

EDPB-EDPS

Joint Opinion 5/2021

on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

18 June 2021

Executive Summary

On 21 April 2021, the European Commission presented its Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (hereinafter "the Proposal"). The EDPB and the EDPS welcome the concern of the legislator in addressing the use of artificial intelligence (AI) within the European Union (EU) and stress that the Proposal has prominently important **data protection implications**.

The EDPB and the EDPS note that the **legal basis** for the proposal is in the first place Article 114 of the Treaty on the Functioning of the European Union (TFEU). In addition, the Proposal is also based on Article 16 of the TFEU insofar as it contains specific rules on the protection of individuals with regard to the processing of personal data, notably restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement. The EDPB and EDPS recall that, in line with the jurisprudence of the Court of Justice of the EU (CJEU), Article 16 TFEU provides an appropriate legal basis in cases where the protection of personal data is one of the essential aims or components of the rules adopted by the EU legislature. The application of Article 16 TFEU also entails the **need to ensure independent oversight for compliance** with the requirements regarding the processing of personal data, as is also required Article 8 of the Charter of the Fundamental Rights of the EU.

Regarding the **scope of the Proposal,** the EDPB and EDPS strongly welcome the fact that it extends to the provision and use of AI systems by EU institutions, bodies or agencies. However, the **exclusion of international law enforcement cooperation from the scope** set of the Proposal raises serious concerns for the EDPB and EDPS, as such exclusion creates a significant risk of circumvention (e.g., third countries or international organisations operating high-risk applications relied on by public authorities in the EU).

The EDPB and the EDPS **welcome the risk-based approach** underpinning the Proposal. However, this approach should be clarified and the concept of "risk to fundamental rights" aligned with the GDPR and the Regulation (EU) 2018/1725 (EUDPR), since aspects related to the protection of personal data come into play.

The EDPB and the EDPS agree with the Proposal when it states that the classification of an **AI system as high-risk does not necessarily mean that it is lawful** per se and can be deployed by the user as such. **Further requirements resulting from the EU data protection law may need to be complied with** by the controller. Moreover, the compliance with legal obligations arising from Union legislation (including on personal data protection) should be a precondition to being allowed to enter the European market as CE marked product. To this end, the EDPB and the EDPS consider that **the requirement to ensure compliance with the GDPR and EUDPR should be included in Chapter 2 of Title III**. In addition, the EDPB and the EDPS consider necessary to adapt the conformity assessment procedure of the Proposal so that third parties always conduct high-risk AI systems' *ex-ante* conformity assessments.

Given the great risk of discrimination, the Proposal prohibits "social scoring" when performed 'over a certain period of time' or 'by public authorities or on their behalf'. However, private companies, such as social media and cloud service providers, also can process vast amounts of personal data and conduct social scoring. Consequently, **the future AI Regulation should prohibit any type of social scoring**.

Remote biometric identification of individuals in publicly accessible spaces poses a high-risk of intrusion into individuals' private lives, with severe effects on the populations' expectation of being anonymous in

public spaces. For these reasons, the EDPB and the EDPS **call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces** - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context. A **ban** is equally recommended **on AI systems categorizing individuals from biometrics into clusters** according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination under Article 21 of the Charter. Furthermore, the EDPB and the EDPS consider that the use of AI to **infer emotions of a natural person is highly undesirable and should be prohibited.**

The EDPB and the EDPS welcome the **designation of the EDPS as the competent authority and the market surveillance authority for the supervision of the Union institutions, agencies and bodies**. However, the role and tasks of the EDPS should be further clarified, specifically when it comes to its role as market surveillance authority. Furthermore, the future AI Regulation should clearly establish the **independency of the supervisory authorities** in the performance of their supervision and enforcement tasks.

The designation of data protection authorities (DPAs) as the national supervisory authorities would ensure a more harmonized regulatory approach, and contribute to the consistent interpretation of data processing provisions and avoid contradictions in its enforcement among Member States. Consequently, the EDPB and the EDPS consider that **data protection authorities should be designated as national supervisory authorities pursuant to Article 59 of the Proposal.**

The Proposal assigns a predominant role to the Commission in the "European Artificial Intelligence Board" (EAIB). Such role conflicts with the need for an AI European body to be independent from any political influence. To ensure its independency, the future AI Regulation should give **more autonomy to the EAIB** and ensure it can act on its own initiative.

Considering the spread of AI systems across the single market and the likelihood of cross-border cases, there is a crucial need for a harmonized enforcement and a proper allocation of competence between national supervisory authorities. The EDPB and EDPS suggest envisaging **a mechanism guaranteeing a single point of contact for individuals concerned by the legislation as well as for companies, for each AI system.**

Concerning the **sandboxes,** the EDPB and the EDPS **recommend clarifying their scope and objectives**. The Proposal should also clearly state that the legal basis of such sandboxes should comply with the requirements established in the existing data protection framework.

The **certification system** outlined in the Proposal is **missing a clear relation to the EU data protection law** as well as to other EU and Member States' law applicable to each 'area' of high-risk AI system and is not taking into account the **principles of data minimization and data protection by design** as one of the aspects to take into consideration **before obtaining the CE marking**. Therefore, the EDPB and the EDPS recommend amending the Proposal as to clarify the relationship between certificates issued under the said Regulation and data protection certifications, seals and marks. Lastly, the DPAs should be involved in the preparation and establishment of harmonized standards and common specifications.

Regarding the **codes of conduct**, the EDPB and the EDPS consider it **necessary to clarify** if the protection of personal data is to be considered among "additional requirements" that can be addressed by these codes of conduct, and to ensure that the "technical specifications and solutions" do not conflict with the rules and principles of the existing EU data protection framework.

