ARTIFICIAL INTELLIGENCE

A PROPOSAL FOR (AI) CHANGE? A succinct overview of the Proposal for Regulation laying down harmonised rules on Artificial Intelligence.

INTRODUCTION

The benefits from the implementation of Artificial Intelligence ("**AI**") systems for citizens are clear. However, the European Commission ("**EC**") seems to be conscious about the rights arising from the use in terms of both safety and human rights. In this context, as part of an ambitious European Strategy for AI, the European Commission has published the proposal for a Regulation on a European approach for AI (the "**Proposal**")[304], where AI is not conceived as an end in itself, but as a tool to serve people with the ultimate aim of increasing human well-being.

The Proposal does not focus on technology, but on the potential use that different stakeholders could make of AI systems and, as a result, potential damages arising from its use. To address potential damages while capturing the full potential of AI related technologies, the Proposal, following an horizontal approach, is based on four building blocks: (i) measures establishing a defined risk-based approach; (ii) measures in support of innovation; (iii) measures facilitating the setting up of voluntary codes of conduct; and (iv) a governance framework supporting the implementation of the Proposal at EU and national level and its adaptation as appropriate.

One may wonder why the Proposal is needed. The functioning of AI systems may be challenging due to its complexity, autonomy, unpredictability, opacity and the role of data within this equation. Such characteristics are not selected in an arbitrary manner but purposely spotted by the regulator as areas of concern in terms of: (i) safety; (ii) fundamental rights; (iii) enforcement of rights; (iv) legal uncertainty; (v) mistrust in technology; and (vi) fragmentation within the EU.

[304] Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Available at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence

The Proposal is not a surprise for many legal experts in the field and, as expected, leverages on, inter alia, the work carried out by the High-Level Expert Group on Artificial Intelligence (Ethics Guidelines for Trustworthy AI[305] and the Policy and Investment Recommendations for Trustworthy AI[306]), the Communication from the EC on Building Trust in Human-Centric Artificial Intelligence[307], the White Paper on Artificial Intelligence[308], including the Data Governance Act[309], the Open Data Directive[310] and other legislative initiatives covered under the European Data Strategy.[311]

The Proposal introduces many aspects that might deserve further clarification as the legislative process goes on. Some are (i) the scope of application of the Proposal; (ii) the definition of AI systems; (iii) the AI-risk based approach; (iv) the role of standards (e.g. conformity assessment and CE marking and process); (v) the role of data, the obligations on data quality and the interaction of the Proposal with the legislation governing both personal and non-personal data; and (vi) the governance structure and the role of the European Commission, the (new) Artificial Intelligence Board, the AI Expert Group and, at a national level, national

[305] HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, *Ethics Guidelines for Trustworthy AI.* April 2019. Available at https://ec.europa.eu/futurium/en/ai-alliance-consultation#:~:text=The%20Ethics%20Guidelines%20for%20Trustworthy%20Artificial%20Intelligence%20%28AI%29,of%20the%20AI%20strategy%20announced%20earlier%20that%20year.

[306] HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, *Policy and investment recommendations for trustworthy Artificial Intelligence,* July 2020. Available at https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence. (Accesed on May 2021).

[307] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2019) 168 final, April 2019. Available at https://ec.europa.eu/jrc/communities/en/community/digitranscope/document/building-trust-human-centric-artificial-intelligence.

[308] White Paper on Artificial Intelligenec - A european appraoch to excellenec and trust, COM(2020) 65 final, February 2020. Available at commission-white-paper-artificial-intelligence-feb2020_en.pdf (europa.eu).

[309] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), COM/2020/767 final. Available at EUR-Lex - 52020PC0767 - EN - EUR-Lex (europa.eu).

[310] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1. Available at EUR-Lex - 32019L1024 - EN - EUR-Lex (europa.eu).

[311] See more information here: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

competent authorities. The following paragraphs shall be devoted to explore some of the above mentioned aspects.

1. AI Definition

Finding an AI definition seemed to be a challenge for the EC and, yet, current definition is not exempt from controversy due to its broadness. As a matter of fact, AI is defined as "*software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*" (Art. 3.1 (1) of the Proposal), where Annex I lays down a list of AI techniques and approaches such as, currently, machine learning, logic -and knowledge based- and statistical.

Although the aim of the EC was to provide a neutral definition in order to cover current and future AI techniques, many stakeholders have already manifested their concerns with regards to the comprehensiveness of this definition. The latter, considering that, while it is convenient to promote flexible legislation, this broad definition including a referral to the Annex I potentially subject to periodical amendments, may raise some legal uncertainty concerns in the industry.

