EUROPEAN LAWYERS
EUROPEAN BARS CCBE BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of European lawyers

Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

CCBE position paper on the proposal for the EU Cloud and AI Development Act (CADA)

19 November 2026

The CCBE welcomes the Commission proposal for the Cloud and AI Development Act (CADA)[1], in particular its aim of strengthening Europe's cloud and AI ecosystem, reducing strategic dependencies in critical digital infrastructure and introducing a single EU-wide framework for assessing cloud and AI sovereignty.

1. General remarks

The CCBE broadly supports the direction of the proposal since it recognises that certain public functions, such as the justice system, require a higher level of operational control, resilience, security and protection against external dependencies. The CCBE maintains its earlier view that justice system should be considered as critical infrastructure for our societies: essential to social cohesion, rule of law and democratic resilience. As a result, it must be supported, protected and resourced accordingly.[2] Furthermore, the proposal must not interfere with the principle of independence of the justice system.

1.1. Independence of the justice system

The CCBE stresses that to maintain its independence, the justice system must retain effective control over critical digital services and must operate in an environment guaranteeing strong safeguards, especially in relation to protecting sensitive and/or privileged data and ensuring service continuity.

Such control should include at minimum the clarity as to who operates the service, where data are processed and stored, who may access the systems, laws regulating provider's obligations to disclose data to law enforcement authorities and laws regulating provider's ability to provide continuity of service.

As the administration of justice becomes increasingly dependent on digital infrastructure, questions about the continuity, governance, ownership, applicable law, subcontracting and technical architecture of these services become important from the perspective of rule of law. This is because a failure of continuity of service, inability to access case files, unlawful or insufficiently safeguarded

[1] Proposal for the Cloud and AI Development Act (CADA): https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada (3 June 2026)

[2] CCBE response to the call for evidence for the EU Cloud and AI Development Act: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20250701_CCBE-response-to-the-call-for-evidence-for-the-EU-Cloud-and-AI-Development-Act.pdf (July 2025)

disclosure of confidential information, or dependence on a provider subject to conflicting legal obligations may affect not only administrative efficiency but also access to justice, equality of arms, rights of defence and the confidentiality of lawyer-client communications.

1.2. Sovereign infrastructure and regulatory ecosystem

The CCBE stresses that sovereign infrastructure must be accompanied by legality, necessity, proportionality, independent oversight, effective remedies and specific safeguards for information covered by professional secrecy or legal professional privilege. The CCBE considers that CADA's requirements should be designed to support and strengthen existing European alternatives. They should not impose requirements that are not yet fully achievable in practice, as this could disproportionately affect lawyers and other justice actors who depend on available service providers and cannot themselves develop the necessary technological alternatives.

While European technological sovereignty can reduce certain third-country dependencies and risks of conflict of laws, it does not, by itself, guarantee compliance with the rule of law. Therefore, it must operate within a broader framework which respects fundamental rights.

From the point of view of the legal profession, the following issues have been of particular significance:

- creating technical means to identify data protected by professional secrecy/legal professional privilege in an online environment;
- protection of such data from disclosure and their exclusion from the scope of production or of preservation orders in accordance with the respective fundamental rights and the jurisprudence of both the CJEU and the ECtHR; and
- identification and authentication of lawyers as authorised professionals in the e-justice systems.

In order to allow clients to communicate with their lawyers without having to fear that law enforcement authorities or other third parties take note of them reaching out to a lawyer, it is, however, essential that the possibility to identify lawyers and privileged information as such remains voluntary allowing for such information to be excluded from access requests and is not imposed as a legally or de facto mandatory requirement.

The experience of CCBE members with the national e-justice system also shows that a domestic, State-operated infrastructure is not in itself a guarantee of reliability or of respect for procedural rights. In this context, **the CCBE stresses that functional sovereignty must include reliability and respect for relevant procedural requirements, transparency of system availability, accountability for system failures and clear procedural consequences for users when a system fails.**

1.3. Protection of professional secrecy and legal professional privilege in a digital environment

Lawyers as independent collaborators in the administration of justice are one of the key users and therefore main stakeholders of the digital infrastructure of the justice system.[3] Therefore, the CCBE

[3] See for example: C-432/23 Ordre des avocats du barreau de Luxembourg (ECLI:EU:C:2024:791)

considers it essential that the future European cloud and AI ecosystem be developed in a manner that recognises the special status of data protected by professional secrecy and legal professional privilege. Confidentiality of lawyer-client communications is not merely a professional obligation of lawyers. The confidentiality of lawyer-client communications is essential to effective legal representation and has long been recognised throughout Europe. It enables clients to communicate fully and frankly with their lawyers, allowing them to provide accurate advice and effective representation, and is therefore a crucial safeguard for the right to a fair trial. Professional secrecy and legal professional privilege are firmly established in European case law and legal instruments and recognised across all EU Member States. They are fundamental principles of the legal profession and are enshrined in the CCBE's Charter on Core Principles and Code of Conduct for European lawyers.

In this context, it must be stressed that the protection afforded by legal professional privilege extends well beyond the safeguards provided for personal data under Regulation (EU) 2016/679 (GDPR). While the GDPR protects personal data of identifiable individuals, LPP protects the substance of lawyer-client communications as such, irrespective of whether they contain personal data. Consequently, compliance with data protection rules alone does not guarantee the confidentiality required by professional secrecy: privileged material may include corporate information, trade secrets, or communications concerning legal persons, none of which fall within the scope of the GDPR, yet all of which remain fully protected. **Any European cloud and AI infrastructure used in the justice ecosystem must therefore be designed to ensure that privileged data cannot be accessed, scanned, mined, or used for training purposes by cloud or AI providers, and that such protection is enforceable against third-country authorities as well.** Treating LPP-protected data merely as a special category of personal data would fall short of the standards established by the case-law of the Court of Justice and would risk undermining the very essence of the right to a fair trial.

1.4. Access to data covered by professional secrecy/legal professional privilege

The CCBE recommends that the recognition of third countries take into account whether the law of the third country protects lawyer-client communications from compelled access by law enforcement authorities (LEAs). Article 18 deals with associated third countries and states that the Commission may, through implementing acts, designate third countries whose cloud service providers can be audited against the EU's Union assurance criteria level 3. This enables the assessment of certain non-EU-controlled providers under the EU cloud sovereignty framework where the Commission considers it appropriate. To this end, the Article imposes six cumulative conditions that that the third country must fulfil listed in point (a) to (f). The CCBE supports including, among the criteria, the absence of measures capable of compelling a provider to stop or disrupt a service, or to disclose data, without the safeguards of EU law. An adequacy decision under the General Data Protection Regulation (GDPR) does not, by itself, address professional secrecy.

1.5. Mechanism to identify lawyers' data

The CCBE advocates in favour of developing technical means to identify lawyers' data. The practical challenge is how law enforcement authorities (LEAs) can identify that data is held by a lawyer, particularly where the lawyer is established in another Member State. Without a reliable mechanism

for identifying and verifying lawyers, the relevant safeguards may be difficult to apply effectively in practice. Appropriate technical measures should therefore enable both LEAs and service providers to recognise when an account belongs to a lawyer. One possible approach would be to require service providers to allow lawyers to indicate their professional status, subject to reliable verification of that status. It is, however, essential that the possibility to identify lawyers and privileged information as such remains voluntary allowing for such information to be excluded from access requests and is not imposed as a legally or de facto mandatory requirement (as explained in section 1.2).

1.6. Extraterritorial application of third country laws

The CCBE further stresses that whenever a provider is subject to a law of a third country, data held within the justice sector and information held by lawyers and their clients may be exposed to risks that are difficult to reconcile with the requirements of EU law. This includes not only risks of unauthorised access to data, but also operational risks such as service disruption, sanctions exposure, vendor lock-in, inability to migrate to other providers or dependence on a small number of providers.

The CCBE has previously raised concerns in relation to the U.S. CLOUD Act, including concerns regarding extraterritorial jurisdiction, conflicts with EU fundamental rights and the GDPR, limited judicial review, lack of post-authorisation supervision, and insufficient protection of legal professional privilege and professional secrecy.[4]

The sanctions imposed by the United States in relation to the International Criminal Court (ICC) illustrate the vulnerability of judicial institutions where their daily functioning depends on services provided by entities subject to third-country legal obligations or geopolitical pressure. The ICC example illustrates a broader risk to confidentiality and to continuity of service where access to communication, collaboration, storage or payment services depends on providers subject to external sanctions regimes or unilateral political decisions.[5]

2. Specific remarks

2.1 Application of CADA to Bars and Law Societies

The CCBE observes that the current wording of the proposed provisions of CADA may allow for the interpretation that the provisions would directly or indirectly affect some Bars or Law Societies in so far as they provide cloud computing/IT services to their members or a broader group of justice professionals. The CCBE considers such interpretation dangerous in terms of possible violation of fundamental rights, especially the independence of legal representation and legal professional privilege and therefore the rule of law.

Bars and Law Societies are not ordinary market operators. As self-governing professional bodies, they are tasked with safeguarding the independence of the legal profession, protecting professional

[4] CCBE Assessment of the U.S. CLOUD Act (February 2019): https://www.ccbe.eu/wp-content/uploads/2026/09/EN_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf

[5] The CCBE statement on the ICC: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/Statements/2026/EN_NA_20260722_CCBE-Statement-in-support-of-the-International-Criminal-Court-in-response-to-sanctions-imposed-by-the-US-administration.pdf

secrecy, and ensuring the proper administration of justice. Applying a recognition and supervision regime designed for commercial providers to such institution's risks undermining the institutional autonomy that is a cornerstone of the rule of law and a precondition for effective legal protection of citizens.

In concrete terms, recognition at assurance level 1 would require self-assessment under Article 19 in accordance with Annex I; assurance levels 2, 3 or 4 would additionally trigger independent audits under Article 20; and Article 26 would empower national competent authorities to inspect the premises of these service providers. While the CCBE does not contest that service providers must demonstrate to the supervisory authority how data is processed and stored, **it is essential that the supervisory authority has no access to the data of lawyers and Bar associations**. This is not a technical detail but a fundamental question of the independence of the Bar from the State, protected under Article 7 of the Charter of Fundamental Rights and the case law on professional secrecy.

The CCBE further observes that the situation of the Bars and the services they provide differ dramatically from one jurisdiction to another. There is a need for greater clarity on whether Bars are providers, operators or merely users of digital justice infrastructure, as their role varies considerably across Member States and any CADA obligations may have significant implications for costs, governance and the independence of the profession. To illustrate this diversity, several examples are given below.

In **Slovenia**, the Bar Association of Slovenia (OZS) is currently renewing its ERP system and the electronic register of lawyers, which will open additional possibilities for digitally connecting the register with other systems. Therefore, the Bar may, by modernising its register and by linking it to e-justice systems, become an authentic source or a provider of services on which public authorities rely.

So far, the Bar has kept the register of lawyers and has issued lawyers' identity cards (Articles 31 and 32 of the Slovenian Bar Act respectively).[6] The register is publicly available on the Bar Association's website and courts rely on it to verify the status of lawyers. The regional assemblies of the Bar also keep special lists of lawyers for free legal aid and for ex officio appointments, and the Bar publishes disciplinary decisions against lawyers.

Under Article 1 of the Slovenian Bar Act, the legal profession is an autonomous and independent service forming part of the justice system.

In **Greece**, the Bars operate extensive digital platforms used by lawyers in their interactions with courts and public authorities. The Greek Bar Associations, through the platform operated under the auspices of the Plenary of Greek Bar Associations, provide a wide range of electronic services, including electronic filing, access to court-related information and various authentication and certification functions.

In **Estonia**, the Estonian Bar is predominantly a customer and a data subject of other organisations' infrastructure rather than a provider. It is not a cloud computing service provider and does not operate the infrastructure through which lawyers communicate with the courts: that infrastructure (e-toimik, the courts' information system) is built and run by the State. The only State information system in

[6] Zakon o odvetništvu, ZOdv: https://pisrs.si/pregledPredpisa?id=ZAKO265

which the Bar has a formal role is the state legal aid information system (RIS), governed by Government Regulation No 13 of 20 June 2021.[7] Since 1 January 2025, its controller is the Ministry of Justice and Digital Affairs and its processors are the Estonian Bar Association and the Centre of Registers and Information Systems (RIK). It is RIK, not the Bar, that is charged with hosting the system (§ 6(2)1).

Moreover, some Bars are regularly upgrading and potentially expanding their services, and therefore their nature and qualification under the proposed CADA may change.

The CCBE is convinced that CADA should not discourage Bars from such developments, nor should it subject them to forms of State supervision that are incompatible with the independence of the profession and the protection of legal professional privilege. **While the CCBE and its members fully recognise the necessity of maintaining a high level of operational control, resilience, security, and protection against external dependencies, we respectfully submit that in order to guarantee the independence of the legal profession such measures are best implemented within the existing self-regulatory frameworks of the Bars and Law Societies.**

If in some cases the Commission sees the necessity that the provisions of CADA apply to Bars and Law Societies, the CCBE insists on adding an express provision ensuring that inspection powers respect the independence of the Bar and do not extend to data protected by professional secrecy and that, where such data are concerned, access is subject to safeguards equivalent to those applicable to searches of law offices: judicial authorisation, precise specification of the data concerned and the involvement of the competent Bar.

The CCBE's research in 9 EU jurisdictions has shown that across all of them searches of law offices require a formal legal basis, almost always in the form of a judicial warrant or reasoned judicial decision.[8] For example:

- In **Belgium**, house and office searches, including the IT systems, require a warrant from an investigating judge, except in cases of consent or when caught red-handed, where the public prosecutor may act.[9]
- In **France,** searches of a lawyer's office or home require a written and reasoned decision issued by a magistrate (*fr. juge des libertés et de la détention*), specifying the offence, purpose, and proportionality regarding the nature of the crime (Article 56-1 Code of Criminal Procedure).
- In **Germany,** searches must be ordered by a judge under Section 105 of the German Code of Criminal Procedure (*ger. Strafprozeßordnung – StPO*)[10] with limited exceptions for exigent circumstances where the public prosecution may act.
- In **Italy,** searches in lawyers' offices must be conducted personally by a judge, or during preliminary investigations by the public prosecutor acting under a reasoned court

[7] Statutes of the State Legal Aid Information System, Adopted 20.06.2021 No. 13, RT I, 25.06.2021, 19

[8] Belgium, France, Germany, Greece, Ireland, Italy, Latvia, the Netherlands and Slovenia

[9] Reference to the law: Article 39bis para 9 of the Belgian Criminal Procedure Code (*fr. Code d'instruction criminelle*): https://www.ejustice.just.fgov.be/cgi_loi/article.pl?language=fr&sum_date=&pd_search=1808-11-27&numac_search=1808111701&page=1&lg_txt=F&caller=list&1808111701=7&trier=promulgation&view_numac=2022b30600fx1804032130fr&dt=CODE+D%27INSTRUCTION+CRIMINELLE&fr=f&choix1=ET#LNK0010

[10] English version: https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

authorisation as per Article 103 of the Italian Criminal Procedure Code (*it. Codice di Procedura Penale, CPP*).[11]

- In **Slovenia,** a law office may be searched only on the basis of a court-issued search warrant, regardless of the field of law.
- In **Ireland**, search warrants are issued by District Court judges or peace commissioners, following sworn information by police.

Moreover, in many jurisdictions, execution of a search warrant in a law office is subject to procedural safeguards to ensure the protection of the legal professional privilege or professional secrecy. The first of such additional safeguards is the presence of the Bar president (or representative) during searches of a law firm (e.g. Belgium, France, Italy, Latvia, the Netherlands, Slovenia). The second additional safeguard applying to the searches of law offices is the different treatment of information in possession of a lawyer or law office. This includes specific provisions on the information to be excluded from the scope of the searches or from the body of evidence to be used at a later stage of the proceedings.

2.2 Risk assessment methodology under Article 29

The CCBE finds it important that the results of the risk assessment under Article 29 ensure a coherent interpretation of the risk level and assurance level to be used in relation to the same sector (or the same activities). This is especially important in the context of the increase in cross-border judicial proceedings and investigative measures, as well as EU-level initiatives aiming to promote the take up of AI and other digital technologies by the justice system.[12]

The CCBE proposes that the methodology to be adopted by the Commission under Article 29(3) requires the consultation of Bars when assessing activities in the justice sector of which the lawyers and Bars are users or in cases where they could be treated as providers. The risk assessment methodology should also incorporate the need to afford the highest level of protection to information covered by professional secrecy. The example of the Estonian courts information system illustrates why such consultation is important. Its users include not only advocates and Bar staff, but also authorised staff of the courts, the prosecutor's office and investigative authorities (§ 7(1)), as the body conducting the proceedings determines the fee on the basis of the information recorded in the system. The system's security class and security level were established by regulation. Under CADA, the same system would be assessed as a justice-sector activity under Article 29 by the Member State concerned, following a methodology established by a Commission implementing act. **In the CCBE's view, that methodology should require consultation of the legal profession.**

Furthermore, some Bars may be qualified trust service providers under eIDAS Regulation. For example, the General Council of the Spanish Bar (CGAE) is a qualified trust service provider through its Certification Authority (ACA), a status which also appears on the Spanish Trusted List, and it issues qualified electronic certificates to lawyers. The CGAE operates the electronic identification and authentication of lawyers (ACA and ACA Plus, and the single access system of the Spanish Bar, which is also offered to local Bars for the identification of their members), services connected with legal aid,

[11] English version: https://canestrinilex.com/assets/Uploads/pdf/cf70b10e21/Italian-Code-of-Criminal-Procedure-canestriniLex.pdf

[12] Digital Justice 2030 Strategy : https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/digitalisation-justice/communication-digitaljustice2030_en

and the exchange of the national roll of lawyers with the Ministry of Justice and with the Generalitat de Catalunya. The CGAE foresees further development of cloud-based qualified certificates during the second implementation phase of ACA Plus. For the sake of accuracy, the CGAE does not operate the platform through which lawyers communicate with courts: in Spain, lawyers access LexNET, operated by the Ministry of Justice, or the equivalent systems of the Autonomous Communities, either directly or through their own case-management software.

3. Final remarks

The CCBE also invites the Commission and other stakeholders to reflect on the diversity of the European IT services market and the impact of the current status quo on smaller jurisdictions. Having stringent provisions risks reducing the number of providers with the required assurance levels and thus, losing on competitive offers as we have a small market where regulation for higher requirements is often adopted prior to supply of the respective service being available on the market. Also, for some Bars, especially from smaller jurisdictions, additional duties to supervise or monitor higher requirements would be an additional burden.

Moreover, the CCBE invites the Commission to consider a possibility of recognising the equivalent national frameworks rather than requiring their re-expression. There are some member states which already have a functioning, mandatory, State-wide assurance regime covering the systems used in the justice sector, which are adopted and applied per system rather than per provider, and not expressed in Union assurance levels.