TABLE OF CONTENTS

1 INTRODUCTION....5
2 ANALYSIS OF THE KEY PRINCIPLES OF THE PROPOSAL....7
2.1 Scope of the Proposal and relationship with the existing legal framework....7
2.2 Risk-based approach....8
2.3 Prohibited uses of AI....10
2.4 High-risk AI systems....12
2.4.1 Need for an *ex-ante* conformity assessment by external third parties....12
2.4.2 Scope of regulation must also cover AI systems already in use....13
2.5 Governance and European AI Board....13
2.5.1 Governance....13
2.5.2 The European AI Board....15
3 INTERACTION WITH THE DATA PROTECTION FRAMEWORK....16
3.1 Relationship of the Proposal to the existing EU data protection law....16
3.2 Sandbox & further processing (Articles 53 and 54 of the Proposal)....17
3.3 Transparency....19
3.4 Processing of special categories of data & data relating to criminal offences....19
3.5 Compliance mechanisms....20
3.5.1 Certification....20
3.5.2 Codes of conduct....20
4 CONCLUSION....22

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC[1],

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[2],

Having regard to the request for a Joint Opinion of the European Data Protection Supervisor and of the European Data Protection Board of 22 April 2021 regarding the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act),

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1 INTRODUCTION

1. The advent of artificial intelligence ('AI') systems is a very important step in the evolution of technologies and in the way humans interact with them. AI is a set of key technologies that will profoundly alter our daily lives, be it on a societal or an economic standpoint. In the next few years, decisive decisions are expected for AI as it helps us overcome some of the biggest challenges we face in many areas today, ranging from health to mobility, or from public administration to education.

2. However, these promised advances do not come without risks. Indeed, the risks are very relevant considering that the individual and societal effects of AI systems are, to a large extent, unexperienced. Generating content, making predictions or taking a decision in an automated way, as AI systems do, by means of machine learning techniques or logic and probabilistic inference rules, is not the same as humans carrying out those activities, by means of creative or theoretical reasoning, bearing full responsibility for the consequences.

3. AI will enlarge the amount of predictions that can be done in many fields starting from measurable correlations between data, invisible to human eyes but visible to machines, making our lives easier and solving a great number of problems, but at the same time will erode our capability to give a causal interpretation to outcomes, in such a way that the notions of transparency, human control, accountability and liability over results will be severely challenged.

4. Data (personal and non-personal) in AI are in many cases the key premise for autonomous decisions, which will inevitably affect individuals' lives at various levels. This is why the

[1] OJ L 295, 21.11.2018, p. 39–98.

[2] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

EDPB and the EDPS, already at this stage, strongly assert that the Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) ('the Proposal')[3] has **important data protection implications**.

5. Allocating the task of deciding to machines, on the basis of data, will create risks to the rights and freedoms of individuals, will impact their private lives and might harm groups or even societies as a whole. The EDPB and the EDPS emphasize that the rights to private life and to the protection of personal data, conflicting with the assumption of machines' decision autonomy underlying the concept of AI, are a pillar of EU values as recognized in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the Charter of Fundamental Rights of the EU (hereinafter "the Charter") (Articles 7 and 8). Reconciling the perspective of growth offered by AI applications and the centrality and primacy of humans vis-a-vis machines is a very ambitious, yet necessary goal.

6. The EDPB and the EDPS welcome the involvement in the regulation of all stakeholders of the AI chain of value and the introduction of specific requirements for solution providers as they play a significant role in the products that make use of their systems. However, responsibilities of the various parties - user, provider, importer or distributor of an AI system - need to be clearly circumscribed and assigned. In particular, when processing personal data, special consideration should be given to the consistency of these roles and responsibilities with the notions of data controller and data processor carried by the data protection framework since both norms are not congruent.

7. The Proposal gives an important place to the notion of human oversight (Article 14) which the EDPB and the EDPS welcome. However, as stated earlier, due to the strong potential impact of certain AI systems for individuals or groups of individuals, real human centrality should leverage on highly qualified human oversight and a lawful processing as far as such systems are based on the processing of personal data or process personal data to fulfil their task so as to ensure that the right not to be subject to a decision based solely on automated processing is respected.

8. In addition, due to the data-intensive nature of many AI applications, the Proposal should promote the adoption of a data protection by design and by default approach at every level, encouraging the effective implementation of data protection principles (as envisaged in Article 25 GDPR and Article 27 EUDPR) by means of state-of-the-art technologies.

9. Lastly, the EDPB and the EDPS emphasize that this joint opinion is provided only as a preliminary analysis of the Proposal , without prejudice to any further assessment and opinion on the effects of the Proposal and it's compatibility with the EU data protection law.

2 ANALYSIS OF THE KEY PRINCIPLES OF THE PROPOSAL

[3] COM(2021) 206 final.

2.1 Scope of the Proposal and relationship with the existing legal framework

10. According to the Explanatory Memorandum, the **legal basis** for the Proposal is in the first place Article 114 of the TFEU, which provides for the adoption of measures to ensure the establishment and functioning of the Internal Market[4]. In addition, the Proposal is based on Article 16 of the TFEU *insofar as it contains specific rules* on the protection of individuals with regard to the processing of personal data, notably restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement[5].

11. The EDPB and EDPS recall that, in line with the jurisprudence of the CJEU, Article 16 TFEU provides an appropriate legal basis in cases where the protection of personal data is one of the essential aims or components of the rules adopted by the EU legislature[6]. The application of Article 16 TFEU also entails the need to ensure independent oversight for compliance with the requirements regarding the processing of personal data, as is also required Article 8 of the Charter.

12. The EDPS and EDPB recall that a comprehensive data protection framework adopted on the basis of Article 16 TFEU already exists, consisting of the General Data Protection Regulation (GDPR)[7], the Data Protection Regulation for the European Union institutions, offices, bodies and agencies (EUDPR)[8] and the Law Enforcement Directive (LED)[9]. According to the Proposal, it is only the additional restrictions regarding the processing of biometric data contained in the Proposal that may be considered as based on Article 16 TFEU and as therefore having the same legal basis as the GDPR, EUDPR or LED. This has important implications for the relationship of the Proposal to the GDPR, EUDPR and LED more generally, as set out below.

