was not as straightforward as granting it, and that the mandatory information relating to data processing was missing.

PERSONAL DATA NEWS

The CJEU imposes strict rules on the collection of biometric data in criminal matters

CJEU, Comdribus, 19 March 2026, C-371/24

In a judgment of 19 March 2026, the Court of Justice of the European Union ruled on the compliance with EU law of French legislation authorising the collection of fingerprints and photographs of any person suspected of having committed or attempted to commit a criminal offence, as well as on the possibility of imposing criminal penalties for refusing to submit to such biometric data collection procedures.

The case concerned an individual who had been arrested during a demonstration and prosecuted for refusing to submit to biometric data collection, even though he had subsequently been acquitted of the offence that had led to his arrest. Convicted solely for refusing to provide the samples, he challenged the compatibility of this conviction with Directive (EU) 2016/680, known as the 'Police-Justice' Directive.

In response to a request for a preliminary ruling from the Paris Court of Appeal, the CJEU first of all noted that fingerprints and photographs constitute biometric data falling within the special categories of personal data, the processing of which is permitted only in cases of 'absolute necessity' within the meaning of Article 10 of Directive 2016/680 and where there are appropriate safeguards for the rights and freedoms of the data subject.

The Court states that the mere fact that there are one or more plausible grounds for suspecting that a person has committed or attempted to commit an offence is not, in itself, sufficient to justify the systematic collection of their biometric data. Such collection is consistent with EU law only if national law defines the purposes pursued with sufficient precision and requires the competent authority to assess, in each individual case, whether that collection is absolutely necessary and proportionate in the light of those purposes.

Furthermore, the Court of Justice states that Article 10 of the Directive imposes a duty on the competent authority to provide a clear statement of reasons. The competent authority must be able to set out, for each data subject, the reasons why the collection of biometric data is absolutely necessary. Such a statement of reasons constitutes an essential safeguard enabling the data subject to understand the reasons for that measure, to be able to exercise their right to an effective judicial remedy, and to enable the competent court to review the lawfulness of that measure. The Court also emphasises that the obligation on the competent authority to justify the 'strictly necessary' nature of the collection does not constitute an excessive constraint, in that such collection cannot, in any event, be systematic in respect of persons reasonably suspected of having committed or attempted to commit a criminal offence on one or more grounds.

Finally, as regards the criminal penalty for refusing to provide biometric data, the Court considers that EU law does not, in principle, preclude national legislation allowing a person to be prosecuted and convicted for such a refusal, even in the absence of prosecution or conviction for the original offence. This possibility of a penalty remains, however, subject to the dual condition that the proposed collection is strictly necessary and that the penalty imposed is proportionate.

PERSONAL DATA NEWS

Decision of the Council of State – data transfer

Council of State, Association les licornes célestes and others v Association Interhop, 20 March 2026, Nos 503159, 504171

In a ruling dated 20 March 2026, the Council of State ruled on the legality of a decision by the CNIL authorising the European Medicines Agency to process health data as part of the DARWIN EU project. This project aims to strengthen collaboration between regulatory agencies and researchers from various European countries through a network for sharing data, resources and expertise.

Several organisations challenged this authorisation on the grounds that Microsoft Ireland, a subsidiary of the US-based company Microsoft, was to be used to host data from the National Health Data System (SNDS). In particular, they cited the risk of data being transferred to the United States and the inadequacy of the technical and legal safeguards put in place.

In this ruling, the Council of State dismissed all the appeals and upheld the CNIL's position. It noted, first of all, that the disputed decision authorises only the processing of health data where such data is hosted in centres located in France, and has neither the purpose nor the effect of authorising the transfer of health data to the United States. The applicants cannot therefore validly argue that the EU–US adequacy decision is unlawful, nor can they claim a breach of the prohibition on transfers outside the European Union.

The High Court also distinguishes between health data and technical data relating to the use of the platform. Whilst the latter may be transferred to the United States, it does not contain any sensitive data and is governed by standard contractual clauses constituting appropriate safeguards within the meaning of the GDPR.

With regard to compliance with the requirements of the GDPR, the Council of State acknowledges that access to the data by the US authorities cannot be entirely ruled out. However, it considers that the measures put in place – such as pseudonymisation, limitation of the retention period, analysis of re-identification risks and traceability of access – offer sufficient safeguards in accordance with Articles 28 and 32 of the GDPR. Furthermore, the Council of State points out that, although Microsoft Ireland holds the 'SecNumCloud' certification issued by ANSSI, it also holds the 'health data host' certification provided for in the Public Health Code (Article L. 1111-8 CSP).

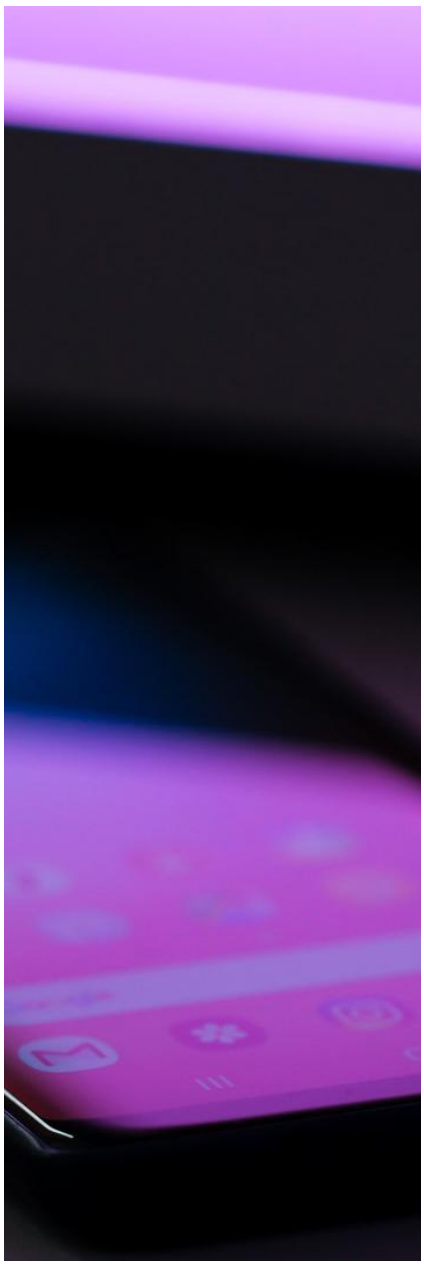
Finally, the judge declined to refer the matter to the Court of Justice of the European Union, considering that no serious difficulty in interpreting EU law justified a preliminary ruling.

This decision confirms a pragmatic approach by the administrative court regarding data transfers, based on a practical assessment of the safeguards put in place. It thus permits the use of service providers based in third countries, including the United States, provided that no transfer of sensitive data is authorised and that appropriate safeguards are effectively in place.

PERSONAL DATA NEWS

The CNIL regulates the use of tracking pixels in emails

CNIL, recommendation on tracking pixels in emails, 12 March 2026



In a recommendation adopted on 12 March 2026, the CNIL sets out guidelines for the use of tracking pixels in emails, an increasingly widespread practice used to measure whether messages are opened or to track recipients' behaviour.

These pixels, which are generally invisible, rely on the remote loading of an image containing identifiers that enable the collection of information such as whether an email has been opened, the IP address or the device used. The CNIL points out that their use constitutes the reading of information from the user's device and, as such, falls under Article 82 of the Data Protection Act, which transposes the ePrivacy Directive.

The recommendation first sets out the division of roles between the various parties involved. The sender of the email is, in principle, the data controller, including where the pixels are implemented by an email service provider acting as a data processor. Where several parties are involved in determining the purposes of the processing, particularly where data is used for their own purposes, a situation of joint responsibility may apply.

With regard to the conditions of lawfulness, the CNIL states that the use of tracking pixels generally requires the prior consent of the recipient. Such consent is required, in particular, where pixels are used to analyse campaign performance, personalise communications, create profiles or detect fraudulent behaviour. Conversely, certain purposes may be exempt from the consent requirement where they are strictly necessary for the requested service . This includes, in particular, security measures contributing to authentication or certain operations limited to managing email deliverability, provided that they comply with the principle of data minimisation and relate to messages requested by the user, such as transactional emails.

The CNIL also emphasises the procedures for obtaining consent. It recommends that consent be obtained at the time the email address is provided, in order to ensure clear information is given regarding the future use of trackers. Failing that, consent may be obtained at a later stage via an email containing no tracking pixels, linking to a dedicated interface requiring positive action on the part of the user.

Finally, the recommendation reiterates the standard requirements of the GDPR, in particular the right to withdraw consent at any time, the need to retain proof of consent, and the obligation to provide clear and accessible information on the purposes for which data is processed.

PERSONAL DATA NEWS

The Constitutional Council puts an end to the accumulation of penalties in relation to electronic marketing

Constitutional Council, Decision No. 2026-1210 QPC, Orange SA, 25 June 2026

Following a referral of a priority preliminary ruling on constitutionality (QPC) by Orange SA, the Constitutional Council ruled on the constitutionality of the provisions of Article L.34-5 of the Post and Electronic Communications Code relating to penalties applicable in the event of direct marketing carried out without the prior consent of the individuals concerned.

In this case, these provisions allowed three separate administrative authorities – the CNIL, ARCEP and the administrative authority responsible for competition and consumer affairs – to impose penalties for the same breaches. The applicant companies argued that this system contravened the constitutional principle of the necessity of offences and penalties by permitting multiple prosecutions and penalties for identical acts.

The Constitutional Council accepts this argument. It notes that the three authorities are competent to penalise the same acts, classified in the same way, by means of administrative sanctions of the same nature, in pursuit of a common objective of protecting users' privacy against unsolicited commercial communications. Such a system disregards the principle of the necessity of offences and th ity of penalties, guaranteed by Article 8 of the 1789 Declaration of the Rights of Man and of the Citizen. The contested provisions are therefore declared to be contrary to the Constitution.

However, in order to avoid the immediate call into question of all ongoing proceedings, the Council has postponed the repeal of the provisions until 31 October 2027. In the meantime, it stipulates that no new proceedings may be brought by another authority where proceedings have already been initiated or where a final penalty has already been imposed for the same acts.

This decision illustrates the central role of the QPC in the scrutiny of punitive measures. The Constitutional Council reiterates that, even in highly regulated areas such as the protection of personal data and electronic communications, the legislature cannot establish multiple enforcement regimes leading to the sanctioning of the same acts in the name of the same social interests. This decision will inevitably lead the legislature to review the coordination of the sanctioning powers of the various independent administrative authorities.

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 key market groups. We seamlessly combine any number of our services to deliver bespoke solutions for our diverse clients.

dwfgroup.com