2. An (overreaching) scope?

To ensure the horizontal application of key requirements developed by the High-Level Expert Group on Artificial Intelligence, the Proposal aims at harmonising certain rules concerning the placing on the market, putting into service and use of AI systems that create a high risk to the health and safety or fundamental rights of natural persons ("**high-risk AI systems**") in the EU.

Based on the intended purpose of the AI system and following a risk based approach, the Proposal: (i) prohibits certain AI practices; (ii) establishes requirements and obligations for high-risk AI systems - both *ex-ante* and *ex-post*; and (iii) sets forth limited transparency obligations for certain AI systems.

Despite the intention to establish a common normative standard for all high-risk AI systems, the application of the Proposal is limited when it comes: (i) to AI systems intended to be used as safety components of products or systems, or which are themselves products or systems covered by certain legislation applying

to aviation, railways, motor vehicles and marine equipment sectors. (Art. 2.2 of the Proposal); and (ii) AI systems used for military purposes.

One may also ask, which are the stakeholders affected by the Proposal considering, in particular, the complexity and comprehensiveness of the AI ecosystem. Here, the European Union legislator seemed to be inspired by Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**") [312], establishing that the Proposal shall apply to:

– Providers of AI systems irrespective of whether they are established within the EU or in a third country outside the EU;

– Users of AI systems established within the EU;

– Providers and users of AI systems that are established in a third country outside the EU, to the extent the AI systems affects persons located in the EU;

– EU institutions, Offices and Bodies.

On the one hand, Art. 3 (2) of the Proposal defines "provider" as the one who "*develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge.* On the other hand, according to Art. 3 (4) "user" means any "*natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity*".

Hence, apart from suggesting a broad territorial scope of application, affecting providers and users located outside the EU, the Proposal seems to bring different obligations down the supply chain, placing on the ultimate provider and professional user of the AI system much of the legal burden coming from the Proposal.

Considering the multiplicity of stakeholders intervening in the AI system lifecycle (e.g. data providers, third-party assessment entities, integrators, software

[312] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

developers, hardware developers, telecom operators, over the top service providers, etc.) and the High-Level Expert Group on Artificial Intelligence Guidelines recommendations on inclusive and multidisciplinary teams for the development of AI systems, the Proposal, in general, fails to provide guidance on how the interaction between AI system supply chain stakeholders shall be.

Therefore, legal issues amongst stakeholders may arise such as potential contractual derogations, attributions of contractual and non-contractual liability and its validity (and compatibility) according to the principle of accountability - as inspiring the whole Proposal. In addition, is worth mentioning that the consistency with other legal frameworks such as defective product legislation is fundamental in order to ensure cohesion and legal certainty - see, to this end, the EC Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics [313].

3. And the Commission said "risk-based approach"

The Proposal provides four non-mutually exclusive categories of risk: (i) unacceptable risk; (ii) high-risk; (iii) other risk - AI with specific transparency obligations; and (iv) low or no risk. Depending on the category of risk, the obligations of providers, users and other stakeholders will vary, from complete prohibition to permission with no restrictions.

3.1. *Prohibition*

In this context, following the category of risk for which there is an unacceptable risk, the EC proposes to prohibit, mainly, the following AI practices:

i. AI systems that deploy subliminal techniques beyond a person's consciousness to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;
ii. AI systems that exploit people's vulnerabilities due to their age, physical or mental disability, in order to distort the behaviour of a person in a manner that causes or is likely to cause harm to that person;

[313] Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final. Available at https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064

iii. AI systems, used by public authorities or on their behalf, for the evaluation or classification of the trustworthiness of natural persons when the social scoring may lead to detrimental or unfavourable treatment: (a) in social contexts which are unrelated to the contexts in which the data was originally generated or collected; or (b) that is unjustified or disproportionate to their social behaviour or its gravity; and

iv. the use of 'real time' remote biometric identification systems in publicly available spaces for law enforcement, unless and in as far as such us is strictly necessary for different objectives (e.g. targeted search for specific potential victims of crime; prevention of specific, substantial and imminent threat to the life of physical safety of natural persons or a terrorist attack, etc.).

While the Proposal prohibits some AI practices that were already under the spotlight of different Member States, such as facial recognition systems (see for instance the decision from the Italian Data Protection Authority -*Garante per la Protezione dei Dati Personali*- with regards to the Sari Real Time system[314]), other cases leave room for interpretation such as "AI systems that exploit people's vulnerabilities" or "AI systems that deploy subliminal techniques". Therefore, the scope of the prohibition of certain AI practices under the Proposal, would be broader in comparison with the specific use cases banned so far within the European Union.