13. As regards the **scope of the Proposal**, the EDPB and EDPS strongly welcome the fact that the Proposal extends to the use of AI systems by EU institutions, bodies or agencies. Given that the use of AI systems by these entities may also have a significant impact on the fundamental rights of individuals, similar to use within EU Member States, it is indispensable that the new regulatory framework for AI applies to both EU Member States and EU institutions, offices, bodies and agencies in order to ensure a coherent approach throughout the Union. As EU institutions, offices, bodies and agencies may act both as providers and

[4] Explanatory memorandum, p. 5.
[5] Explanatory memorandum, p. 6. See also recital (2) of the proposal.
[6] Opinion of 26 July 2017, *PNR Canada*, Opinion procedure 1/15, ECLI:EU:C:2017:592, paragraph 96.
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.
[8] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98.
[9] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

users of AI systems, the EDPS and EDPB consider it fully appropriate to include these entities within the scope of the Proposal on the basis of Article 114 TFEU.

14. However, EDPB and EDPS have serious concerns regarding the exclusion of international law enforcement cooperation from the scope set out in Article 2(4) of the Proposal. This exclusion creates a significant risk of circumvention (e.g., third countries or international organisations operating high-risk applications relied on by public authorities in the EU).

15. The development and use of AI systems will in many cases involve the processing of personal data. Ensuring clarity of the relationship of this Proposal to the existing EU legislation on data protection is of utmost importance. The Proposal is without prejudice and complements the GDPR, the EUDPR and the LED. While the recitals of the Proposal clarify that the use of AI systems should still comply with data protection law, **the EDPB and EDPS strongly recommend clarifying in Article 1 of the Proposal that the Union's legislation for the protection of personal data**, in particular the GDPR, EUDPR, ePrivacy Directive[10] and the LED, shall apply to any processing of personal data falling within the scope of the Proposal. A corresponding recital should equally clarify that the Proposal does not seek to affect the application of existing EU laws governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments.

2.2 Risk-based approach

16. The EDPB and the EDPS **welcome the risk-based approach** underpinning the Proposal. The Proposal would apply to any AI systems, including those which do not involve the processing of personal data but can still have an impact on interests or fundamental rights and freedoms.

17. The EDPB and the EDPS note that some of the provisions in the Proposal leave out the risks for groups of individuals or the society as a whole (e.g., collective effects with a particular relevance, like group discrimination or expression of political opinions in public spaces). The EDPB and the EDPS recommend that societal/group risks posed by AI systems should be equally assessed and mitigated.

18. The EDPB and the EDPS are of the view that the Proposal's risk-based approach should be clarified, and the concept of "risk to fundamental rights" **aligned with the GDPR**, insofar as aspects related to the protection of personal data come into play. Whether they are end-users, simply data subjects or other persons concerned by the AI system, the absence of any reference in the text to the individual affected by the AI system appears as a blind spot in the Proposal. Indeed, the obligations imposed on actors vis-a-vis the affected persons should emanate more concretely from the protection of the individual and her or his rights. Thus, the EDPB and the EDPS urge the legislators to explicitly address in the Proposal the **rights and remedies available to individuals** subject to AI systems.

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC.

19. The EDPB and EDPS take note of the choice of providing an exhaustive list of **high-risk AI systems**. This choice might create a black-and-white effect, with weak attraction capabilities of highly risky situations, undermining the overall risk-based approach underlying the Proposal. Also, this list of high-risk AI systems detailed in annexes II and III of the Proposal lacks some types of use cases which involve significant risks, such as the use of AI for determining the insurance premium, or for assessing medical treatments or for health research purposes. The EDPB and the EDPS also highlight that those annexes will need to be regularly updated to ensure that their scope is appropriate.

20. The Proposal requires the **providers** of the AI system to perform a risk assessment, however, in most cases, the (data) controllers will be the **users** rather than providers of the AI systems (e.g., a user of a facial recognition system is a 'controller' and therefore, is not bound by requirements on high-risk AI providers under the Proposal).

21. Moreover, it will **not always be possible for a provider to assess all uses** for the AI system. Thus, the initial risk assessment will be of a more general nature than the one performed by the user of the AI system. Even if the initial risk assessment by the provider does not indicate that the AI system is "high-risk"" under the Proposal, this should not exclude **a subsequent (more granular) assessment** (data protection impact assessment ('DPIA') under Article 35 of the GDPR, Article 39 of EUDPR or under Article 27 of the LED) **that should be made by the user of the system**, considering the context of use and the specific use cases. The interpretation of whether under the GDPR, the EUDPR and the LED a type of processing is likely to result in a high-risk is to be made independently of the Proposal. However, the classification of an AI system as posing "high-risk" due to its impact on fundamental rights[11] **does trigger a presumption of "high-risk" under the GDPR, the EUDPR and the LED to the extent that personal data is processed.**

22. **The EDPB and the EDPS agree with the Proposal when it specifies that the classification of an AI system as high-risk does not necessarily mean that it is lawful *per se* and can be deployed by the user as such. Further requirements resulting from the EU data protection law may need to be complied with by the controller.** Furthermore, the underlying reasoning to Article 5 of the Proposal that, unlike prohibited systems, the high-risk systems may be permissible in principle is to be addressed and dispelled in the Proposal, especially since the proposed CE marking does not imply that the associated processing of personal data is lawful.

23. However, the compliance with legal obligations arising from Union legislation (including on the personal data protection) should be precondition to being allowed to enter the European market as CE marked product. To this end, the EDPB and the EDPS **recommend including in Chapter 2 of Title III of the Proposal the requirement to ensure compliance with the GDPR and the EUDPR**. These requirements shall be audited (by third party audit) before

[11]The European Union Agency for Fundamental Rights (FRA) has already addressed the need to conduct fundamental rights impact assessments when using AI or related technologies. In its 2020 report, "Getting the future right – Artificial intelligence and fundamental rights", FRA identified "pitfalls in the use of AI, for example in predictive policing, medical diagnoses, social services, and targeted advertising" and stressed that "private and public organisations should carry out assessments of how AI could harm fundamental rights" to reduce negative impacts on individuals.

the CE marking in line with the accountability principle. In the context of this third-party assessment, the initial impact assessment to be performed by the provider will be especially relevant.

24. Having regard to complexities triggered by the development of AI systems, it should be pointed out that the technical characteristics of AI systems (e.g., the type of AI approach) could result in greater risks. Therefore, any AI system risk assessment should consider **the technical characteristics** along **with its specific use cases and the context** in which the system operates.

25. In the light of the above, the EDPB and the EDPS recommend specifying in the Proposal that **the provider** shall perform an initial risk assessment on the AI system at stake **considering the use-cases** (to be specified in the Proposal - complementing for instance Annex III, 1(a), where the use-cases of AI biometric systems are not mentioned), and that the **user** of the AI system, in its quality of data controller under the EU data protection law (if relevant), shall perform the DPIA as detailed provided in Article 35 GDPR, Article 39 of the EUDPR and Article 27 LED, considering not only the technical characteristic and **the use case**, but **also the specific context** in which the AI will operate.

26. Moreover, some of the terms mentioned in Annex III of the Proposal, e.g. the term "essential private services" or small-scale provider using creditworthiness assessment AI for their own use, should be clarified.

2.3 Prohibited uses of AI

27. The EDPB and the EDPS consider that **intrusive forms of AI** – especially those who may affect human dignity – are to be seen as prohibited AI systems under Article 5 of the Proposal instead of simply being classified as "high-risk" in Annex III of the Proposal such as those under No. 6. This applies in particular to data comparisons that, on a large scale, also affect persons who have given no or only slight cause for police observation, or processing which impairs the principle of purpose limitation under data protection law. The use of AI in the area of police and law enforcement requires area-specific, precise, foreseeable and proportionate rules that need to consider the interests of the persons concerned and the effects on the functioning of a democratic society.

28. Article 5 of the Proposal risks paying lip service to the "values" and to the prohibition of AI systems in contrast with such values. Indeed, the criteria referred to under Article 5 to "qualify" the AI systems as prohibited **limit the scope of the prohibition** to such an extent that it could turn out to be meaningless in practice (e.g. "causes or is likely to cause [...] physical or psychological harm" in Article 5 (1) (a) and (b); limitation to public authorities in Article 5(1)(c); vague wording in and points (i) and (ii) under (c); limitation to "real time" remote biometric identification only without any clear definition etc.).

29. In particular, the use of AI for "social scoring", as foreseen in Article 5(1) (c) of the Proposal, can lead to discrimination and is against the EU fundamental values. The Proposal only prohibits these practices when conducted 'over a certain period of time' or 'by public authorities or on their behalf'. Private companies, notably social media and cloud service

providers, can process vast amounts of personal data and conduct social scoring. Consequently, **the Proposal should prohibit any type of social scoring**. It should be noted that in the law enforcement context, Article 4 LED already significantly limits – if not in practice prohibits – such type of activities.

30. **Remote biometric identification** of individuals in publicly accessible spaces poses a high-risk of intrusion into individuals' private lives. Therefore, the EDPB and the EDPS **consider that a stricter approach is necessary**. The use of AI systems might present serious proportionality problems, since it might involve the processing of data of an indiscriminate and disproportionate number of data subjects for the identification of only a few individuals (e.g., passengers in airports and train stations). The **frictionless** nature of remote biometric identification systems also presents transparency problems and issues related to the legal basis for the processing under the EU law (the LED, the GDPR, the EUDPR and other applicable law). The problem regarding the way to properly inform individuals about this processing is still unsolved as well as the effective and timely exercise of the rights of individuals. The same applies to **its irreversible, severe effect on the populations'** (reasonable) **expectation of being anonymous in public spaces**, resulting in a direct negative effect on the exercise of freedom of expression, of assembly, of association as well as freedom of movement.

31. Article 5(1)(d) of the Proposal provides an extensive **list of exceptional cases** in which 'real-time' remote biometric identification in publicly accessible spaces is permitted for the purpose of law enforcement. The EDPB and the EDPS consider **this approach flawed** on several aspects: First, it is unclear what should be understood as "a significant delay" and how should it be considered as a mitigating factor, taking into account that a mass identification system is able to identify thousands of individuals in only a few hours. In addition, the intrusiveness of the processing does not always depend on the identification being done in real-time or not. Post remote biometric identification in the context of a political protest is likely to have a significant chilling effect on the exercise of the fundamental rights and freedoms, such as freedom of assembly and association and more in general the founding principles of democracy. Second, the intrusiveness of the processing does not necessarily depend on its purpose. The use of this system for other purposes such as private security represents the same threats to the fundamental rights of respect for private and family life and protection of personal data. Lastly, even with the foreseen limitations, the potential number of suspects or perpetrators of crimes will almost always be "high enough" to justify the continuous use of AI systems for suspect detection, despite the further conditions in Article 5(2) to (4) of the Proposal. The reasoning behind the Proposal seems to omit that when monitoring open areas, the obligations under EU data protection law need to be met for not just suspects, but for all those that in practice are monitored.

32. For all these reasons, the EDPB and the EDPS **call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals - in any context.** The current approach of the Proposal is to identify and list all AI systems that should be prohibited. Thus, for consistency reasons, **AI systems for**

large-scale remote identification in online spaces should be prohibited under Article 5 of the Proposal. Taking into account the LED, the EUDPR and GDPR, the EDPS and EDPB cannot discern how this type of practice would be able to meet the necessity and proportionality requirements, and that ultimately derives from what are considered acceptable interferences of fundamental rights by the CJEU and ECtHR.

33. Moreover, the EDPB and EDPS **recommend a ban**, for both public authorities and private entities, on **AI systems categorizing individuals from biometrics (for instance, from face recognition) into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination prohibited under Article 21 of the Charter, or** AI systems whose scientific validity is not proven or which are in direct conflict with essential values of the EU (e.g., polygraph, Annex III, 6. (b) and 7. (a)). Accordingly, "**biometric categorization**" should be **prohibited under Article 5**.

34. It also **affects human dignity to be determined or classified by a computer as to future behavior independent of one's own free will**. AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending of reoffending criminal offences, cf. Annex III, 6. (a), or for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of a natural person or on assessing personality traits and characteristics or past criminal behavior, cf. Annex III, 6. (e) used according to their intended purpose will lead to pivotal subjection of police and judicial decision-making, thereby objectifying the human being affected. Such AI systems touching the essence of the right to human dignity should be prohibited under Article 5.

35. Furthermore, the EDPB and the EDPS consider that the use of AI to **infer emotions of a natural person is highly undesirable and should be prohibited,** except for certain well-specified use-cases, namely for health or research purposes (e.g., patients where emotion recognition is important), always with appropriate safeguards in place and of course, subject to all other data protection conditions and limits including purpose limitation.

2.4 High-risk AI systems

2.4.1 Need for an *ex-ante* conformity assessment by external third parties

36. The EDPB and the EDPS welcome that AI systems that pose a high-risk must be subject to a prior conformity assessment before they can be placed on the market or otherwise put into operation in the EU. In principle, this regulatory model is welcomed, as it offers a good balance between innovation-friendliness and a high level of proactive protection of fundamental rights. In order to be brought to use in specific environments like decision-making processes of public service institutions or critical infrastructure, ways to investigate the full source code must be laid out.

37. However, the EDPB and the EDPS advocate adapting the conformity assessment procedure under Article 43 of the Proposal to the effect that an ***ex ante*** **third-party conformity assessment must generally be carried out for high-risk AI**. Although a third-party conformity assessment for high-risk processing of personal data is not a requirement in the

GDPR or EUDPR, the risks posed by AI systems are yet to be fully understood. The general inclusion of an obligation for third-party conformity assessment would therefore further strengthen legal certainty and confidence in all high-risk AI systems.

2.4.2 Scope of regulation must also cover AI systems already in use

38. According to Article 43(4) of the Proposal, high-risk AI systems should be subject to a new conformity assessment procedure whenever a significant change is made. It is right to ensure that AI systems comply with the requirements of the AI Regulation throughout their lifecycle. AI systems that have been placed on the market or put into service before application of the proposed regulation (or 12 months thereafter for large-scale IT systems listed in Annex IX) are excluded from their scope, unless those systems are subject to 'significant changes' in design or intended purpose (Article 83).

39. Yet, the threshold for 'significant changes' is unclear. Recital 66 of the Proposal specifies a lower threshold for conformity re-assessment "whenever a change occurs which may affect the compliance". A similar threshold would be appropriate for Article 83, at least for high-risk AI systems. Additionally, in order to close any protection gaps, it is necessary that AI systems already established and in operation - after a certain implementation phase - also comply with all requirements of the AI Regulation.

40. The manifold possibilities of personal data processing and external risks affect the security of AI systems, too. The focus of Article 83 on "significant changes in design or intended purpose" does not include a reference to changes in external risks. A reference to changes of the threats-scenario, arising from external risks, e.g., cyber-attacks, adversarial attacks and substantiated complaints from consumers therefore should be included in Article 83 of the Proposal.

41. Moreover, as the entry into application is envisaged for 24 months following the entry into force of the future Regulation, the EDPS and EDPB do not consider it appropriate to exempt AI systems already placed on the market for an even longer period of time. While the Proposal also provides that the requirements of the Regulation shall be taken into account in the evaluation of each large-scale IT system as provided by the legal acts listed in Annex IX, the EDPB and EDPS consider that requirements concerning the putting into service use of AI systems should be applicable from the date of application of the future Regulation.

2.5 Governance and European AI Board

2.5.1 Governance

42. The EDPB and the EDPS welcome the designation of the EDPS as the competent authority and the market surveillance authority for the supervision of the Union institutions, agencies and bodies when they fall within the scope of this Proposal. The EDPS stands ready to fulfil its new role as the AI regulator for the EU public administration. Moreover, the role and tasks of the EDPS are not sufficiently detailed and should be further clarified in the Proposal, specifically when it comes to its role as market surveillance authority.

43. The EDPB and the EDPS acknowledge the allocation of financial resources, which is foreseen for the Board and the EDPS, acting as a notifying body, in the Proposal. However, the fulfillment of the new duties foreseen for the EDPS, whether when acting as notified body, would require significantly higher financial and human resources.

44. Firstly, because the wording of Article 63 (6) states that the EDPS "shall act as market surveillance authority" for Union institutions, agencies and bodies that fall within the scope of the Proposal, which does not clarify if EDPS is to be considered a fully embodied "market surveillance authority", as foreseen in Regulation (EU) 2019/1020. This raises questions about the duties and powers of the EDPS in practice. Secondly, and provided that the former question is answered affirmatively, it is unclear how the role of the EDPS, as foreseen in EUDPR can accommodate the task foreseen in Article 11 of the Regulation (EU) 2019/1020, which include "effective market surveillance within their territory of products made available online" or "physical and laboratory checks based on adequate samples". There is the risk that taking up the new set of tasks without further clarifications in the Proposal might endanger the fulfillment of its obligations as data protection supervisor.

45. However, the EDPB and the EDPS underline that some provisions of the Proposal defining the tasks and powers of the different competent authorities under the AI regulation, their relationships, their nature and the guarantee of their independence seem unclear at this stage. Whereas Regulation 2019/1020 states that market surveillance authority must be independent, the draft regulation does not require Supervisory authorities to be independent, and even requires them to report to the Commission on certain tasks carried out by market surveillance authorities, which can be different institutions. Since the proposal also states that DPAs will be the market surveillance authorities for AI systems used for law enforcement purposes (Article 63 (5)) it also means that they will be, possibly via their national supervisory authority, subject to reporting obligations to the Commission (Article 63 (2)), which seems incompatible with their independency.

46. Therefore, the EDPB and the EDPS consider that those provisions need to be clarified in order to be consistent with Regulation 2019/1020, EUDPR and the GDPR, and the Proposal should clearly establish that Supervisory authorities under the AI Regulation must be completely independent in the performance of their tasks, since this would be an essential guarantee for the proper supervision and enforcement of the future Regulation.

47. The EDPB and the EDPS would also like to recall that data protection authorities (DPAs) are already enforcing the GDPR, the EUDPR and the LED on AI systems involving personal data in order to ensure the protection of fundamental rights and more specifically the right to data protection. Therefore, DPAs already have to some extent, as required in the Proposal for the national supervisory authorities, an understanding of AI technologies, data and data computing, fundamental rights, as well as an expertise in assessing risks to fundamental rights posed by new technologies. In addition, when AI systems are based on the processing of personal data or process personal data, provisions of the Proposal are directly intertwined with the data protection legal framework, which will be the case for most of the AI systems in the scope of the regulation. As a result, there will be interconnections of competencies between supervisory authorities under the Proposal and DPAs.

48. Hence, the designation of DPAs as the national supervisory authorities would ensure a more harmonized regulatory approach, and contribute to the consistent interpretation of data processing provisions and avoid contradictions in its enforcement among Member States. It would also benefit all stakeholders of the AI chain of value to have a single contact point for all personal data processing operations falling within the scope the Proposal and limit the interactions between two different regulatory bodies for processing that are concerned by the Proposal and GDPR. As a consequence, the EDPB and the EDPS consider that **DPAs should be designated as the national supervisory authorities pursuant to Article 59 of the Proposal**.

49. In any event, insofar as the Proposal contains specific rules on the protection of individuals with regard to the processing of personal data adopted on the basis of Article 16 TFEU, compliance with these rules, notably restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement, **must be subject to the control of independent authorities**.

50. However, there is no explicit provision in the Proposal that would assign competence for ensuring compliance with these rules to the control of independent authorities. The only reference to competent data protection supervisory authorities under GDPR, or LED is in Article 63(5) of the Proposal, but only as "market surveillance" bodies and alternatively with some other authorities. The EDPB and the EDPS consider that this set up does not ensure compliance with the requirement of independent control set out in Article 16(2) TFEU and Article 8 of the Charter.

2.5.2 The European AI Board

51. The Proposal establishes a "European Artificial Intelligence Board" (EAIB). The EDPB and the EDPS recognize the need for a consistent and harmonized application of the proposed framework, as well as the involvement of independent experts in the development of the EU policy on AI. At the same time, the Proposal foresees to give a predominant role to the Commission. Indeed, not only would the latter be part of the EAIB but it would also chair it and have a right of veto for the adoption of the EAIB rules of procedure. This contrasts with the need for an AI European body independent from any political influence. Therefore, the EDPB and the EDPS consider that the future AI Regulation should give **more autonomy to the EAIB**, in order to allow it to truly ensure the consistent application of the regulation across the single market

52. The EDPB and the EDPS also note that no power is conferred to the EAIB regarding the enforcement of the proposed Regulation. Yet, considering the spread of AI systems across the single market and the likelihood of cross-border cases, there is a crucial need for a harmonized enforcement and a proper allocation of competence between national supervisory authorities. The EDPB and the EDPS therefore recommend that the cooperation mechanisms between national supervisory authorities be specified in the future AI Regulation. The EDPB and EDPS suggest to impose a mechanism guaranteeing a single point of contact for individuals concerned by the legislation as well as for companies, for each AI system, and that for organisations whose activity covers more than half of the Member States of the EU,

the EAIB may designate the national authority that will be responsible for enforcing the AI Regulation for this AI system.

53. Furthermore, considering the independent nature of the authorities that shall compose the Board, the latter shall be entitled to act on its own initiative and not only to provide advice and assistance to the Commission. The EDPB and the EDPS therefore stress the need for an extension of the mission assigned to the Board, which in addition does not correspond to the tasks listed by the Proposal.

54. To satisfy those purposes, the **EAIB shall have sufficient and appropriate powers**, and its legal status should be clarified. In particular, for the material scope of the future Regulation to remain relevant, it seems necessary to involve the authorities in charge of its application in its evolution. Hence, the EDPB and the EDPS recommend that the EAIB should be empowered to propose to the Commission amendments of the annex I defining the AI techniques and approaches and of the annex III listing the high-risk AI systems referred to in article 6(2). The EAIB should also be consulted by the Commission prior any amendment of those annexes.

55. Article 57(4) of the Proposal foresees exchanges between the Board and other Union bodies, offices, agencies and advisory groups. Taking into account their previous work in the field of AI and their human rights expertise, the EDPB and EDPS recommend to consider the Fundamental Rights Agency as one of the observers to the Board.

3 INTERACTION WITH THE DATA PROTECTION FRAMEWORK

3.1 Relationship of the Proposal to the existing EU data protection law

56. A clearly defined relationship between the Proposal and existing data protection law is an essential prerequisite to ensure and uphold the respect and application of the EU acquis in the field of personal data protection. Such EU law, in particular the GDPR, the EUDPR and the LED, has to be considered as a prerequisite on which further legislative proposals may build upon without affecting or interfering with the existing provisions, including when it comes to the competence of supervisory authorities and governance.

57. In the view of the EDPB and the EDPS, it is therefore important to clearly avoid in the Proposal any inconsistency and possible conflict with the GDPR, the EUDPR and the LED. This not only for the sake of legal certainty, but also to avoid that the Proposal has the effect of directly or indirectly jeopardizing the fundamental right to the protection of personal data, as established under Article 16 of the TFEU and Article 8 of the Charter.

58. In particular, self-learning machines could protect the personal data of individuals only if this is embedded by conception. The immediate possibility of exercising the rights of individuals under Article 22 (Automated individual decision-making, including profiling) GDPR or Article 23 EUDPR, regardless of the purposes of processing, is also essential. In this regard, other rights of the data subjects related to the right of deletion, the right of correction

according to the data protection legislation, must be provided in the AI systems from the very beginning, whatever the chosen AI approach or the technical architecture.

59. Using personal data for AI systems learning may lead to the generation of biased decision-making patterns at the core of the AI system. Thus, various safeguards and in particular a qualified human oversight in such processes should be required to ensure that data subjects rights are respected and guaranteed, as well as to avoid any and all negative effects for individuals. Competent authorities should also be able to propose guidelines to assess bias in AI systems and assist the exercise of human oversight.

60. Data subjects should always be informed when their data is used for AI training and / or prediction, of the legal basis for such processing, general explanation of the logic (procedure) and scope of the AI-system. In that regard, individuals' right of restriction of processing (Article 18 GDPR and Article 20 EUDPR) as well as deletion / erasure of data (Article 16 GDPR and Article 19 EUDPR) should always be guaranteed in those cases. Furthermore, the controller should have explicit obligation to inform data subject of the applicable periods for objection, restriction, deletion of data etc. The AI system must be able to meet all data protection requirements through adequate technical and organizational measures. A right to explanation should provide for additional transparency.

3.2 Sandbox & further processing (Articles 53 and 54 of the Proposal)

61. Within the existing legal and moral boundaries, it is important to promote European innovation through tools such as a sandbox. A sandbox gives the opportunity to provide safeguards needed to build trust and reliance on AI systems. In complex environments, it may be difficult for AI practitioners to weigh all interests in a proper manner. Especially for small and medium enterprises with limited resources, operating in a regulatory sandbox may yield quicker insights and hence foster innovation.

62. Article 53, section 3 of the Proposal states that the sandbox does not affect supervisory and corrective powers. If this clarification is useful, there is also a need for the production of direction or guidance on how to strike a good balance between being a supervisory authority on the one hand and giving detailed guidance through a sandbox on the other.

63. Article 53, section 6 describes that the modalities and conditions of the operation of the sandboxes shall be set out in implementing acts. It is important that specific guidelines be produced in order to ensure consistency and support in the establishment and operation of sandboxes. However, binding implementing acts could limit each Member State's ability to customise the sandbox according to their needs and local practices. Thus, the EDPB and the EDPS recommend that the EAIB should provide guidelines for sandboxes instead.

64. Article 54 of the Proposal seeks to provide a legal basis for further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox. The relationship of Article 54(1) of the Proposal to Article 54(2) and recital 41 of the Proposal and thus also to existing EU data protection law remains unclear. However, the GDPR and the EUDPR already have an established basis for 'further processing'. Especially

with regard to cases where it is in the public interest to allow further processing; balancing between the controller's interests and the data subject's interests do not have to hinder innovation. The Article 54 of the Proposal currently does not address two important issues (i) under what circumstances, using which (additional) criteria are the interests of data subjects weighed, and (ii) whether these AI systems will only be used within the sandbox. The EDPB and the EDPS welcomes the requirement for a Union or Member State law when processing personal data collected under the LED in a sandbox, but recommend to further specify what is envisaged here, in a manner that aligns with the GDPR and the EUDPR, mainly by clarifying that the legal basis of such sandboxes should comply with the requirements established in Articles 23 (2) GDPR, 25 EUDPR, and precise that every use of the sandbox must undergo a thorough evaluation. This also applies to the full list of conditions from Article 54(1) point (b to j).

65. Some additional considerations regarding the reuse of data in Article 54 of the Proposal indicate that operating a sandbox is resource intensive and that it is therefore realistic to estimate that only a small number of businesses would get the chance to participate. Participating in the sandbox could be a competitive advantage. Enabling reuse of data would require careful consideration of how to select participants to ensure they are within the scope and to avoid unfair treatment. The EDPB and the EDPS are concerned that enabling reuse of data within the framework of the sandbox diverges from the accountability approach in the GDPR, where the accountability is placed on the data controller, not on the competent authority.

66. Furthermore, the EDPB and the EDPS consider that given the objectives of the sandbox, which are to develop, test and validate AI systems, the sandboxes cannot fall within the scope of the LED. While the LED provides for the reuse of data for scientific research, the data processed for that secondary purpose will be subject to GDPR or EUDPR and no longer to LED.

67. It is not clear what a regulatory sandbox will encompass. The question arises whether the proposed regulatory sandbox includes an IT infrastructure in each Member State with some additional legal grounds for further processing, or whether it merely organizes access to regulatory expertise and guidance. The EDPB and the EDPS urge the legislator to clarify this concept in the Proposal and to clearly state in the Proposal that the regulatory sandbox does not imply an obligation on competent authorities to provide its technical infrastructure. In any cases, financial and human resources must be provided to the competent authorities accordingly to such clarification.

68. Finally, the EDPB and the EDPS would like to emphasize the development of cross-border AI-systems that will be available to the European Digital Single Market as a whole. In the case of such AI-systems, the regulatory sandbox as a tool for innovation should not become a hindrance for cross-border development. Therefore, the EDPB and the EDPS recommend a coordinated cross-border approach that is still sufficiently available at a national level for all SME's, offering a common framework across Europe without being too restrictive. A balance between European coordination and national procedures must be struck in order to avoid

conflicting implementation of the future AI Regulation which would hinder EU-wide innovation.

3.3 Transparency

69. The EDPB and the EDPS welcome that high-risk AI systems shall be registered in a public database (referred to under Article 51 and 60 of the Proposal). This database should be taken as an opportunity to provide information for the public at large on the scope of application of AI system and on known flaws and incidents that might compromise their functioning and the remedies adopted by providers to address and fix them.

70. A key democratic principle is the use of checks and balances. Therefore, the fact that the transparency obligation does not apply to AI systems used to detect, prevent, investigate, or prosecute criminal offences is too broad of an exception. A distinction must be made between AI systems that are used to detect or prevent and AI systems that aim to investigate of help the prosecution of criminal offenses. Safeguards for prevention and detection have to be stronger because of the presumption of innocence. Moreover, the EDPB and the EDPS regret the absence of cautionary warnings in the proposal, which can be interpreted as a greenlight for the use of even unproven, high-risk AI systems or applications.

71. In those cases where little to no transparency can be given to the public due to reasons of secrecy, even in a well-functioning democracy, safeguards should be in place and those AI systems should be registered with and provide transparency to the competent supervisory authority.

72. Ensuring transparency in AI systems is a very challenging goal. The fully quantitative decision-making approach of many AI systems, inherently different from human approach mostly relying on causal and theoretical reasoning, may conflict with the need to get a prior understandable explanation of machine outcomes. The Regulation should promote new, more proactive and timely ways to inform users of AI systems on the (decision-making) status where the system lays at any time, providing early warning of potential harmful outcomes, so that individuals whose right and freedoms may be impaired by machine's autonomous decisions may react, or redress the decision.

3.4 Processing of special categories of data & data relating to criminal offences

73. The processing of special categories of data in the area of law enforcement is governed by the provisions of the EU data protection framework, including the LED as well as its national implementation. The Proposal claims not to provide a general legal ground for processing of personal data, including special categories of personal data, cf. recital 41. At the same time, Article 10 (5) of the Proposal reads "the providers of such systems may process special categories of personal data". Furthermore, the same provision requires additional safeguards, also giving examples. Thereby, the Proposal seems to interfere with the application of the GDPR, the LED and the EUDPR. While the EDPB and the EDPS welcome the attempt to arrange for adequate safeguards, a more coherent regulatory approach is needed, as the current provisions do not seem sufficiently clear to create a legal basis for the processing of

special categories of data, and need to be complemented with additional protective measures that still need to be assessed. Moreover, when personal data have been collected by processing within the scope of the LED the possible additional safeguards and limitations stemming from the national transpositions of the LED will need to be taken into account.

3.5 Compliance mechanisms

3.5.1 Certification

74. One of the main pillars of the Proposal is certification. The certification system outlined in the Proposal is based on a structure of entities (Notifying Authorities/Notified Bodies/Commission) and a conformity assessment/certification mechanism covering the mandatory requirements applicable to high-risk AI systems, and based on European harmonized standards under Regulation (EU) No 1025/2012 and common specifications to be established by the Commission. This mechanism is different from the certification system aimed at ensuring compliance with data protection rules and principles, outlined in Articles 42 and 43 of the GDPR. It is however not clear how certificates issued by notified bodies in accordance with the Proposal may interface with data protection certifications, seals and marks provided for by the GDPR, unlike what it is provided for other types of certifications (see Article 42(2) with regard to certifications issued under Regulation (EU) 2019/881).

75. As far as high-risk AI systems are based on the processing of personal data or process personal data to fulfil their task, these misalignments may generate legal uncertainties for all concerned bodies, since they may lead to situations in which AI systems, certified under the Proposal and marked with a CE marking of conformity, once placed on the market or put into service, might be used in a way which is not compliant with the rules and principles of data protection.

76. The Proposal is missing a clear relation to the data protection law as well as other EU and Member States law applicable to each ‘area’ of high-risk AI system listed in Annex III. In particular, the proposal should include the principles of data minimization and data protection by design as one of the aspects to take into consideration before obtaining the CE marking, given the possible high level of interference of the high-risk AI systems with the fundamental rights to privacy and to the protection of personal data, and the need to ensure a high level of trust in the AI system. Therefore, the EDPB and the EDPS recommend amending the Proposal so as to clarify the relationship between certificates issued under the said Regulation and data protection certifications, seals and marks. Lastly, the data protection authorities should be involved in the preparation and establishment of harmonized standards and common specifications.

77. In connection with Article 43 of the Proposal, relating to the conformity assessment, the derogation from the conformity assessment procedure set out in Article 47 seems to be very broad including too many exceptions such as reasons of exceptional reasons of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets. We would propose the legislators to narrow them down.

3.5.2 Codes of conduct

78. According to Article 69 of the Proposal, the Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct (CoCs) intended to foster the voluntary application by providers of non-high-risk AI systems of the requirements applicable to high-risk AI systems, as well as additional requirements. In line with recital 78 of the GDPR, the EDPB and the EDPS recommend identifying and defining synergies between these instruments and the codes of conduct provided for by the GDPR which support data protection compliance. In this context, it is relevant to clarify if the protection of personal data is to be considered among "additional requirements" that can be addressed by the CoCs referred to in paragraph 2 of Article 69. It is also relevant to ensure that the "technical specifications and solutions", addressed by the CoCs referred to in paragraph 1 of Article 69, as designed to foster compliance with the requirements of the AI draft Regulation, do not conflict with the rules and principles of the GDPR and the EUDPR. By doing so, adherence to these tools by providers of non-high-risk AI systems - as far as such systems are based on the processing of personal data or process personal data to fulfil their task - would represent an added value, since this will ensure that controller and processors will be able to fulfil their data protection obligations in the use of those systems.

79. At the same time, the legal framework for trustworthy AI would result complemented by the integration of CoCs, so as to foster trust in the use of this technology in a way that is safe and compliant with the law, including the respect of fundamental rights. However, the design of these instruments should be strengthened by envisaging mechanisms aimed at verifying that such codes provide effective "technical specifications and solutions" and set out "clear objectives and key performance indicators to measure the achievement of those objectives" as integral parts of the codes in question. Moreover, the absence of any reference to (mandatory) monitoring mechanisms for codes of conduct designed to verify that providers of non-high-risk AI systems comply with their provisions, as well as the possibility for individual providers to draw up (and implement themselves) the said codes (see section 5.2.7 of the explanatory memorandum) may further weaken the efficacy and enforceability of these instruments.

80. Lastly, the EDPB and the EDPS ask for clarifications with regard to the types of initiatives the Commission may develop, according to recital 81 of the Proposal, "to facilitate the lowering of technical barriers hindering cross-border exchange of data for AI development".

4 CONCLUSION

81. Even though the EDPB and the EDPS welcome the Proposal of the Commission and consider that such a regulation is necessary to guarantee the fundamental rights of EU citizens and residents, they consider that the Proposal needs to be adapted on several issues, to ensure its applicability and efficiency.

82. Given the complexity of the Proposal as well as the issues it aims to tackle, a lot of work remains to be done until the Proposal can give birth to a well-functioning legal framework, efficiently supplementing the GDPR in protecting basic human rights while fostering innovation. The EDPB and the EDPS will continue to be available to offer their support in this journey.

Brussels, 18 June 2021

For the European Data Protection Board	For the European Data Protection Supervisor
The Chair	The Supervisor
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI