Brussels, 6 June 2019

Dear Members of the High-Level Expert Group on Artificial Intelligence,

On behalf of BSA | The Software Alliance,[1] I congratulate you on the publication of the High-Level Expert Group on Artificial Intelligence ("HLEG") Ethics Guidelines for Trustworthy AI. BSA, whose Members are leaders in the development of cutting-edge AI tools, and have worked globally to ensure that Artificial Intelligence is designed and deployed responsibly, considers the Guidelines an important step for ethical development and deployment of AI in the European Union.

As the HLEG continues its work to develop the Policy and Investment Recommendations on AI, BSA would like to offer some thoughts and guiding principles on important issues surrounding AI, as well as its own analysis of EU Legislation affecting AI, and recommendations on future-proof policies and investment.

1. **AI is a global phenomenon.** More and more the discourse in the EU is veering towards a contrast in AI development of European interests against other countries BSA and its Members have a global presence and are proud to be heavily invested in developing AI technologies and tools globally, including in the EU. To portray AI as a competitive three-way race with a zero-sum outcome would be counterproductive and reductive of such a multi-faceted phenomenon, while feeding into the narrative that there would be AI winners and losers. BSA strongly cautions against this approach, and supports an EU that welcomes global leaders in AI development to ensure the highest standards in ethics and research.
2. **Research and Education.** BSA and its Members are strong supporters of additional efforts in the fields of education, research, infrastructure and workforce development. BSA has developed global policies to aid in these efforts, and believes that Trustworthy and Responsible AI can only be achieved through effective, inclusive and multilayered engagement with all stakeholders, from the private sector to academia, from policymakers to citizens. Ensuring that AI is well understood at all level is a fundamental factor for its development and deployment in the EU.
3. **Future-proof rules.** BSA strongly support a risk-based approach to regulatory efforts, to ensure that context and purpose of AI tools are fully taken into account when developing policies and legislation that support innovation and healthy competition. Moreover, BSA would caution against overly pervasive efforts in the space of data localization and ownership, as well as protectionist policies that would hamper EU and non-EU actors

[1] BSA | The Software Alliance (www.bsa.org)is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

from fully competing in the EU. The Digital Single Market is a fundamental pillar of the EU's economy, and AI developers will provide a significant boost to jobs, growth and research.

Following BSA's submissions to the EU High-Level Expert Group ("HLEG") on Artificial Intelligence ("AI") earlier this year, BSA would like to submit additional feedback to the HLEG in the context of its second workstream, on Policy and Investment, whose objective is to provide recommendations to the European Commission on policies and possible regulatory efforts to foster AI development in the EU.

To assist in that analysis, the first part of the attached document evaluates some of the existing and developing regulatory efforts by the EU which would already affect and be applicable to AI development and deployment in Europe. BSA also recognizes that designing specific policies and investments may be also necessary to further encourage and strengthen the uptake and development of AI in the European Union. The second part of the document provides an overview of best practices and recommendations that BSA has developed globally in its Five Key Pillars for Responsible Artificial Intelligence.

We remain at your disposal for any additional questions or comments you may have. We look forward to working with you on the development of Artificial Intelligence in the European Union.

Yours faithfully,

Thomas Boué
Director General, Policy – EMEA
BSA | The Software Alliance

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

The European Union legislation landscape on Artificial Intelligence and BSA's Best Practices and Recommendations to achieve Responsible AI in Europe

The present document provides a non-exhaustive overview on the body of law already regulating development and deployment of AI, in the hope it can assist the EU High-Level Expert Group ("HLEG") on Artificial Intelligence ("AI") in recommending to the Commission that a thorough analysis and impact assessment of each piece of legislation should be carried out, so that the EU can strike the delicate balance between fostering innovation and an harmonious body of law.

At the same time, BSA has developed a series of global principles, best practices and recommendations to encourage and support the development and deployment of Responsible AI. While some of those principles and recommendations are more pertinent to the HLEG's Ethical Guidelines, BSA would like to underline the importance of ensuring that the Policy and Investment Recommendations focus on fundamental aspects such as Sound Data Innovation Policies, Education and Workforce Development.

The recently released HLEG Ethical Guidelines were not meant to seek specific amendments to the legal or regulatory landscape, in light of AI developments. And the HLEG correctly suggested that the legislative status quo regarding regulation of AI is robust, stating that "AI systems do not operate in a lawless world. A number of legally binding rules at European, national and international level already apply or are relevant to the development and use of AI systems today" (p. 6). Complementing the Ethical Guidelines, the Policy and Investment workstream aims, in a first phase, at identifying the legal and regulatory landscape that would be applicable to AI. Then, in a second phase, it would possibly recommend regulatory action in areas where there may be gaps.

In order to contribute to the inventory being carried out by the HLEG, BSA has prepared a detailed, but not necessarily exhaustive, overview of legislation already regulating AI, underlining the risk of over-regulating and creating an overlap of rules that would significantly hamper AI in the EU.

While AI tools will be used and deployed in a variety of different fields of human activity, BSA's focus is primarily on the development of enterprise AI and its use in the business-to-business context. At the same time, it is important to highlight that the EU Treaties and the Charter of Fundamental Rights of the EU do apply to all instances of AI development and deployment in the EU. Similarly, the EU and national frameworks on Cybersecurity are equally important components of AI development and deployment, but is not addressed in this document.

In the context of Cybersecurity, BSA continues to stress the importance to promote the adoption of international standards in any Europe-based efforts. As Technical Robustness and Safety have been identified as one of the three pillars for Trustworthy AI, as well as one of the seven requirements set forth by the HLEG, the EU – and ENISA in particular – should endeavor to engage at the international level for the development of international standards in cooperation with global partners. Cybersecurity is a transnational challenge that demands international cooperative solutions; such cooperation depends upon effective, proactive diplomacy.[2]

[2] For more information about BSA's recommendations and work on an International Cybersecurity Policy Framework, please refer to bsacybersecurity.bsa.org.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

EU Legislation affecting AI Development in Europe

GPDR

The General Data Protection Regulation ("GDPR") includes provisions that impact AI development and use.[3] GDPR defines "personal data" broadly, as any information that directly or indirectly identifies or could be used to identify natural persons (Art. 4(1)). This broad definition captures much of the data used to engineer and train AI systems, as well as data used by AI systems to generate predictions and make recommendations. GDPR also applies heightened protections to certain uses of personal data, such as use of biometric data, profiling, and automated decision-making without human intervention.

As detailed below, GDPR comprehensively regulates the use of personal data throughout the lifecycle of an AI tool: from inception, to deployment, and ultimately to removal from the market. Importantly, GDPR's rules mirror many of the principles endorsed by the HLEG Guidelines. The Guidelines set out 7 requirements for "Trustworthy AI": accountability; privacy and data governance; human agency and oversight; diversity, non-discrimination and fairness; technical robustness and safety; transparency; and societal and environmental wellbeing. Virtually all of these requirements are reflected in GDPR.

Importantly, GDPR does not approach these requirements only from the perspective of protecting personal data; as the European Data Protection Board ("EDPB") has made clear, GDPR also serves the purpose of protecting other fundamental rights, including preventing discrimination and the right to human autonomy. For example:

- **Fairness.** GDPR requires that processing be "fair." Accordingly, when conceiving, designing, and using an AI solution that involves personal data, fairness is a legally mandated consideration. While GDPR does not define "fairness," regulators have made clear that it reaches widely. As the UK Information Commissioner's Office ("ICO") has explained, for example, "[i]n general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should" (emphasis ours). [4]

- **Legal basis for collection and subsequent use of personal data.** Before processing personal data (including collecting that data, using it to train algorithms, combining it with other data to obtain insights etc.), controllers must point to an appropriate legal basis under GDPR. For example, among other legal bases, controllers may rely on: (1) the consent of individuals, whom must be "informed" and able to be withdrawn; or (2) their own legitimate interests for processing the personal data, as long as these interests are not overridden by the interests or fundamental rights and freedoms of the individual (Art. 7). These steps should provide for a balance of interests during all stages of processing personal data (whether by automated means or otherwise).

- **Transparency.** Data controllers are required to ensure that all processing activities with respect to personal data are presented to data subjects in a transparent way. In addition, of

[3] Note also that as part of the data protection reform package that resulted in the GDPR, the EU introduced the Data Protection Directive for Police and Criminal Justice Authorities. This Directive governs the processing of personal data by law enforcement authorities ("LEAs") in the context of criminal offences, including where LEAs make decisions about individuals solely based on AI. Pursuant to that Directive, for example, an LEA is prohibited from using automated decision-making that produces an adverse effect on or significantly affects the individual, unless authorized by EU or Member State law, where that law provides "appropriate safeguards for the rights and freedoms of the data subject, or at least the right to obtain human intervention" (Art. 11).

[4] *See* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/.

particular relevance to AI solutions, where "automated decision-making, including profiling"[5] is deployed, individuals must be provided with "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" (Arts. 13, 14 and 15). In other words, the GDPR's transparency requirement is not limited to identifying the controller, for example, or where the data is stored; it also requires that the "logic and consequences" of AI systems be explained to data subjects. GDPR also requires intelligibility — and specifically, that information be provided in a manner that is "concise, transparent, intelligible and easily accessible" (Art. 12).

- **Data subject rights and automated decision-making.** GDPR confers a wide range of rights on individuals, such as the right to access their personal data and to ask data controllers to erase their personal data. Significantly, individuals also have the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" (Art. 22). In such cases, data subjects have the right "to obtain human intervention" and "to contest the decision" (Art. 22(3)). By requiring human intervention and enabling individuals to prevent certain decisions about them being made purely via machine-based learning, the GDPR integrates the human oversight principle into EU law in case of legal or other 'severe' decisions.

- **Assessing the impact of data processing.** When conducting processing activities that are "likely to result in high risk to the rights and freedoms of natural persons," data controllers must carry out a "data protection impact assessment" ("DPIA") (Art. 35). GDPR provides for instances where it is mandatory to conduct a DPIA. This includes where a processor engages in "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing" and on which the controller bases certain decisions that produce "legal effects" on the individual or significantly impact him/her in another way (Art. 35(3)(a)). The assumption GPDR makes is that in this specific field automated processing could bear a potential risk of discrimination or bias against individuals, and thus must be subject to higher risk assessment obligations than other forms of processing. In carrying out a DPIA, controllers must assess, among other elements, the risk to the "rights and freedoms of data subjects" (Art. 35(7)). The requirement to conduct a DPIA thus extends further than simply assessing the *privacy* impact of a processing activity on an individual; instead, GDPR requires controllers to make an assessment of the impact of the activity on fundamental rights as a whole. The Article 29 Working Party noted that a DPIA "primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion."[6]

- **Data protection by design and data protection by default.** When AI developers build their systems, they are required to consider the privacy of individuals throughout the design, construction and deployment of their technologies. In particular:

    - *Privacy by design* is one of the central tenets of GDPR (Art. 25). It requires data controllers, when determining the means and purposes of the processing of personal data and during the processing activity itself, to take account of data protection

[5] "Profiling" is defined in Art. 4(4) GDPR to mean: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

[6] *See* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 at p. 15. This opinion of the Article 29 Working Party was later endorsed by the EDPB.

principles. These principles include (but are not limited to) data minimization — i.e., ensuring that personal data is only processed where "adequate, relevant and limited to what is necessary" (Art. 5(1)(c)) — as well as lawfulness, fairness and transparency (Art. 5(1)(a)).

- *Privacy by default* requires data controllers to "implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed" (Art. 25). In other words, when assessing the amount of personal data collected, the extent of processing activities, the storage of that data, and its accessibility (either within an organization or to third parties), data controllers should always apply a strict "purpose limitation" test.

ePrivacy Regulation

Many AI applications will depend on natural language recognition, voice recognition, and an understanding of how and when people communicate. For this reason, many AI applications and tools require training datasets comprised of the content of, and data about, communications. The collection and use of such data may often therefore be also regulated by the e-Privacy regulation ("ePR").

The ePR is still undergoing legislative review. For the purposes of this analysis, therefore, the Commission's original proposed text will be used as reference. As a preliminary point, the scope of the Regulation is quite broad, as also non-personal data (e.g., machine data) would be included. Also, it appears likely to apply additional restrictions (beyond those in GDPR) on the collection and use of "electronic communications data" — a term defined broadly to include both the content of communications and metadata (e.g., when a communication was sent, and to whom) associated with that data.

In particular, the Commission proposal for the ePR would prohibit the processing of "electronic communications data" without grounds set out in the Regulation (except by end-users) (Art. 5). "Electronic communication services" (a term defined broadly, that includes many types of communications providers, including online mail, instant messaging, VoIP, and other so-called "over-the-top" or "OTT providers") and networks could process such data on limited enumerated grounds. This includes, for example, the purpose of transmission, maintaining or securing networks, or detecting errors in transmission (Art. 6(1)). Further, electronic communications services may process electronic communications metadata where necessary for limited purposes (i.e., to detect fraud), or subject to end-user consent (and subject to further conditions) (Art. 6(2)). Finally, electronic communications services may also process the content of communications, but only based on the consent of the end-user (or end-users). Electronic communication services are also under strict limits in terms of their ability to retain these data types (Art. 7).

In addition, the ePR mandates as a general rule that end-user consent be obtained where "information" would be collected from end-user devices (Art. 8), although exceptions may be available in certain cases. This requirement applies to all parties except end-users (i.e., not only to electronic communication service and network providers).

Collectively, the limitations on processing in Article 6 will directly impact the development of many AI applications. In particular, as many AI system are developed and deployed in compliance with GDPR, and in most cases process data on the basis of legitimate interest. The ePR proposals – including the amended versions of the European Parliament and of the Council of the EU – do

not provide for additional grounds for processing beyond consent, therefore would severely limit AI deployment and development in the EU. This is particularly true in the case of AI and Machine-to-Machine communications, which often may not be technically able to rely on a consent-only based model.

Liability legislation

According to the draft HLEG Guidelines, "[w]hen unjust adverse impact occurs, accessible mechanisms should be foreseen that ensure adequate redress" (Guidelines, p.50). The HLEG Guidelines acknowledge that existing EU safety legislation and liability frameworks increase AI's trustworthiness.

The EU has a long-established framework providing strong protection for consumers and – more broadly – citizens. This has led to the highest standards globally for developing and deploying new products in the EU, alongside a strong Member State enforcement regime. The current liability regime has proven in time its fitness for purpose and its ability to adapt to new technologies.

- **Product Liability Directive:**

The Commission is in the process of assessing whether existing product safety and liability regulations are fit for purpose in light of the challenges posed by AI. In mid-2019, the Commission will issue guidance on the Product Liability Directive and a report on the broader implications for, potential gaps in and orientations for, the liability and safety frameworks for artificial intelligence, the Internet of Things and robotics. This includes a planned review of the Product Liability Directive in the Commission's next term. The Product Liability Directive provides the EU regime for liability for damage caused by goods *outside* of a contract. The Directive is one of the longest-standing elements of the *consumer acquis*, and has stood the test of time to cater for a broad range of innovative products. In place for over 30 years, the Directive has, by ensuring protection for consumers for faulty products, provided a basis for consumer trust that has helped to drive demand for a huge range of digital products on the market today.

The Directive defines 'product' as "all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable" (Art. 2).

The Directive lays down a series of requirements – including that producers are strictly liable for defects (Art. 1) (the Directive provides that a product is defective if it "does not provide the safety which a person is entitled to expect, taking all circumstances into account," Art. 6); and that producers cannot limit this liability contractually (recital 7). The Directive's proven longevity, and its demonstrated ability to adapt to new products, ensure that its application is still pertinent to the ever developing Single Market.

- **Machinery Directive:**

This Directive, in force since 2009, applies to a wide range of products (listed in Art. 1), which would encompass AI-powered machines, such as autonomous robots and 3D printers. The Directive sets out a framework governing health and safety requirements for machinery (designed for consumer or industrial use) placed on the EU market. Annex I lays down "essential" health and safety requirements; the Directive (Art. 7) also provides that where machinery is manufactured in conformity with a harmonized standard, it will be presumed to comply with certain of the Directive's requirements. The Regulation leaves it to manufacturers to determine

what technical solutions to use to meet their safety obligations. This approach provides for flexibility for manufacturers, and also allows new standards to be developed as technology evolves and new risks emerge.

Because the Machinery Directive is largely technology-agnostic, it is equipped to regulate the safety of both current and emerging machinery, including, in some cases, AI-enabled machines. The general principles laid down in the Directive ensure that the rules continue to remain relevant even as technology becomes more sophisticated — *see*, for example, the principle of "safety integration," which applies to the design and construction of all machinery (Annex I).

Establishing liability requires Member States and the Commission to be proactively engaged — e.g., by assessing whether the machinery in question conforms with the relevant safety rules — and gives manufacturers the opportunity to be heard (*see* Art. 11 (the "Safeguard clause"), Art. 12, and Art. 20 on legal remedies). The liability regime also provides Member States with discretionary powers to introduce penalties for infringements (Art. 23), where appropriate.

Free Flow of Data Regulation ("FFoD Regulation")

The FFoD Regulation,[7] adopted in November 2018, aims to improve the mobility of *non*-personal, electronic data to achieve "data-driven growth and innovation" across the EU digital single market (recital 13). The Regulation introduces (among other requirements) the following rules:

- **Prohibition on data localization.** The FFoD Regulation prohibits Member States from adopting or maintaining localization requirements over non-personal data — that is, rules *requiring* data to be processed in a specific Member State or *preventing* the processing of data in another Member State. The Regulation includes an exception where a requirement can be justified on public security grounds (Art. 4); and

- **Expanding porting of data.** The FFoD Regulation also requires the Commission to encourage stakeholders to develop self-regulatory codes of conduct that facilitate the "porting" of data, enabling organizations to move data between cloud service providers and/or back to in-house servers. To facilitate porting, data must be provided "in a structured, commonly used and machine-readable format including open standard formats" (Art. 6).

The FFoD Regulation complements the GDPR, which provides for free flow of *personal* data in the Union. By minimizing the barriers to the movement of data across the Member States, the FFoD (and GDPR) will facilitate sharing and use of such data for AI innovation and research across the EU. The FFoD Regulation also enables those developing and using AI solutions to move their data between providers, allowing them to choose providers who offer services that best match their needs. This, in turn, ensures that the EU remains a competitive environment for commercial and non-commercial development of AI solutions.

Public Sector Information Directive (Recast) ("Recast PSI Directive")

While the FFoD Regulation focuses on data mobility, the Recast PSI Directive, adopted in January 2019, aims to improve access to public sector data. More specifically, the Recast Directive seeks to facilitate the re-use of public sector data by third parties, including private entities acting for commercial (or non-commercial) purposes. Similar to the FFoD Regulation, the

[7] Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN.

PSI Directive will foster AI development in the EU, ensuring that important datasets held by public entities are shared with the public.

The Directive promotes wider access to public sector information by:

- **Expanding the scope of the law:** the Recast PSI Directive extends, subject to certain conditions, the re-use obligations to documents[8] generated by "public undertakings" (in addition to "public sector bodies") — that is, entities in various utility sectors, such as water, energy and transport, public transportation providers, public air carriers and ship-owners (Art. 1(1)(b)).
- **Bringing new data types within scope of re-use obligations:** The Recast PSI Directive includes the following data types within the scope of the law, which should increase access to and reuse of valuable data: "dynamic data," (documents in an electronic form, subject to frequent or real-time updates," such as traffic, satellite and weather data); "research data," (digital documents collected or produced in the course of scientific research activities); "high value datasets," (documents held by public sector bodies and public undertakings the re-use of which is associated with important socio-economic benefits. [9]

Facilitating access to public sector data is essential for the development and functionality of AI systems and tools. The more high quality data that feeds into AI systems, the more sophisticated the output over the long-term. This not only benefits developers of AI, but also has an impact on various industries and the public at large, who increasingly rely on meaningful and useful information that is mined and analyzed from large datasets — including data generated by the public sector.

Directive on Copyright in the Digital Single Market

Copyright rules have a significant impact on development and deployment of AI. Text and Data Mining ("TDM"), in particular, is a fundamental process for AI. TDM is a form of software-enabled analytics that unlocks correlations and identifies useful knowledge from information that rests undiscovered in various datasets, large and small. Humans can process and harness the results of TDM for a myriad of valuable purposes and across different industries and sectors.[10] TDM also entails a process of verification — that is, referring back to the underlying information in order to verify the results of TDM, helping to ensure its accuracy and consistency. The HLEG Guidelines consider data accuracy, reliability and reproducibility as fundamental elements of one of the seven requirements: Technical robustness and safety.

The European Commission published its proposal for a Directive for Copyright in the Digital Single Market in September 2016 ("DSM Copyright Directive"),[11] where it moved to establish a narrow exception to copyright covering TDM activities. The exception would have *exclusively* applied to scientific research organizations acting on a non-profit basis. Leaving aside

[8] "Documents" refers to any content in any medium whatsoever (i.e., including electronic form) or any part of such content (Art. 2(5) Recast PSI Directive).
[9] To ensure stakeholder involvement when the Commission adopts delegated acts to identify the list of high value datasets and define the framework for their publication and re-use, the European Parliament has proposed an amendment to the Directive requiring the Commission to carry out public consultations with all interested parties, including re-users of public sector data, before adopting delegated acts.
[10] As analytic methods continue to evolve rapidly, TDM is now used by organizations of all sizes and in every sector of the economy to analyze enormous volumes of data, in line with EU data protection rules, and generate insights that would have been unimaginable just 10 years ago.
[11] Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market, 2016/0280 (COD)

considerations as to whether or not TDM should be a copyright-related process at all,[12] the Commission's proposal would have created significant uncertainty throughout the EU. A narrow exception for TDM would have moved in the opposite direction of global trends. Japan, the United States, Canada, and Singapore extend, or are in the process of extending, legal protections for both commercial and non-commercial TDM.

The Commission's proposed DSM Copyright Directive predated its 2018 Communication on Artificial Intelligence for Europe ("AI Strategy")[13] and the subsequent Communication on a Coordinated Action Plan on Artificial Intelligence ("AI Action Plan")[14]. In particular, the AI Strategy seeks to ensure that all sectors, private and public, benefit from AI:

"*Europe can only reap the full benefits of AI if it is available and accessible to all. The Commission will* ***facilitate access of all potential users, especially small and medium-sized enterprises, companies from non-tech sectors and public administrations, to the latest technologies and encourage them to test AI***."[15]

The Commission also acknowledged in the AI Strategy the importance of TDM as part of the successful development of AI, including TDM's ability to "read" large datasets to extract knowledge. The Commission considers TDM to play a vital role in the modernization of EU copyright rules (AI Strategy at p. 11). The AI Strategy objectives are laudable and ambitious, and a narrow exception for TDM in the proposed new DSM Copyright Directive would have significantly limited AI development in the EU. During the Trilogue negotiations on the Copyright Directive, the Commission changed its approach to TDM and supported a broader mandatory exception to be enacted by all Member States. The final result of the negotiations was to confirm such an exception. The Directive was approved by Member States and the European Parliament in 2019. Enacting a broad mandatory TDM exception at the national level would strengthen the EU's position as a global leader in AI development, modernizing the Digital Single Market and aiming to satisfy its AI private sector investment objectives for the 2018-2020 period and beyond.[16]

Cross border data transfers in Trade Agreements

In 2018, the European Commission published a proposal setting out text on cross-border data transfers ("Cross-Border Data Proposal") intended for inclusion in future EU trade and investment agreements with third countries.[17] Similar to the FFoD Regulation discussed above, the Cross-Border Data Proposal seeks to remove barriers to the transfer of data across borders and prohibit data localization, except that this Proposal aims to remove such barriers with regard to transfers

[12] Copyright protection is intended to protect an author's interest in expressive output. While copyright protects the specific expression of factual information, it does not extend to the facts themselves. Because the purpose of TDM is to unlock unprotected factual information, the incidental copies made during the TDM process do not conflict with nor unreasonably prejudice the legitimate interests of copyright holders.

[13] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, COM(2018)237. Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625 (PDF).

[14] Communication from the Commission to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions on a Coordinated Plan on Artificial Intelligence, COM(2018)795. Available at: https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-795-F1-EN-MAIN-PART-1.PDF.

[15] *Ibid*., 3

[16] *Ibid.,* 3 "*To support joint efforts,* ***the Commission is increasing investments in AI*** *under the research and innovation framework programme Horizon 2020 to around* ***EUR 1.5 billion by the end of 2020*** *[…]* ***If Member States and the private sector*** *(beyond established partnerships)* ***make similar investment efforts, the total investments in the EU*** *will grow to around EUR 7 billion per year, totalling* ***more than EUR 20 billion by the end of 2020***."

[17] *See* European Commission, *EU Proposal for provisions on cross-border data flows and protection of personal data and privacy*, available at http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf.

with third countries, rather than within the EU. As with the FFoD Regulation, ensuring that data can be transferred freely across borders is vital to the EU's AI leadership, given the critical role that access to large datasets plays in both the development and deployment of AI. This proposal is important to allow EU companies to "import" data from third countries so they can offer their services directly within the EU.

Article 1 of the Cross-Border Data Proposal states that the parties to any trade agreement incorporating this text "are committed to ensuring cross-border data flows to facilitate trade in the digital economy." It then lists four types of measures that the Parties agree "shall not . . . restrict[]" cross-border data transfers, which align to a significant extent with the provisions set out in the FFoD Regulation:

1. Requiring the use of computing facilities or "network elements" within a Party's territory, including by requiring that such facilities or elements are locally certified or approved;
2. Requiring the localization of data in a Party's territory for storage or processing;
3. Prohibiting storage or processing of data in the territory of the other Party; or
4. Making cross-border data transfers conditional on the use of computing facilities or network elements, or on other localization requirements, in the Parties' territory.

Article 1 represents the first time that the EU has endorsed binding trade commitments specifically focused on cross-border data transfers. Also, when countries today seek to impose limits on cross-border data transfers, they often do so through one or more of the measures listed in Article 1. Thus, commitments from the EU's trading partners not to adopt or maintain such measures could be useful, including in helping the EU achieve its AI ambitions.

Article 2 of the proposal, however, introduces an exception that risks undermining these commitments. It states that each Party may adopt and maintain whatever safeguards "*it deems appropriate* to ensure the protection of personal data and privacy," including through "rules for the cross-border transfer of personal data." (emphasis added).[18] It adds that "nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards."

This text could allow the EU's trading partners to adopt measures on privacy or data protection grounds that severely restrict cross-border data transfers, even if these measures are far more restrictive than the rules on third-country data transfers set out in the GDPR. Furthermore, the fact that each party can adopt whatever measure "it deems appropriate" suggests that these measures could not be challenged under the agreement, even if they had protectionist, trade-inhibiting effects. For instance, an EU trading partner could impose strict data localization mandates on data that was essential for the development of AI, while benefitting from the EU's relatively more liberal rules (as set out in the GDPR) for such transfers. Indeed, the proposal could have the unintended consequence of encouraging additional data localization requirements and greater protectionism, through the pretense of advancing data protection.

As the HLEG considers possible changes to EU law impacting AI development, it should consider recommending revisions to the Cross-Border Data Transfer Proposal that would significantly narrow the scope of Article 2. This would help ensure that people and enterprises across the EU can reap the full benefits of trade in AI and that EU companies operate on a level playing field with their foreign counterparts with regard to their access to and use of AI and data.

[18] Paragraph 3 of Article 2 defines "personal data," consistent with the GDPR, to mean "any information relating to an identified or identifiable natural person."

Best practices and recommendations: Five Key Pillars for Responsible Artificial Intelligence

Software innovation is fostering the development of a range of cutting-edge technologies, such as artificial intelligence (AI), that offer great promise to improve lives and help solve intractable problems. AI solutions are already leading to improvements in healthcare, advances in education, more robust accessibility tools, stronger cybersecurity, and increased business productivity and competitiveness, impacting every sector.

AI also has the potential to generate substantial economic growth and enable governments to provide better and more responsive government services while addressing some of the most pressing societal challenges.

A flexible policy framework is necessary to enable successful deployment of AI products and services. BSA has identified five key pillars for facilitating responsible AI innovation.[19]

1) Building Confidence and Trust in AI Systems
2) Sound Data Innovation Policy
3) Cybersecurity and Privacy Protection
4) Research and Development
5) Workforce Development

The holistic approach taken by BSA makes it so that certain aspects of our Five Key Pillars are better suited to address the concerns raised by the HLEG Guidelines, and we were delighted to participate to the public consultation for the Guidelines at the beginning of 2019, with a comprehensive submission highlighting the many common principles and recommendations put forward by BSA and the HLEG. The final version of the Guidelines and the BSA recommendations in the context of Trustworthy and Responsible AI largely overlap, and provide an excellent framework for the ethical development of AI.

With regards to additional suggestions in the context of Policy and Investment Recommendations for AI in the European Union, BSA would like to draw the attention of the HLEG to two key aspects: Sound Data Innovation Policy and Workforce Development.

Sound Data Innovation Policy

At its core, AI is a technology that augments human intelligence, helping people make better informed decisions by identifying relationships, patterns, and trends in data that would be imperceptible to humans. Although AI research dates back several decades, advances in the availability of computing power, highly sophisticated algorithms, and data have recently accelerated its use in the marketplace.

AI systems are "trained" by ingesting enormous volumes of data. The benefits of AI are therefore dependent on the quantity and quality of data that is available for training. As a result, government policies affecting the ability to access and share data have a significant influence on the development of AI.

[19] For more information please visit ai.bsa.org.

In particular, BSA recommends:

- **Ensure Data Can Move Freely Across Borders**: the Free Flow of Data Regulation (please see above) is a fundamental stepping stone in this endeavor. At the same time, the current language for Cross Border Data Flows in Trade Agreement may lead to detrimental effects for data flows. Similarly, data flows with critical international partners of the EU need to be safeguarded, in particular the EU-U.S. Privacy Shield framework.
- **Access to Government Data and Public Sector Information**: as mentioned above, the Recast PSI Directive is an excellent legislative initiative, and BSA commends the Commission for its quick adoption and meaningful stakeholder engagement.
- **Facilitate Value-Added Data Services**: Governments should pursue policies that facilitate the business-to-business exchange of data and boost the development of AI services, including by:
    - Ensuring companies can enter enforceable contracts that create data sharing arrangements; and
    - Avoiding the creation of new rights in business data that could add unnecessary transaction costs.

Workforce Development

Although changes are taking place, using software to create solutions to enrich every aspect of our lives presents great opportunity. Software innovation is transforming every sector of the American economy. A recent Software.org: the BSA Foundation study shows the software industry contributed more than €1 trillion to the EU GDP in 2016 — a $90 billion increase in just the last two years. The study also showed that the software industry is a powerful job creator, supporting more than 12 million jobs through direct, indirect, and induced contributions, with significant effect in each of the EU Member States. And there are many more jobs available than there are people qualified to fill them.

Both the government and the private sector have important roles in implementing policies that will prepare the next generation for the jobs of the future and allow the current workforce to transition successfully into the new job environment. In particular, the EU and its Member States should:

- **Improve Access to STEM Education**: STEM education equips students with problem solving, critical thinking, and other abilities that are important for jobs in virtually every industry. Making STEM education inclusive and widely available builds interest in developing in-demand skills and expands the available workforce for technology-related jobs.
- **Expand Workforce Retraining**: Emerging technologies will create new jobs and change the skills demanded in many existing jobs. In addition to preparing the next generation workforce, we must ensure the current workforce has access to the skills needed as the job market evolves.
- **Create Alternative Pathways to the Evolving Workforce**: As our economy changes, we need to consider whether our education model should change as well. In the new economy, technical schools, apprenticeships, boot camps, and other alternative pathways may be just as effective as traditional classrooms in generating the skills and interests necessary to thrive in 21st century careers.