3.2. *High-level risk*

The proposed regulation establishes quite a broad list of sectors and uses potentially falling within the high-level risk category that, could be amended from time to time by the EC. In particular, according to Art. 6 of the Proposal, an AI shall be classified as high-risk, in the following scenarios:

i. In cases where the following two conditions are met:

[314] Italian Data Protection Authority, Opinion on the system SARI REAL TIME, [9575877], March 2021. Available in Italian at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877

a. the AI system is intended to be used as a safety component of a product or is itself a product, covered by the list of Union harmonisation legislation listed in Annex II of the Proposal.

b. the products whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment in order to be placed on the market or put into service pursuant to legislation contained in Annex II.

ii. For the AI systems provided in Annex III.

Therefore, the current list of high-level risk AI systems is contained in Annexes II and III of the Proposal. While Annex II covers a wide range of products or safety component of products governed by sectorial European Union law, such as machinery, transport, medical devices or radio equipment; Annex III defines some high-risk applications such as biometric identification and identification of natural persons, management and operation of critical infrastructures, AI for recruitment purposes, law enforcement, or education and vocational training.

High-level risk AI systems are at the centre of the Proposal, which establishes a set of obligations covering the entire AI lifecycle - from its design to its implementation. Such requirements include: (i) to carry out a conformity assessment and subsequent CE marking; (ii) transparency and information obligations; (iii) sign up in the EU database for high-risk AI practices; (iv) logging of activities; (v) human oversight; (vi) record-keeping and documentation obligations; (vii) establishment of risk and quality management systems; (viii) robustness, accuracy and cybersecurity obligations; and (ix) use of high-quality datasets for training, validation and testing. Most relevant obligations both, for AI providers and users, are the following:

Provider obligations	**User obligations**
– Establish and implement quality management system.	– Operate AI systems in accordance with instructions of use.

– Elaborate and keep up to date technical documentation. – Logging obligations to enable users to monitor the operation of the high-risk AI system. – Conduct conformity assessments, and potentially re-assessment of the system in case of significant modifications. – Conduct post-market monitoring. – Collaborate with market surveillance authorities.	– Ensure human oversight when using of AI system. – Monitor operation for possible risks. – Inform the provider or distributor about any serious incident or any malfunctioning. – Compliance with existing legal obligations (e.g. GDPR).

Source: L. SIOLI, CEPS webinar -European approach to the regulation of artificial intelligence (April 2021).

As suggested, high-risk AI systems concentrate the bulk of requirements established in the Proposal, lacking guidance in some aspects and introducing some caveats that, hopefully, will be clarified during the legislative process.

3.3. *Other risk*

Operators placing, putting into service or using AI systems having a lesser risk than high-risk AI systems shall still have to comply with transparency obligations vis-à-vis users and implementers, such as: (i) notification to humans that are interacting with an AI system, unless such interaction is evident; (ii) notification to humans that are being subject to emotional recognition or biometric categorisation systems; and (iii) application of labels to 'deep fakes', unless the use of 'deep fakes' becomes necessary for public interest reasons (e.g. criminal offences) or it is necessary for the exercise of fundamental rights (Art. 54 of the Proposal).

This category of risk comes also with different caveats that prevent the application of different notification obligations. As anticipated, some clarification could be also needed here. When doesthe interaction with an AI system becomes evident? How should the 'notifications' be carried out?

3.4. *Limited or no risk*

Although AI systems under this category do not result in mandatory obligations for its providers and users, the Proposal imposes the EC and the European AI Board to encourage the development of codes of conduct to enhance transparency and information about such "low or no risk" AI systems (Art. 69 of the Proposal).

In light of the above, although the EC understands that, in general, most AI systems will not entail a high-risk, one may observe a set of rules are widely applicable to all categories of risk in order to enhance, inter alia, transparency, safety and accountability within the AI ecosystem.

4. Measures in support of innovation

A very welcome mechanism are the AI regulatory sandboxes. Regulatory sandboxes represent a regulatory concept based on "experimental legislation", where technology companies can test and develop their innovations benefiting, for instance, from the exemption of the application of certain specific rules or legal regimes under a controlled environment. In particular AI regulatory sandboxes provide a controlled environment where the development, testing and validation of innovative AI systems are facilitated for a period of time before coming into the market under the supervision of Member states authorities or the European Data Protection Supervisor.

