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 a regulation on harmonised rules on fair access to and use of data (Data Act)

Introduction and Executive summary

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 46 countries and, through them, more than 1 million European lawyers. The CCBE responds regularly on behalf of its members on policy issues which affect European citizens and lawyers.

On 23 February 2022, the European Commission presented a proposal for a regulation on harmonised rules on fair access to and use of data (Data Act). It aims to ensure fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data.

Following its analysis of the proposal, the CCBE concludes:

- **The personal and material scope of the Data Act proposal is too broad.**
- **The Data Act should provide for a general provision to ensure an adequate protection of PS/LPP. Therefore:**
  - **Recital (7) should be amended to include that the Regulation should be without prejudice on professional secrecy under national law, such as rules on the protection of professional communications between lawyers and their clients.**
  - **Article 1 should be amended to include a paragraph 5 stating that the regulation shall not affect national rules on the protection of professional secrecy. The obligations provided for by this Regulation should not apply to professionals subject to professional secrecy, as provided for by national law, where such obligations would lead these professionals to breach their professional secrecy.**
- **The scope and the conditions for making the data available to public bodies should be clarified. The lack of a clear definition of the concepts of "*exceptional need*", "*public emergency*", and the reference to national procedures creates a high risk of divergent interpretations of the concepts involved and increases the likelihood of interference with fundamental rights. The proposal should delineate more clearly the types of situations that would constitute a public emergency.**
- **The justification for a data request should be better defined in the proposal. Justifying circumstances such as the inability to adopt legislative measures in time, as well as the reduction of administrative burdens, should be withdrawn from the proposal.**
- **The proposal should exclude the possibility for public bodies to request data covered by professional secrecy, as well as the obligation for data holders to disclose such data.**

- **The EU institutions and cloud service providers should take actions in order to ensure that reasonable technical, legal and organisational measures are in place to prevent unauthorised access to data covered by professional secrecy or legal professional privilege.**

- **The obligations of Article 30 are not sufficiently justified and do not respect the principle of technological neutrality. These provisions should be removed from the proposal.**

General comments

The CCBE notes that the proposal for a Data Act has a wide scope, covering many situations and addressees which are not necessarily related, and containing rules pursuing different goals. Indeed, the proposal provides for rules on users' right to access and use data generated by the use of products or related services (article 3 and following); on unfair contractual terms (article 13); on data availability for the public sector (article 14-22); on data processing services, which are more commonly considered as cloud services providers (articles 23-26), international transfer of non-personal data (article 27), interoperability (articles 28-29) and smart contracts (30).

In particular, the obligation to make data accessible (Article 3(1)) or to make them available (Article 4(1)) can apply to almost anyone, as there is hardly any delimitation of the circle of data holders, products, related services or the nature of the data. The definitions in Article 2 in this respect are excessively broad. Also, the application of obligations on related products and services to virtual assistants, in accordance with Article 7(2), further broadens the scope and suggests, in relation to the definition of related service in Article 2(3), a broad conception of the link between the service and the product, which is now only loosely linked to the need to exploit the product.

The CCBE considers that the personal and material scope of the Data Act proposal is too broad (Art. 1 §§1-2).

I. The necessity to guarantee professional secrecy / legal professional privilege ("PS/LPP")

A. A strengthened protection of PS/LPP

The CCBE recalls that for lawyers to be effective in defending their clients' rights, there must be confidence that communications between them are kept confidential. Most legal systems share a common understanding that if the right of the citizen to safeguard confidentiality, i.e. the right of the citizen to be protected against any divulging of his/her communication with his/her lawyer, were to be denied, people may be denied access to legal advice and to justice. PS/LPP are thus seen as instruments by which access to justice and the maintenance of the rule of law can be achieved.

All European countries have national provisions in order to ensure the protection of the right and duty of the lawyers to keep clients' matters confidential. In some jurisdictions, that is achieved by attaching to those communications the protection of legal professional privilege, and in other jurisdictions by treating them as professional secrets. Both approaches, however, seek to achieve the same end: the protection of information

generated within lawyer-client relationship for the purpose of giving or receiving legal advice, in both contentious and non-contentious matters, and/or representation in any type of legal proceedings. This absolute obligation of confidentiality rests directly upon the lawyer and cannot be waived by the client in most jurisdictions. In some Member States, professional secrecy has a constitutional status aimed to guarantee fundamental rights such as the right to privacy or fair trials rights. In some jurisdictions, violation of professional secrecy by the lawyers, such as the disclosure of covered data, is a criminal offence.

The European Court of Human Rights ("ECtHR") has repeatedly linked the respect for PS/LPP to the observance of **Articles 6 and 8 of the European Convention on Human Rights** ("ECHR"), stating that "*the right of everyone to a fair trial*"[1] *is dependent upon the "relationship of trust between [the lawyer and the client]*" and repeatedly highlighting that undermining PS/LPP may violate Article 8, which protects the right to respect for private and family life. Indeed, **Article 8 "*affords strengthened protection to exchanges between lawyers and their clients*"**. The Court specifies that "*this is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants. Yet they cannot carry out this essential task if they are unable to guarantee to those they are defending that their exchanges will remain confidential*" [2].

The protection of confidentiality of lawyer-client communications has also been recognized as a **general principle of EU law** by the European Court of Justice[3] and has a **legal basis in the EU Charter of Fundamental Rights within its articles 7 on the right to privacy and 47 on the right to a fair trial**.

B. The Data Act and PS/LPP

The Data Act proposal provides for several obligations to make data available. The CCBE notes that Recital (7) of the Data Act proposal provides that "*no provisions of this Regulation should be applied or interpreted in such a way as to diminish or limit the right to the protection of personal data or the right to privacy and confidentiality of communications*", with specific references to the GDPR[4] and the e-privacy directive[5]. It also contains provisions in order to guarantee respect of trade secrets or intellectual property rights. The CCBE welcomes such provisions but considers them unsufficient to ensure the protection of PS/LPP, as guaranteed by the ECHR and EU primary law, as such principle may cover data which are not personal nor protected by trade secrets.

The CCBE recalls that when the European legislator adopted transitional provisions to modify the e-privacy directive to adapt it to the fight against child abuse, it explicitly provided for a general clause on the protection of PS/LPP, clarifying that the new rules should be "***without prejudice to the rules on professional secrecy under national law, such as rules on the protection of professional communications, between doctors and their patients, between journalists and their sources, or between lawyers and their clients, in particular since the confidentiality of communications between lawyers and their clients is key to ensuring the effective exercise of the rights of the defence as an essential part of the right to a fair trial***".

The CCBE considers that the Data Act should provide for a general provision to ensure an adequate protection of PS/LPP. Therefore:

[1] ECtHR, Michaud v. France (12323/11), 2012, §§117-118
[2] ECtHR, Kopp v. Switzerland (23224/94), 1998
[3] ECJ, AM&S v. Commission, (155/79), 1982, §18
[4] Regulation (EU) 2016/679
[5] Directive 2002/58/EC

- **Recital (7) should be amended to include *in fine* that the Regulation should be without prejudice on professional secrecy under national law, such as rules on the protection of professional communications between lawyers and their clients.**

- **Article 1 should be amended to include a paragraph 5 stating that the regulation shall not affect national rules on the protection of professional secrecy. The obligations provided for by this Regulation should not apply to professionals subject to professional secrecy, as provided for by national law, where such obligations would lead these professionals to breach their professional secrecy.**

II. Obligation to make data available for public sector bodies and Union institutions, agencies or bodies in case of "exceptional need"

Article 14(1) of the Data Act proposal provides for the obligation of data holders to make data available for public authorities, EU institutions, agencies and bodies in case of "*exceptional need*". The CCBE notes that this access is framed in Article 15, 16, 17 and following. The scope of exceptional need is defined in Article 15 as the need to respond to a public emergency, and Article 16 excludes activities carried out for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or for customs or taxation administration. Article 17 contains the conditions to be met by the requests.

However, the CCBE raises deep concerns over such request for data by public bodies. As underlined by the European Data Protection Board ("EDPB") and the European Data Protection Supervisor ("EDPS") "***the principles of necessity and proportionality, the legal basis must also define the scope and manner of the exercise of their powers by the competent authorities and be accompanied by sufficient safeguards to protect individuals against arbitrary interference***"; in this regard the EDPB and the EDPS "***observe that the circumstances justifying the access are not narrowly specified and consider it necessary for the legislator to define much more stringently the hypotheses of emergency or exceptional need***"[6].

The CCBE considers that the broad provisions on public body data requests create a risk of misuse, despite the conditions of the proposal providing that (a) this obligation to make data available to public bodies will not affect personal data and (b) that such data may not be used for prevention, investigation, detection or prosecution of criminal or administrative offenses, execution of criminal penalties, customs/taxation administration etc. History has demonstrated time and again that it is very difficult to enforce these prohibitions, and the difference between non-personal data and personal data is very vague even after years of common GDPR experiences, and the more non-personal data one may have access to, the easier it is to identify or otherwise narrow down the possible scope of persons affected. No doubt, there will certainly be public bodies that yield to such temptation of easy access to such vast data mines, the question is more how we will be able to find that out.

Therefore, the CCBE considers that the scope and the conditions for making the data available to public bodies should be clarified.

Regarding the justifications of a data request by public bodies, the proposal requires the demonstration of an "exceptional need". According to article 15, such "exceptional need" relates to the necessity to respond to a public emergency, to prevent or recover from a public emergency, or to fulfil a task in a public interest

[6] EDPB-EDPS Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to the use of data (Data Act), 4 May 2022, p.3

provided by the law. The notion of "public emergency" is broadly defined in article 2(10) as an "*an exceptional situation negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or substantial degradation of economic assets in the Union or the relevant Member State(s)*". It should be noted that Recital (57) gives examples of public emergencies, such as public health emergencies, those resulting from environment degradation, major natural or human-induced disasters. The recital refers *in fine* to public emergencies determined according to the respective procedures of the Member States or international organisations.

The CCBE considers that the lack of a clear definition of the concepts of "exceptional need", "public emergency", and the reference to national procedures creates a high risk of divergent interpretations of the concepts involved and increases the likelihood of interference with fundamental rights. It supports the recommendations of the EDPB and the EDPS to amend the proposal to delineate more clearly the types of situations that would constitute a public emergency[7].

Moreover, the CCBE has similar concerns over the justification for a data request where the lack of available data prevents the public authority from fulfilling a specific task in a public interest explicitly provided by law. For this justification, article 15(c) refers to two situations: (1) when the public authority has been unable to obtain data by alternative means, including where legislative measures cannot be passed in time to make data available, or (2) when the obtention of data would substantively reduce administrative burden.

In this regard, the CCBE supports the conclusions of the European data protection authorities[8] and considers that:

- **The possibility to request data, when legislative measures cannot be adopted in time, goes against the conditions of article 52(1) of the Charter of Fundamental Rights of the EU according to which any limitation to fundamental rights must be provided by the law.**
- **The reduction of administrative burden cannot constitute a sufficient justification to interfere with fundamental rights.**

Such circumstance should be withdrawn from the proposal which should better define the justification for a data request.

Finally, while articles 17(2)(c), 18(5) and 19(2) contains provisions to protect trade secrets, **the proposal does not offer any protection of data subject to PS/LPP.**

As above mentioned, the proposal should exclude the possibility for public bodies to request data covered by professional secrecy, as well as the obligation for data holders to disclose such data.

III. Requirements regarding the use of cloud services

The Data Act contains rather detailed provisions related to data processing service providers, more commonly called cloud service providers, aiming to assist cloud users in switching service providers (article 23 to 26, and 29). Moreover, non-SME cloud service providers have to "*take reasonable technical, legal and organisational measures*" to prevent international transfer or governmental access to non-personal data (article 27.1).

The CCBE notes that in the last years, cloud computing services have matured significantly. Security processes have become more robust with widely accepted third-party attestations and assurances on the reliability of IT security controls. However, certain information security controls are still lacking. **As long as the service**

[7] EDPB-EDPS Joint Opinion 02/2022, §78
[8] EDPB-EDPS Joint Opinion 02/2022, §79

provider (or any underlying platform or infrastructure provider) is technically able to read and access the data of the lawyer, the risks of unauthorised access, and thus breaches of confidentiality and PS/LPP obligations will remain a serious concern for lawyers. Similar concerns arise from the reuse of client data for other purposes or unlawful interception of communications by authorities[9].

The CCBE is currently working on the use of cloud services by lawyers in Europe. The overall objective of this action is to make professional secrecy fit for the digital age by defining defence mechanisms against unauthorised access to information covered by professional secrecy.

In this regard, the CCBE calls on the EU institutions and cloud service providers to take actions in order to ensure that reasonable technical, legal and organisational measures are in place to prevent unauthorised access to data covered by PS/LPP.

IV. Essential requirements of smart contracts

Article 30 provides that vendors of an application using smart contracts are required to comply with the listed essential requirements, such as robustness, safe termination etc., which shall serve as a basis for a declaration of conformity and the details of which will be later set out by standards.

With regard to Article 30, the CCBE would like to highlight that in its current form, without any interim measures, this is a dangerous, unnecessarily rushed approach. The CCBE firmly believes that regardless of any technical means used, consumer protection and any other legal obligations set out by law have to be maintained by all parties.

A declaration of conformity is an appropriate tool for mature markets with existing standards on e.g. safety or other requirements, freeing the regulator, among others, from the burden of having to update the legislative requirements frequently. But it was never intended to be used to outsource the regulatory burden to larger market participants having the necessary resources to send experts to EU standardisation bodies, such as ETSI.

No one really expects any guidance or standards in the coming years on how the essential requirements set out in the Data Act proposal could be implemented in distributed ledgers. There are no transitory or implementation measures referring to smart contract in the Data Act proposal, and smart contract issues were not investigated in the impact assessment. This is more a problem of legal certainty and the appropriateness of the intended regulatory approach, than a direct problem of lawyers, but businesses in Europe will probably look to their lawyers in the EU for guidance in these matters, and based on the current provisions, lawyers will not be able to provide such guidance.

Therefore, the CCBE considers the wide-ranging obligations of Article 30 are not sufficiently justified and do not respect the principle of technological neutrality. These provisions should be removed from the proposal.

[9] Guide on the use of AI-based tools by lawyers and law firms in the EU, 2022, p. 47,48 and 51.