Although the modalities, conditions and other criteria shall be governed by the corresponding implementing acts, the Proposal seems to introduce some flexibilities when it comes to further data processing in this context (Arts. 53 and 54 of the Proposal).

The EC has proved particularly sensitive to small-scale providers and start-ups, providing some advantages through the Proposal in order to enable greater access to available resources and establish a level playing field regardless of the size and scope of the company. It is remarkable, for instance, the differentiation that from the very beginning is made between "providers" and "small-scale providers" (Art. 3 of the Proposal) in an attempt to foster the creation of a level-playing field also adapted to micro or small enterprises.

For instance, the Proposal foresees priority access to AI sandboxes to be legally granted for small-scale providers and start-ups (Art. 55 of the Proposal); organisation of awareness raising activities about the Proposal (Art. 55 of the Proposal); or the consideration -by the EC and the European AI Board- of the specific interests and needs of small-scale providers and start-ups when encouraging and drawing up codes of conduct (Art. 69.4 of the Proposal).

5. Governance structure and enforcement

Governance structure and enforcement seem to bear some similarities with the GDPR. As such, the Proposal creates the European Artificial Intelligence Board, which shall coordinate its activities with the corresponding National Competent Authorities. This, as such, is not the only novelty but, always at the European level, the EC is expected to act as secretariat and a supporting AI Expert Group (potentially equivalent to the High-Level Expert Group on Artificial Intelligence) to be created in the future.

In addition, administrative sanctions mirror those established in the GDPR, broken down to different scales depending on the severity of the infringement and amounting to up to 30 million of euros or the 6% of the total worldwide annual turnover of the preceding financial year for most severe infringements (Art. 71 of the Proposal). The EC itself does not seem entitled to impose sanctions, since this task has been attributed to Member States' national authorities.

Some questions are still left open, such as coordination mechanisms between authorities, in particular with regards to cross-border infringements of the Proposal. In addition, there is still some lack of clarity on what the specific authorities are expected to have competence at a national level. Current local Data Protection Authorities? Brand-new national AI authorities?

Finally, current administrative procedures mimicking, to a great extent, the current EU competition law system and the GDPR, also risk leading to fragmentation and heterogeneity between Member States. In particular, the lack of a clear decision review mechanism at a European level (i.e. administrative sanctions are only reviewed at a national level) and the entitlement of authorities to decide on an infringement having an impact in more than one member state, remain unclear.

6. "What's in" for Intellectual Property?

As one may understand, the main focus of the Proposal is not Intellectual Property ("**IP**") but an horizontal approach to AI. Still, even though IP is only referred to twice throughout the Proposal, some questions remain unanswered, in particular, how to ensure the compliance with the obligations set forth in the Proposal while protecting IP rights and trade secrets. Here, the dichotomy between access and protection to ensure easy implementation, safety and interoperability of AI systems could need to be revisited.

Regarding transparency and information to users when using high-risk AI systems, several points can be made. What does it mean that the "*operation is sufficiently transparent to enable users to interpret the system's output*" foreseen in Art. 13 of the Proposal? Does IP act as a facilitator or as a barrier to this transparency requirement? Does the current IP legal system foresee appropriate mechanisms in order to access necessary information?

Apart from specific transparency obligations, some other legal requirements set forth in the Proposal may entail the communication of different business and technology related information to other operators. For instance, how to ensure appropriate risk and quality assessment systems while there is protected information for stakeholders having to implement such systems? Do different stakeholders along the AI supply chain need to access IP and trade secret protected information or data? Which are the IP barriers to ensure data interoperability?

One may argue, for instance, from a copyright perspective, that the entitlement to "*observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program*" (Art. 5.3 of the Software Directive[315]) or the possibility to decompile the software (Art. 6 of the Software Directive) could not be of great use in cases where software is being

[315] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0024&from=EN

periodically modified, considering also that observing, studying, testing or decompiling such software most of times becomes a costly process.

With regards to patent law, can the current "*sufficient disclosure*" obligation standard (see, for instance Art. 83 of the European Patent Convention[316] be enough to ensure a "*sufficiently transparent*" operation? Could Art 27 (k) of the Agreement on a Unified Patent Court[317] (providing that acts covered under Art. 6 of the Software Directive do not constitute an infringement in particular with regards to de-compilation and interoperability) inspire reverse engineering exceptions for the purposes to obtain information allowed under previously mentioned Art. 5 of the Software Directive?

Trade Secrets Directive[318] regime is even more restrictive than previous "de-compilation" exception and only allows reverse engineering or access to information where the acquirer of the trade secret is free from any legally valid duty to limit the acquisition of the trade secret (Art. 3.1 (b) of the Trade Secrets Directive). Nevertheless, the novelty of the Trade Secrets Directive and the lack of case law causes some legal uncertainty.

Moreover, the Proposal establishes the obligation to disclose the AI source code to enforcement authorities. Although this practice could be covered under specific or general exemptions provisions currently in force based on the principle of public interest (e.g. Art. 1.2 (b) and Recital 11 of the Trade Secrets Directive), how is access to the source code useful for enforcement authorities? What is the scope of source code to be disclosed? That of the trained AI model? The validated AI model? The code to build the AI model? In practice, the above could lead to divergent practices between national authorities, which could be

[316] Convention on the Grant of European Patents (European Patent Convention), 17th Edition, November 2020. Available at http://documents.epo.org/projects/babylon/eponet.nsf/0/53A0FE62C259803BC12586A90058BCAD/$File/EPC_17th_edition_2020_en.pdf

[317] Agreement on a Unified Patent Court, OJ C 175, April 2013. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42013A0620%2801%29

[318] Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943

requesting slightly different types of information, in particular when it comes to AI systems using machine learning approaches.

Also in this context, Art. 70 of the Proposal with regards to disclosure obligations, particularly protects the confidentiality of information and data communicated to national competent authorities and notified bodies involved in the application of the Proposal. In this line, authorities shall carry out "*their tasks and activities in such a manner as to protect, in particular: (i) intellectual property rights, and confidential business information or trade secrets of a natural or legal person, including source code, except the cases referred to in Article 5* [of the Trade Secrets Directive]", where the latter provision foresees four exceptions to trade secrets rights. At this stage, albeit the protection of IP rights, confidential information and trade secrets was addressed by the legislator when drafting the Proposal, the same appears to leave room to authorities to decide which the concrete measures for its protection shall be without providing ulterior guidance (i.e. *"carrying out activities in such a manner as to protect")*.

In addition, the Proposal provides that "*the increased transparency obligations will also not disproportionately affect the right to protection of intellectual property (Article 17(2) [EU Charter of Fundamental Rights*[319]*), since they will be limited only to the minimum necessary information for individuals to exercise their right to an effective remedy and to the necessary transparency towards supervision and enforcement authorities"* and that "*when public authorities and notified bodies need to be given access to confidential information or source code to examine compliance with substantial obligations, they are placed under binding confidentiality obligations*". Therefore, the purpose to set a proper balance between IP and trade secret rights and access to information and data seems clear. However, guidance on concrete measures by national and notified bodies to protect IP, confidential information and trade secrets is desirable.

An additional effort must be done in connection to the above mentioned aspects and, consistently with sectorial regulation having an impact on access (and

[319] Charter of Fundamental Rights of the European Union, 2000/C 364/01. Available at https://www.europarl.europa.eu/charter/pdf/text_en.pdf

protection) of information covered under IP, build a congruent system that ensure the appropriate trade-off between access and protection, not only from a theoretical perspective, but following a pragmatic approach.

Conclusion

The Proposal is very much needed in order to ensure the "human-centred approach" to AI underlined on numerous occasions by different EU Institutions and comes after a long process that, as can be appreciated, has led to what could be considered a well-structured and timely Proposal. Albeit an unprecedented piece of legislation, European Union institutions must ensure that the final outcome does not lead to a burdensome regulation that, in connection with, *inter alia* legislation governing data protection, digital services and sectorial regulation, becomes a complex regulatory maze for companies to navigate through - redounding in a chilling effect to innovation and, as a result, issues connected to the development of the hoped-for fruitful strong digital and AI ecosystem.

Notwithstanding the above, the clarification on certain provisions, consistency with the current IP and data protection legal frameworks, and the application of lessons learnt from the GDPR could make the Proposal "future-proof", also considering the current business, geopolitical and societal context[320]. Also, an appropriate *vacatio legis* term between the adoption of the final text and its entry into force in order to adapt and additional guidance on the governance and enforcement structures shall be fundamental.

Now, the text is into "*inter-institutional*" negotiations, going to the European Parliament and Council for further debate, where different public and private stakeholders shall have the opportunity to get involved.

RUBÉN CANO

Also available at: https://iplens.org/2021/05/11/a-proposal-for-ai-change-a-succinct-overview-of-the-proposal-for-regulation-laying-down-harmonised-rules-on-artificial-intelligence/

[320] See, for instance, Communication from the Commission to the European Parliament and the Council on Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, COM(2020)264 final. Available at https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf