Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 124

AI Risk Management in Tax Audits: A Comparative Review of the EU and US Regulatory Approaches

Amedeo Rizzo & Giorgio Hassan

2024

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Authors

Amedeo Rizzo is a Doctor of Philosophy (DPhil) in Law at the University of Oxford, Exeter College, and Academic Tutor at St Catherine's College (Oxford) in the UK. He works as an Academic Fellow at Bocconi University and SDA Bocconi School of Management (Italy), where he coordinates the Master of Corporate Tax Law and several research centers, including the Accounting & Tax Policy Observatory (OFC) and the Transfer Pricing Forum, and the Tax Strategies Project. He is a Visiting Scholar of law and technology at the Singapore Management University, Yong Pung How School of Law.
Professionally, he is the Chairman of Lyra Analytics, a data analytics company, the Executive Director of the Innovation Policy Network, and one of the founding partners of the Italian audit company, Imperium Audit.
Prior to his D.Phil. in Law at the University of Oxford, Amedeo obtained an M.Sc. in Taxation from the University of Oxford (distinction), an M.Sc. in Business Administration and Law (summa cum laude) and a B.Sc. in Business Administration, both from Bocconi University.

Giorgio Hassan is a Research Assistant at the Accounting & Tax Policy Observatory (OFC) at SDA Bocconi School of Management, where he carries out research in tax law, tax policy, and law and technology. He is also Editor in Chief of the journal Bocconi Legal Papers.
Professionally, he is the Coordinator at the Tech Regulation Hub of the Innovation Policy Network. He has previously worked in the Tax Consulting Team of BonelliErede in Milan, Italy.

General Note about the Content

Suggested Citation

This TTLF Working Paper should be cited as:
Amedeo Rizzo & Giorgio Hassan, AI Risk Management in Tax Audits: A Comparative Review of the EU and US Regulatory Approaches, Stanford-Vienna TTLF Working Paper No. 124, http://ttlf.stanford.edu.

Copyright

Abstract

This paper focuses on the AI risk management framework that applies to tax authorities under the EU and US legal systems. In recent years, the development of AI has entered the field of tax administration, revolutionizing the planning and operational tasks of tax authorities. In this scenario, it is crucial that taxpayers are not unduly exposed to any risk of harm arising from the unsafe implementation of AI by tax authorities. In this regard, the EU legal framework – with the GDPR and the recent AI Act – and the US legal framework – with the recent Executive Order on the development of Safe, Secure, and Trustworthy AI – provide valuable sources of risk-based obligations that could adequately address the risks of AI in the tax domain.

On the EU side, the GDPR and AI Act have a complementary approach – a "rights-based approach" in the case of the GDPR, and a "risk-based approach" in the case of the AI Act – and an overlapping scope of application. In the field of AI risk management, the potential overlap between the GDPR and the AI Act may provide valuable indications for adapting the GDPR-based risk management framework to the realm of AI, and, at the same time, for interpreting the scope of the AI Act in light of the rights provided under the GDPR. On the US side, the risk management obligations stemming from the Executive Order on Safe AI draw from the recent developments in AI regulation in the EU, providing measures that have a similar scope to the requirements of the AI Act. From this perspective, we discuss that the EU and US approaches to AI regulation are slowly aligning and are similarly able to address the risks arising from the use of AI in the tax domain – such as, particularly, the risks concerning AI-enabled discrimination and human-AI interaction. However, both in the EU and the US, it is unclear whether the risk management framework provided by these regulations can effectively extend to tax authorities. Except for the GDPR, the AI Act and the Executive Order seem to consider tax-related AI systems at a lower risk class compared to other categories of "high-risk" or "risk-impacting" AI systems. The misalignment in the classification of tax-related AI systems could jeopardize the application of the AI risk management framework provided in these regulations, and consequently, expose taxpayers to significant risks of harm.

For this reason, we argue that the risks concerning the use of AI in tax administration, and the benefits that could derive from the adoption of a risk management framework inspired by these three regulations, should convince EU and US lawmakers to adopt a precautionary and uniform approach to the risk categorization of tax-related AI systems. Particularly, lawmakers should locate tax-related AI systems among the pool of high-risk and rights-impacting systems for the purposes of the AI Act and the Executive Order, for the better interest of taxpayers in the EU and the US.

Keywords

Risk Management, Artificial Intelligence, Tax Audits, Tax Controls

Table of Contents

1. Introduction

The implementation of artificial intelligence (AI)[1] in the field of tax administration is revolutionizing the structure of tax audits worldwide. Tax authorities have now increased their reliance on AI systems for performing fundamental tasks in the areas of taxpayer assistance, internal case management, and large-scale tax controls.

The progressive digitalization of tax administration was first addressed by the OECD, in 2016.[2] With its paper, the OECD highlighted the key opportunities and challenges in establishing, operating, or improving advanced analytics functions in tax administrations, laying the groundwork for the progressive digitalization of tax systems in this decade. The OECD approach focused on applying statistical and machine learning techniques to uncover insights from data, and ultimately to make better decisions about how to deploy resources to the best possible effect.[3]

To this end, the OECD advised tax authorities to implement predictive and prescriptive analytics to better understand what actions should be taken for any chosen group of taxpayers.[4] The application of advanced analytics in tax administration would have covered a number of areas, including audit case selection, filing & payment compliance, debt management, taxpayer assistance, and cluster analysis.

Several countries have followed the suggestions of the OECD and have now implemented AI technologies to carry out multiple administrative activities. In Europe, it was reported that tax authorities are testing or have implemented AI applications in the areas summarized in Table 1.

---

[1] The High-Level Expert Group on Artificial Intelligence (AI HLEG) of the European Commission defines AI systems as: "systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals." High-Level Expert Group on Artificial Intelligence (2019), *A definition of AI: Main capabilities and scientific disciplines*. European Commission, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341 [accessed 15 September 2024].

[2] OECD (2024). Technologies for Better Tax Administration. [online] Available at: https://www.oecd.org/en/publications/technologies-for-better-tax-administration_9789264256439-en.html [Accessed 15 Sep. 2024].

[3] *Id*.

[4] *Id*.

Table 1. Definitions of AI applications of AI used by tax administrations in the EU.

Nudging	Algorithms to adapt the language of standard communication of taxpayers based on an analysis of individual taxpayer data.
Taxpayer assistance	Virtual conversational assistants used to assist taxable persons by providing automated guidance.
Real-time risk detection	Tools that identify suspicious transactions and flag those for potential further audits. They usually analyze tax returns to identify under-reported income.
AI web-scraping	Algorithms to automatically collect taxpayer data from freely accessible sources or e-commerce and e-sharing platforms, e.g. Amazon, Airbnb, and eBay.
Social Network Analysis (SNA)	Algorithms that visually represent a network of individual taxpayers using graph theory, representing a network of taxpayers as a combination of nodes for individuals or points of interest.
External Risk-management systems (risk-scoring)	Tools that create risk profiles to segment individual taxpayers into categories of risks and operate a centralized selection of taxpayers to be audited. They assess fiscal risks of tax processes carried out and segment individual taxpayers into categories of risks to subsequently prioritize the taxpayers to be selected for audits.
Automated calculation/verification of tax information	Algorithms that automatically calculate and/or verify prices of real estate without any individual manual inputs from tax officials.
Automated verification of tax returns	Tools that automatically process tax returns to conduct, correct, withdraw, revoke, cancel, or amend tax returns and credits of withheld taxes and prepayments.

Source: AI Taxadmin.EU – University of Antwerp*:* *https://www.uantwerpen.be/en/projects/aitax/*

In the US, the Biden Administration has consistently emphasized the importance of expanding the use of AI in tax controls to tackle tax abuses by multinational companies and high-net-worth individuals.[5]

Supported by a new analysis of the prospective revenues that would derive from the development of AI in tax auditing,[6] the US Internal Revenue Service (IRS) has now implemented a new strategic plan aimed at investing part of the resources derived from the Inflation Reduction Act into the implementation of AI in tax audits.[7]

[5] In this regard, a recent study found that an additional $1 spent auditing taxpayers above the 90th income percentile yields more than $12 in revenue, while audits of below-median income taxpayers yield $5, while for the sc. "marginal audits" the revenue per $1 rises to $2.99in the 90-99th percentile, $4.35 in the 99-99.9th percentile and $8.63 in the top 0.1% Furthermore, the study found that on average, taxpayers pay more in taxes for at least 10 years following an audit, and the subsequent revenue generated is three times greater than the quantity collected during the initial audit. See William C. Boning et *al*. (2023), 'A Welfare Analysis of Tax Audits Across the Income Distribution', *NBER Working Paper No. 31376*, available at https://www.nber.org/papers/w31376 [accessed 15 September 2024].

[6] IRS, *Return on Investment: Re-Examining Revenue Estimates for IRS Funding* (February 2024), available at https://www.irs.gov/pub/irs-pdf/p5901.pdf [accessed 15 September 2024].

[7] IRS*, Internal Revenue Service Inflation Reduction Act Strategic Operating Plan FY2023 – 2031* (5 April 2023), available at *https://www.irs.gov/pub/irs-pdf/p3744.pdf [accessed 15 September 2024].*

Pursuing this trend, the OECD has recently designed a new model for tax administration – "Tax Administration 3.0" – that calls for new strategies to integrate administrative processes with the digital systems that taxpayers use in their daily lives, in order to enhance compliance and minimize the burdens of existing tax systems.[8]

Among the various areas of application for AI, a major focus should be placed on the use of advanced technologies to predict cases of evasion and tax avoidance. The increasing reliance on tax scoring algorithms to carry out audit decision-making processes could progressively outweigh the role of human intervention in tax proceedings, exposing taxpayers to a wide range of risks. From this perspective, the implementation of AI in tax audits requires the adoption of appropriate risk management measures by tax authorities to prevent the risks connected with the progressive automation of tax proceedings.[9]

In this paper, we focus on the risk management provisions that apply to Tax Authorities in the EU and the US, comparing their approach to AI regulation and suggesting specific policy measures to better target the risks associated with the use of AI in tax.

In our view, drawing a comparison between the EU and the US is worth doing for several reasons. Primarily, the EU and the US have deployed a shared effort for implementing common regulations in the field of AI risk management,[10] making it worth addressing the main similarities and differences that they have adopted so far. Secondly, both the EU and the US are taking significant steps in implementing AI in various fields of public administration, including tax administration, in

[8] OECD (2020), *Tax Administration 3.0: The Digital Transformation of Tax Administration*, OECD Publishing, Paris, https://doi.org/10.1787/ca274cc5-en. [accessed 15 September 2024].
[9] See *infra*, section 2.
[10] To this end, the US-EU Trade and Technology Council ("TTC") has implemented a joined roadmap on the Evaluation and Management Tools for Trustworthy AI and Risk management (available online at https://digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management [accessed 15 September 2024]), which aims to advance shared terminologies and taxonomies and inform the EU and US approaches to AI risk management and trustworthy AI. On the sixth meeting of the TCC, the Council published a joined statement reaffirming it commitment to a "*risk-based approach to artificial intelligence (AI) and to advancing safe, secure, and trustworthy AI technologies*". See EU Commission Press Corner, *Joint Statement EU-US Trade and Technology Council of 4-5 April 2024 in Leuven, Belgium* (5 April 2024), available at https://ec.europa.eu/commission/presscorner/detail/en/statement_24_1828 [accessed 15 September 2024].

accordance with the indications of the OECD. Accordingly, the nature and scope of the risk management measures undertaken by the EU and the US have great significance from a perspective of taxpayer protection, as the scope of the risk management framework adopted by tax authorities can positively or negatively affect the exposure of taxpayers to the risks of AI.

2. The Risks of AI in Public Administration

In both the private and public sectors, the use of AI systems to perform decision-making processes underlines a variety of risks. Recently, the Massachusetts Institute of Technology (MIT) has performed a survey collecting the risks relating to the use of AI based on the analysis of 43 risk management frameworks and several academic studies.[11] The MIT found that the use of AI systems can expose to approximately 700 different risks, which have been classified into the following domains: discrimination and toxicity;[12] privacy and security;[13] misinformation; malicious use;[14] human-computer interaction;[15] socio-economic and environmental harms; safety, failures, and limitations of AI systems.[16]

In the field of tax controls, the risks associated with AI might concern several of the above domains, including discrimination, data security, human/AI interaction, and lack of transparency in automated decision-making processes.

[11] MIT Future Tech, *The AI Risk Repository: A Comprehensive Meta-Review, Database, and Taxonomy of Risks From Artificial Intelligence*, published online (2024), available at https://airisk.mit.edu/ [accessed 15 September 2024].
[12] This domain includes risks such as unfair discrimination and misrepresentation, exposure to toxic content, or unequal performance across groups of individuals. *Id*., p. 31.
[13] Including the risks that arise when an AI system is vulnerable or compromised by unauthorized third parties. *Id*., p. 31.
[14] Such as in the case when an AI system is used to perform cyberattacks, weapon development or use, mass harm, fraud, scams, and targeted manipulation. *Id*., p. 31.
[15] Including the risks that arise when humans develop inappropriate relationships or expectations with AI systems, or simply delegate key decisions to AI systems. *Id*. p. 31.
[16] Which include, for our purposes, the risks that lie within the use of AI systems that lack capacity, robustness, transparency or interpretability. *Id*. p. 31.

Particularly, the risk of "human overreliance" on the outcome of AI systems is one of the most impactful risks affecting the use of AI in public administration, due to the lack of training and individual responsibility of the public officers that interact with AI systems[17]. In turn, a higher amount of reliance on the outcome of AI systems would transfer to an insufficient degree of human oversight, increasing the risk of bias and opacity in the functioning of AI systems. Accordingly, the risks connected to the interaction between humans and AI are intrinsically related to the risks concerning the rights of taxpayers, such as the right not to be discriminated against or the right to receive an explanation of the outcome of a decision.

Furthermore, the collection of large amounts of personal data by tax authorities could trigger significant risk in terms of data vulnerability. This risk might appear in two different forms: on the one hand, AI systems might memorize or infer personal data about individuals, potentially altering the outcome of the decision-making process;[18] on the other hand, the data held by tax authorities could be illegally accessed, shared, or leaked to the public, potentially raising distrust and discontent among the public.[19]

For all the above reasons, the use of AI in tax controls requires appropriate measures to prevent any possible risk of harm. Both in the EU and the US, lawmakers have engaged in several regulatory efforts to mitigate the risks associated with AI by public bodies, by imposing multiple risk-based obligations on state entities that have implemented or are planning to implement advanced technologies in public administration.

---

[17] See Saar A.B. and Busuioc M. (2023), 'Human–AI Interactions in Public Sector Decision Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice' 33 Journal of Public Administration Research and Theory, p. 153.

[18] In several studies it was found that AI models – especially large-language models ("LLM") – tend to memorize personal features about individuals that they had been trained with and retrieve such information at the stage of implementation. See CNIL, *AI: ensuring GDPR compliance* (21 September 2022), available at https://www.cnil.fr/en/ai-ensuring-gdpr-compliance [accessed 15 September 2024].

[19] In the US, for instance, an authorized contractor has unlawfully entered the databases of the IRS and disclosed data pertaining to hundreds of thousand US taxpayers. See IRS, *IRS communication on data disclosure* (10 March 2024), available at https://www.irs.gov/newsroom/irs-communication-on-data-disclosure [accessed 15 September 2024].

In the next sections, we examine the risk management framework that applies to European and US tax authorities in the field of AI. First, we focus on the risk-based obligations that apply to EU tax authorities under the General Data Protection Regulation (GDPR) and the recent AI Act. Secondly, we address the evolving framework of AI regulation in the US, focusing on the obligations imposed on the IRS under the new Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (EO).

Building on this analysis, we then compare the risk management obligations in the EU and the US, by focusing on how the provisions of the GDPR, AI Act, and EO address the overall risks concerning the use of AI in the tax domain.

3. The EU Perspective: AI Risk Management under the GDPR and the AI Act

3.1. AI risk management under the GDPR

In principle, the GDPR applies to the processing of personal data by automated means and the processing of personal data that form part – or are intended to form part – of a filing system.[20] The obligations set by the GDPR fall upon the data controller –*i.e.* the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data – or upon the data processor, that is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[21]

Art. 5 GDPR lays down the principles of data processing,[22] by primarily stating that processing should comply with the principles of fairness and transparency.[23] Furthermore, the personal data that form

[20] Art. 1 GDPR.
[21] Art. 3(7)(8) GDPR.
[22] Article 6 of the Data Protection Directive 95/46—and in Article 5 of the Convention 108.
[23] According to Recital 39, GDPR, the principle of transparency requires that any information and communication relating to the processing of personal data be easily accessible and provided in plain and easily understandable language.

the object of processing should be: (i) adequate, relevant, and limited to what is necessary for the purposes for which they are processed (Art. 5(1)(c) ["*purpose limitation*"]);[24] (ii) accurate and, where necessary, kept up to date (Art. 5(1)(d) ["*accuracy*"]); (iii) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (Art. 5(1)(e) ["*storage limitation*"]; and (iv) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage (Art. 5(1) (f) ["*integrity and confidentiality*"]).

Under Art. 6 GDPR, the processing of personal data shall be lawful only if and to the extent that it is based on the consent of the data subject or other legitimate basis, such as when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.[25]

a) Risk-based obligations

Under the GDPR, the adoption of a risk management framework is necessary to ensure compliance and accountability.[26] [27]

[24] In this regard, Art. 6(4)(d) GDPR provides that in considering the compatibility of a new purpose, the controller must take into account, among other factors, the possible consequences of the intended further processing of data subjects. However, this assessment is not required when the data subject has consented to the processing of the personal data, or when the processing is performed in accordance with Union or Member State law.
[25] Art. 6(1)(e) GDPR.
[26] Consistently with Art. 5(2) GDPR, which provides that the controller shall be responsible for, and be able to demonstrate compliance with, the principles set under Art. 5(1) ("*accountability*").
[27] The scope of the risk-based approach of the GDPR was clarified by the WP29 under a statement on the role of a risk-based approach in data protection legal frameworks. In its statement, the WP29 clarified that the rights granted to the data subject and the principles found in Art. 5 GDPR should be respected regardless of the level of the risks that the latter incur through the data processing involved. Accordingly, the risk-based approach of the GDPR is not alternative, but rather complementary, to its right-based approach, as it provides specific requirements and obligations aimed at fulfilling the principles and the individual rights provided by the GDPR. See Article 29 Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks* (30 May 2014), available at https://www.huntonak.com/privacy-and-information-security-law/assets/htmldocuments/uploads/sites/18/2014/06/wp218_en.pdf [accessed 15 September 2024].

The risk-based obligations are set out in Chapter 4 and are aimed at ensuring compliance with the GDPR in every stage of data processing, in accordance with the principles of data protection by design and data protection by default, provided by Art. 25 GDPR.[28]

To this end, Art. 24 GDPR, in conjunction with Recital 78, requires the controllers and processors to implement appropriate technical and organizational measures to fulfill their data protection obligations. More precisely, Art. 24 GDPR requires the controller[29] to implement measures appropriate to the nature, scope, context, and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.[30]

Art. 32 GDPR utilizes the same wording to address the matter of data security, by requiring both the controller and processor to ensure a level of security appropriate to the risks associated with the processing of personal data. [31] Furthermore, under Art. 33 and 34 GDPR, the controllers to notify individuals and Data Protection Authorities (DPAs) of a data breach in cases where such a breach "is likely to result in a high risk to [their] rights and freedoms".[32]

In addition, the GDPR encompasses specific obligations that are triggered only in cases of high-risk processing. First, when data processing is performed by public authorities, or when (if performed by private parties) the processing applies on a large scale of data subjects or targets specific categories of personal data, the controllers and processors shall designate a data protection officer (DPO) to

---

[28] With regard to the principles of privacy by design and by default, see the guidelines from the Spanish Data Protection Agency: AEPD, *A Guide to Privacy by Design* (October 2019), available at https://www.aepd.es/guides/guide-to-privacy-by-design.pdf [accessed 15 September 2024], and AEPD, *Guidelines for Data Protection by Default* (October 2020), available at https://www.aepd.es/guides/guidelines-for-data-protection-by-default.pdf [accessed 15 September 2024].

[29] To ensure accountability in relation to these obligations, the GDPR calls for a clear allocation of responsibilities between controllers and processors, by distinguishing the cases where data processing is subject to "joint control" from the cases where the processing is performed by a third party (*i.e.,* the processor) on behalf of a controller. See Recital 79 GDPR.

[30]. Articles 24 and 25(1) are "*meta-obligations",* in the sense that *"they regulate how controllers should interpret and apply other norms in the GDPR*". Quelle, C. (2018), 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach', 9(3) *European Journal of Risk and Regulation*, p. 506.

[31] See CNIL, *Practice guide for the security of personal data* (26 March 2024), available at https://www.cnil.fr/en/practice-guide-security-personal-data-2024-edition [accessed 15 September 2024].

[32] See EDPB, *Guidelines 1/2021 on Examples regarding Data Breach Notification* (14 December 2021), Available at https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en [accessed 15 September 2024].

perform the tasks set out in Art. 39. Second, Article 35(1) provides that controllers have the obligation to conduct a Data Protection Impact Assessment (DPIA) for types of processing that are likely to result in a high risk to the rights and freedoms of individuals, taking into account the nature, scope, context, and purposes of the processing.[33]

b) Right-based obligations

The risk management framework required by the GDPR is also influenced by the applications of the rights provided under Chapter 2 to the subjects of data processing and automated decision-making.

Primarily, Art. 13, 14, and 15 GPDR require the controllers to provide the data subjects with a set of clear and understandable information concerning the processing of their personal data. To this end, the data subjects should be informed, *inter alia*, on[34] the existence, scope, and purpose of the processing; on the period for which the personal data will be stored, or at least the criteria used to determine that period; and finally, on the existence of the right to request from the controller access to and rectification or erasure of personal data. Further transparency obligations are required to inform the data subject of the legal basis for processing, the transfer of data to third parties or third countries, the existence of automated decision-making, and the right to object to the collection of personal data and/or lodge a complaint to the supervisory authority.

The transparency obligations set out under these articles ensure that data processing complies with the principles of the GDPR, and respectively, with the principles of fairness, transparency, purpose limitation, storage limitation, and data accuracy. Furthermore, these obligations stem from the general obligation provided by Art. 12 GDPR, which uptakes the principle of transparency in the provision of information and communications to data subjects.

[33] On the scope of the DPIA, see *infra*, section 3.3.

[34] Data controllers can waive this obligation in several cases, among which when the provision of such information proves impossible or would involve a disproportionate effort, especially when processing is performed in the public interest. In these cases, the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests (Art. 14(5)(d) GDPR).

In certain circumstances, data subjects have the right to ask for the rectification and erasure of their personal data or request for a restriction of processing. [35] In particular, data subjects may exercise their right to erasure when the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, when they revoke consent or object to the lawfulness of processing, or when the processing otherwise violates the provisions of the GPDR.[36]

Furthermore, the GDPR encompasses a set of rights to the addressees of automated decision-making. To this end, Art. 22 GDPR provides that "*the data subject shall 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*."[37] However, the right not to be subject to solely automated decision-making can be waived when automated decision-making is authorized under Union or Member State law. In these cases, the controller should ensure, at minimum, that the data subjects are able to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. Moreover, under Art. 15(h) GDPR, the subjects of automated decision-making shall be provided meaningful information about the logic involved in the decision.[38]

---

[35] In the Schrems judgment, the ECJ expressly addressed the relationship between the right to data rectification/erasure and the right to pursue an effective legal remedy, by stating that '*legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter'*. See CJEU, C 362/14, *Maximillian Schrems v Data Protection Commissioner*, EU:C:2015:650, para. 95.

[36] See Recital 65, GDPR. However, the controller can object to the erasure of personal data when it would render impossible or seriously impair the objective of the processing when such objective is pursued (*inter alia*) in the public interest (Art. 16(3)(d)).

[37] See Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679* (3 February 2018), available at https://ec.europa.eu/newsroom/article29/items/612053 [accessed 15 September 2024], commented by Veale M. and Edwards L. (2018), 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling', 34(2) Computer Law and Security Review, pp. 398-404.

[38] Brkan, M. (2019) 'Do Algorithms Rule the World? Algorithmic Decision Making and Data Protection in the Framework of the GDPR and Beyond', 27(2) International Journal of Law and Information Technology, pp. 91-121: Bygrave L.A., 'Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making' (2019), in Yeung K. and Lodge M. (eds.), *Algorithmic Regulation,* Oxford University Press, p. 246; Edwards L. and Veale M. (2017), 'Slave to the Algorithm: Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For', 16(1) Duke Law & Technology Review , p. 18; Wachter S., Mittelstadt B., Floridi L. (2017), 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', 7(2) International Data Privacy Law, pp. 76-99.

Lastly, when personal data are processed on grounds of public interest, the data subject should be able to contest, at any time, the processing of their personal data.[39]

c) Implications for the use of AI in tax administration

Tax authorities, among other public bodies, are, in principle, bound by the principles and obligations provided under the GDPR. However, Member States can resort to the restriction clause provided by Art. 23 GDPR to limit or exclude the application of the GPDR in the tax domain, for prevailing matters of public interest. Still, any limitation or exclusion on the application of the GDPR, as provided in Art. 23, should be compliant with the principle of proportionality.[40]

At first sight, the effective scope of application of the GDPR to public authorities might seem unclear. In the realm of tax law, valuable indications on this matter have been provided in recent landmark rulings of the ECHR and CJEU.

Particularly, with the cases LB vs Hungary[41] and SS SIA,[42] the European Courts established that the collection of data by tax authorities should comply with the principles of data protection law, if not expressly waived under European or domestic law. Furthermore, in the recent SCHUFA ruling,[43] the CJEU determined when an AI-supported individual decision constitutes "automated decision-making" for the purposes of the GDPR, laying down specific requirements that could possibly impact the realm of tax law.

---

[39] Art. 21, GDPR.

[40] On the principle of proportionality, see Tridimas, T. (2018) 'The Principle of Proportionality' in Schütze R. and Tridimas T. (eds), *Oxford Principles Of European Union Law: The European Union Legal Order: Volume I*, Oxford University Press: "*Strictly speaking, in formal terms, the application of proportionality entails a three-part test. First, it must be established whether the measure is suitable to achieve a legitimate aim (test of suitability). Secondly, it must be established whether the measure is necessary to achieve that aim, namely, whether there are other less restrictive means capable of producing the same result (the least restrictive alternative test). Thirdly, even if there are no less restrictive means, it must be established that the measure does not have an excessive effect on the applicant's interests (proportionality stricto sensu)." However, "the Court does not necessarily distinguish between the second and the third conditions. Also, in some cases the Court finds that a measure is compatible with proportionality without searching for less restrictive alternatives or even where such alternatives seem to exist*".

[41] ECHR (Grand Chamber), *L.B. vs Hungary* (Application no. 36345/16).

[42] CJEU (Fifth Section), SS SIA, C-175/20, EU:C:2022:124

[43] CJEU, C-634/21, *SCHUFA Holding,* EU:C:2023:957

i) The collection of data by tax authorities under the GDPR

The cases LB vs Hungary and SS SIA similarly established that the collection of data by tax authorities should not violate the principles of data protection law unless specific exceptions apply.

In LB vs Hungary,[44] the Court of Strasbourg found Hungary in breach of Article 8 of the ECHR,[45] due to the Hungarian legislative policy publishing online the personal data of taxpayers who were in debt. The Court held Hungary liable for not demonstrating that the legislature sought to strike a fair balance between the relevant competing individual and public interests in publishing the list, without considering whether their interference in the private life of the affected taxpayers was compliant with the principle of proportionality, as required under Art. 8(2) ECHR.[46]

In this regard, the Court added that the assessment of whether interference in the private life of a citizen is compliant with the principle of proportionality should be addressed under the principles of data protection law, including the principles of purpose limitation, data minimization, data accuracy, and storage limitation.[47]

In the case of SS SIA,[48] the CJEU affirmed that the collection by the tax authorities of taxpayers' personal data from a third party should be subject to the principles set under Art. 5, GDPR.[49] After establishing tax authorities are liable under the GDPR, the CJEU further examined whether the provisions of the GPDR can be waived by public authorities in the absence of an express exemption under domestic law. In answering this question, the CJEU clarified that any limitation to the

---

[44] On LB vs Hungary, see Contrino, A. (2023), 'Evolutionary (on a supranational level) and involutionary (at an internal level) pressures regarding the balance between the right to protection of taxpayers' data and the needs to combat tax evasion', published online, *Rivista Diritto Tributario*, available at https://www.rivistadirittotributario.it/wp-content/uploads/2023/10/Contrino.pdf [accessed 15 September 2024].

[45] Particularly, Art. 8 ECHR states the following: "(1) *Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".*

[46] *LB vs Hungary* (*supra,* note 45), paragraph 138.

[47] *Id*. paragraph 123.

[48] On SS SIA, see Tomo, A. (2024), 'Tax Information, Third Parties and GDPR: Legal Challenges and Hints from the Court of Justice' 32(4) EC Tax Review, pp. 152-162.

[49] *Id*., paragraphs 30-47.

application of the GDPR shall be, in any case, provided by law.[50] Furthermore, the legislative measure that exempts public authorities from the application of the GDPR shall define the scope of the exemption[51] and include the safeguards and guarantees for data subjects[52] to prevent any risk of harm.[53]

Accordingly, based on these two rulings, tax authorities are bound by the provisions of data protection law that are not expressly waived by domestic tax law. This includes, primarily, the principles provided under Art. 5 GDPR, and, additionally, the risk-based and right-based obligations that we have addressed in this section.

Still, these rulings do not provide clear guidance as to whether tax authorities should be also subject to the right-based obligations that apply to the providers of automated decision-making. In this regard, relevant insights can be drawn from the recent SCHUFA ruling.

ii) Automated decision-making in tax proceedings under the GDPR

In the recent SCHUFA ruling, the CJEU addressed the legitimacy of algorithmic scoring systems under the GDPR, providing specific criteria to identify when the outcome of an algorithmic score constitutes automated decision-making.[54]

The case concerned a German citizen who was denied a loan application by the bank due to the low credit score she was awarded by an independent agency of risk scoring (SCHUFA). Upon notification of the loan rejection, the recurrent demanded the SCHUFA agency to disclose the variables that determined her credit risk score. The agency objected to the request on grounds of trade secrecy, and

[50] SS SIA (*supra*, note 44), para. 54
[51] In this regard, see also CJEU, *Privacy International*, C-623/17, EU:C:2020:790, para. 65.
[52] Consistently with CJEU, *Prokuratuur*, C-746/18, EU:C:2021:152, para. 48.
[53] SS SIA (*supra*, note 44), para. 55. Note that this interpretation is consistent with the scope of Art. 52 CFREU and Recital 41 of the GDPR.
[54] Biber, S.E. (2023), 'Between Humans and Machines: Judicial Interpretation of the Automated Decision-Making Practices in the EU', *University of Luxembourg Working Paper No. 19*, available at https://papers.ssrn.com/abstract=4662152 [accessed 15 September 2024], and Silveira, A. (2024) 'Automated individual decision-making and profiling [on case C-634/21-SCHUFA (Scoring)]' 8(2) *UNIO–EU Law Journal*, pp. 74-85.

so did the German Data Protection Agency. As a result, the recurrent appealed the decision of the DPA before the German Administrative court. After examining the case, the court sent a preliminary ruling to the CJEU, asking whether SCHUFA was bound to comply with the provisions set by the GDPR in relation to automated decision-making, including the duty to provide explanations on the outcome of the risk score to the loan applicant pursuant to Art. 15(h) GDPR.

It is worth noting that, in principle, the rights and obligations concerning automated decision-making only apply to fully automated decisions, while the credit risk score provided by SCHUFA was not the sole determinant of the bank's decision to reject the loan application.[55]

However, in the SCHUFA ruling, the CJEU interpreted the notion of automated decision-making with an innovative meaning. Essentially, the Court held that credit scoring should be regarded as an "automated individual decision" – even if it was a "preliminary act" in the overall application process – whenever it played a determinant role in the rejection of the loan application. Therefore, the Court concluded that the use of credit scoring systems that constitute "automated decision-making" can only be deemed legitimate if *(i)* it constitutes a lawful exception to the general prohibition on the use of automated decision-making under Art. 22 GDPR, and if *(ii)* it complies with the obligations provided by the GDPR in relation to automated individual decisions.

Given the similarity between credit and tax risk scoring, the SCHUFA ruling might provide the groundwork for extending these guarantees to the realm of tax controls. According to the perspective of the CJEU, tax risk scores would qualify as "automated individual decisions", similarly to credit

[55] Hurley, M. and Adebayo, J. (2016)'Credit scoring in the era of big data' 18 *Yale Journal of Law and Technology*, p. 148; Aggarwal, N. (2021) 'The norms of algorithmic credit scoring' 80(1) *Cambridge Law Journal*, pp. 42-73; Boo T., Croxson K., and Giles A. (2021), 'Algorithmic fairness in credit scoring' 37(3) Ox*ford Review of Economic Policy*, p. 585-617; Sargeant H. (2023), 'Algorithmic decision-making in financial services: economic and normative outcomes in consumer credit' 3(4) *AI Ethics*, pp. 1295-1311; Spindler G. (2023), 'Algorithms, credit scoring, and the new proposals of the EU for an AI Act and on a Consumer Credit Directive' 15(3-4) *Law and Financial Markets Review*, pp. 239-261; Garcia A.C.B. et *al*. (2024), Algorithmic discrimination in the credit domain: what do we know about it? 39(4) *AI & Society*, pp. 2059-2099.

risk scores, whenever algorithmic scoring played a determinant role in the issuance of an act of assessment.[56]

Should automated tax risk assessment be interpreted as "automated decision making" under the GDPR, tax authorities would be bound to comply with the obligations set for automated decision-making processes under data protection law. This possibility would significantly impact the AI risk management framework that is required under the GPDR since tax authorities should implement appropriate measures to ensure that the scope of automated decision-making complies with the principle of proportionality while providing taxpayers with the right to receive human intervention, hearings, and explanations along the decision-making process.

3.2. AI risk management under the AI Act

a) Risk management obligations

The EU AI Act was published in the Official Journal (OJ) of the European Union on 12 July 2024,[57] after being formally adopted by the Parliament[58] and Council[59] at the end of several stages of negotiation. The implementation of the AI Act followed a provisional agreement[60] between the

[56] The Court agreed with Adv. Gen. Pikamae on the fact that "*the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes 'automated individual decision-making' within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person*." CJEU, *SCHUFA Holding* (*supra*, note 43) para. 75.
[57] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 ["Artificial Intelligence Act"].
[58] European Parliament Press Release, *Artificial Intelligence Act: MEPs adopt landmark law* (13 March 2024), available at https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law [accessed 15 September 2024].
[59] Council of the EU Press Release, *Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on A*I (21 May 2024), available at https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/ [accessed 15 September 2024],
[60] European Parliament Press Release, *Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI* (09/12/2023), available at https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai [accessed 15 September 2024].

Parliament and the Council on a compromise text including several amendments proposed by the Parliament.[61]

In principle, the AI Act provides a set of obligations that are meant to promote the uptake of human-centric and trustworthy AI.[62] The AI Act is set to address the risks that AI systems may pose to the fundamental rights of European citizens[63] – as reflected in the Charter of the Fundamental Rights of the European Union[64] (CFREU) –, by mitigating the risks connected to the specific characteristics of the functioning of AI systems – such as opacity, complexity, data dependency, and autonomous behavior.[65]

The AI Act applies to "AI systems", which are defined as machine-based systems that, for explicit or implicit objectives, are able to infer, from the input data, how to generate outputs such as that can influence physical or virtual environments – such as predictions, content, recommendations, or decisions (see Art. 3(1), in conjunction with Recital 12 of the AI Act).

Within this category, AI systems are classified based on risk.[66] Every risk sub-category defined by the AI Act is bound to comply with different obligations. The requirements provided by the AI Act translate into specific obligations for several partiers along the AI value chain, but mainly upon the providers and deployers of an AI system.

A provider of an AI system is defined as a natural or legal person, public authority, agency, or other body that develops an AI system or a General Purpose AI (GPAI) model, and places it on the market

[61] See, in particular, the Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).
[62] Art. 1, AI Act.
[63] *Id*., consistently with Recitals 1, 2, 3, and 6, AI Act.
[64] "Charter of the Fundamental Rights of the European Union", 2012/C 326/02.
[65] In this regard, see EU Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM(2021) 206 final*, 4.
[66] In principle, the AI Act lays down specific requirements and obligations for "high-risk systems", while providing harmonized transparency rules for "certain" systems and specific rules for the marketing of "general-purpose" AI models. See Art. 1(2), letters (b) to (e), AI Act.

or puts the AI system into service under its own name or trademark, whether free of charge or not.[67] Providers of high-risk AI systems are required to comply with the obligations provided under Articles 16 to 22, which will be examined below.

A deployer of an AI system is defined as a natural or legal person, public authority, agency, or other body using an AI system for professional purposes and under its authority.[68] [69] Deployers of high-risk AI systems are set to comply with the obligations provided under Articles 26 and 27, which will be examined below.

In the case of high-risk AI systems, additional obligations apply to the "importers"[70] and "distributors"[71] of AI systems, respectively under Articles 23 and 24 of the AI Act.

i) Unacceptable Practices

Chapter II establishes a list of AI practices that are prohibited, as they expose European citizens to an unacceptable level of risk.[72] This list includes AI-enabled manipulative and deceptive techniques, social scoring systems, criminal risk profiling systems, systems that create or expand facial recognition databases by scraping facial images on internet or CCTV, systems that infer the emotions of natural persons, "real time" biometric systems[73] and biometric categorization systems that are based on the sensitive data of natural persons.

---

[67] Art. 3(3), AI Act.
[68] Art. 3(4), AI Act.
[69] Article 25, in conjunction with Recitals 83 and 84, provides the criteria to recognize when the deployer or another party (such as the distributor or importer of the system) shall (also) be considered the provider of the system, and therefore be bound to comply with the relevant obligations.
[70] Under Art. 3(6), AI Act, "importer" is defined as "a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country".
[71] Under Art. 3(7), AI Act, "distributor" is defined as "a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market".
[72] On the unacceptable practices under the AI Act, see Neuwirth R.J. (2023), *Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA)*, Computer Law & Security Review (48) n. 105798, and Neuwirth R.J., Migliorini S. (2022), *Unacceptable Risks in Human-AI Collaboration: Legal Prohibitions in Light of Cognition, Trust and Harm*, CEUR Workshop Proceedings, available at https://ceur-ws.org/Vol-3547/paper4.pdf [accessed 15 September 2024].
[73] The prohibition on solely "real time" biometric systems has been widely criticized, among others, by the EDPB and EDPS, which have called for a general ban on the use of biometric systems in any public context. See EDPB-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised*

ii) High-risk AI systems

Chapter III concerns the AI systems that are classified as high-risk for the purposes of the AI Act. The requirements for high-risk AI systems are listed under Articles 9 to 14.

Primarily, high-risk AI systems should be subject to a risk management process that runs throughout the lifecycle of the system, in order to identify, estimate, evaluate, and address the risks of AI systems.[74] The risk management process should ensure that the residual risk associated with each hazard, and the overall residual risk for AI systems, is reduced to an "acceptable risk"[75] through appropriate measures of risk elimination, risk mitigation, and human oversight.

Furthermore, the providers of high-risk AI systems are required to keep records and draw up the technical documentation to assess the compliance of the AI system with the relevant requirements and facilitate post-market monitoring.[76] High-risk AI systems should technically allow for the automatic recording of events (logs) throughout the whole lifecycle of the system, covering the period of use of the system, the input data, the reference database used in the search of the system, and the identification of the natural persons involved in the verification of the results of the system.[77]

High-risk AI systems are also subject to specific obligations to ensure compliance with the principles of data quality, accuracy, robustness, and cybersecurity. In this regard, Art. 10 provides a set of data

rules on artificial intelligence (Artificial Intelligence Act), p. 11, available at https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en [accessed 15 September 2024].

[74] On Art. 9 of the AI Act, see Schuett J. (2023), 'Risk Management in the Artificial Intelligence Act' *European Journal of Risk Regulation* [published online], available at https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risk-management-in-the-artificial-intelligence-act/2E4D5707E65EFB3251A76E288BA74068 [accessed 15 September 2024].

[75] In this regard, Schuett (*id*.) argues that defining the acceptability of a risk is an ethical problem, which would require further guidance by regulators. See also See Mittelstadt B. (2019), 'Principles Alone Cannot Guarantee Ethical AI' 1 *Nature Machine Intelligence*, pp. 501-507, and Goodman, B. (2021) 'Hard Choices and Hard Limits in Artificial Intelligence' (2021) *AIES '21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society,* pp 112-121.

[76] See Art. 11 and 12, in conjunction with Recitals 66 and 71, AI Act.

[77] On the role of record-keeping in ensuring fairness in AI, see Toivonen M., Saari E (2023)., 'How Society Can Maintain Human-Centric Artificial Intelligence' in Toivonen M. and Saari E. (eds.), *Human-Centered Digitalization and Services*, Singapore, Springer, p. 317.

governance and management practices for high-risk systems,[78] while Art. 15 provides that high-risk systems should maintain appropriate levels of accuracy, robustness, and cybersecurity throughout the lifecycle of the system.[79]

Within Chapter III, Section 3 addresses the obligations of the providers and deployers of high-risk AI systems. Primarily, the providers are required to comply with the requirements for high-risk systems set under section 2, by fulfilling the obligations provided under Articles 16 to 20 of the AI Act. Secondly, the AI Act requires the providers to design and develop the system in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately, in order to facilitate compliance.[80] To this end, the providers of AI systems should: *i)* provide specific instructions of use that include concise, complete, correct, and clear information that is relevant, accessible, and comprehensible to deployers;[81] *ii)* design and develop the system in such a way that ensures meaningful human intervention by the deployers of the system.[82]

In turn, under Art. 26, the deployers shall take appropriate technical and organizational measures to use and monitor the system in accordance with the instructions for use and provide adequate human

[78] It is worth noting that the data governance and management practices set under Art. 10 have significant attention for biases, which are considered a probable source of discrimination in violation of Union Law. To this end, Art. 10 requires the providers to complete and sufficiently representative datasets for training and evaluation, and to implement appropriate measures to detect, prevent, and mitigate biases that are likely to have a negative impact on fundamental rights or lead to discrimination prohibited under Union law. See *infra,* section 3.3.

[79] On cybersecurity and robustness in AI, see Sarker, I.H. (2023) 'Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: a comprehensive overview' (6) *Security and Privacy* 295. With regard to the principles of cybersecurity and robustness in the AI Act, see Henrik N., Miriam Rateike M., and Finck M. (2024), 'Robustness and Cybersecurity in the EU Artificial Intelligence Act', *Generative AI and Law (GenLaw '24) Workshop at 41 st International Conference on Machine Learning, Vienna, Austria,* available at https://blog.genlaw.org/pdfs/genlaw_icml2024/4.pdf [accessed 15 September 2024]; Carovano, G., and Meinke A. (2023) 'Improving Fairness and Cybersecurity in the Artificial Intelligence Act' *EWAF'23: European Workshop on Algorithmic Fairness, June 07–09, 2023, Winterthur, Switzerland,* available at https://ceur-ws.org/Vol-3442/paper-43.pdf [accessed 15 September 2024]; Casarosa, F. (2022) 'Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between the Artificial Intelligence Act and the Cybersecurity Act' (3) *International Cybersecurity Law Review*, pp.115-130.

[80] In this regard, see Busuioc M., Curtin D., Almada M., (2023) 'Reclaiming transparency: contesting the logics of secrecy within the AI Act', 3 *European Law Open* pp. 79-105.

[81] Art. 13(1), AI Act.

[82] Art. 13(2), AI Act.

intervention. Furthermore, the deployers should cooperate with the providers in keeping automatically generated logs and managing the input data, when under their control.[83]

The deployers should also comply, *inter alia*, with specific transparency requirements, which consist of informing individuals that they are subject to the use of the high-risk AI system[84] and to perform, under specific conditions laid down under Art. 27(1), a fundamental rights impact assessment.[85]

iii) Other AI systems

The systems that do not qualify as "high-risk" for the purposes of the AI Act are only subject to limited requirements provided in Chapter IV (for "certain" AI systems) and V (for GPAI systems) of the AI Act.

Under Chapter IV, Art. 50 provides transparency obligations for the providers of "certain" AI systems, which include "medium" and "low" risk AI systems, including biometric identification. Indeed, the AI Act recognizes that "certain systems that interact with natural persons or generate content may pose specific risks of impersonation or deception irrespective of whether they qualify as high-risk or not".[86] Accordingly, these systems should be subject to appropriate transparency measures, without prejudice to the application of the provisions concerning high-risk AI systems.[87]

To this end, Art. 50 requires the providers to ensure that AI systems intended to interact directly with natural persons "are designed and developed in such a way that the natural persons concerned are

[83] The obligations provided under Art. 26 should be read in conjunction with Recital 91, AI Act.
[84] Under Art. 26(11), AI Act, this obligation applies towards high-risk systems provided under Annex III, when they make decisions or assist in making decisions related to natural persons. However, this obligation does not prejudice the scope of application of Article 13 of Directive (EU) 2016/680, which provides that under certain conditions, "*Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject […] to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned."* On the right to receive an explanation under the LED Directive, see Goodman B. and Flaxman S. (2017) 'European Union regulations on algorithmic decision-making and a "right to explanation'" (38) *AI magazine*, pp. 50-57, and Quintel, T. (2018), 'Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive' 4 *European Data Protection Law Review*, p.104.
[85] On the scope of the FRIA, see *infra,* section 3.3.
[86] Recital 132, AI Act.
[87] *Id*.

informed that they are interacting with an AI system", unless when the use of AI is apparent to the individual.[88] In the case of emotion recognition systems or biometric identification systems, the deployers should provide information in accordance with the GDPR or the Law Enforcement Directive (LED), as applicable in the case at hand (Art. 50(3)).

It is worth noting the transparency obligations provided under Art. 50 shall not apply in the realm of law enforcement unless those systems are available for the public to report a criminal offense. This exception is further clarified by Recital 132, which provides that the transparency obligations that apply to medium or low-risk AI systems should be subject to targeted exceptions to take into account the special needs of law enforcement.

Lastly, Chapter V provides specific risk management and reporting obligations to the providers and deployers of general-purpose AI systems.[89]

b) Right-based obligations

The final text of the AI Act includes a set of right-based obligations that result from the amendments of the European Parliament, which shared the concerns of the European Data Protection Board (EDPB) regarding the lack of right-based obligations in the Commission Proposal of the AI Act.[90]

Art. 85 provides a right to lodge a complaint with a Marketing Surveillance Authority for an infringement of the provisions of the AI Act. This provision should be read in conjunction with Art. 99(10), AI Act, which provides that "the exercise of powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and national law, including effective

[88] The obligations laid down under Art. 50 provide different transparency requirements based on the system. More specifically: in the case of AI systems that interact directly with natural persons, the provider must inform the end users that they are interacting with an AI system (Art. 50(1)); in the case of AI systems generating synthetic content, the provider shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as generated or manipulated by AI (Art. 50(2)); in the case of deep-fakes, the deployer must disclose to individuals that the content has artificially produced or modified with AI; equivalent obligations apply when an AI system generates or manipulates text which is published with the purpose of informing the public on matters of public interest (Art. 50(4)).

[89] Helberger N. and Diakopoulos N. (2023), 'ChatGPT and the AI Act' 12 *Internet Policy Review*, pp. 1-12.

[90] In this regard, see Watcher S. (2024), 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond', 26 *Yale Journal of Law and Technology*, p. 693.

judicial remedies and due process". Art. 86 then provides that a person who is affected by a decision[91] taken by the deployer on the basis of the output from a high-risk AI system should be provided with clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision. This provision echoes the scope of Art. 15(h) GDPR, but expressly limits the right to receive an explanation only to the "main elements" of the decision made by the deployer.

Furthermore, the second and third paragraphs of Art. 86 provide that the right to receive an explanation can be excluded or limited under Union and domestic law and that Art. 86 shall not apply when a right to receive an explanation is otherwise provided by Union or domestic law.

For these reasons, the scope of Art. 86 AI Act does not seem to provide additional right-based obligations on the deployers of AI systems. On the one hand, due to the limited scope of Art. 86, deployers could resort to the instructions of use and available methods and tools at their disposal to provide explanations on the "main elements" of the decision, thus satisfying the threshold set under Art. 86. On the other hand, Art. 86 does not apply in any case where a right to receive an explanation is otherwise provided, or in any case in which the decision is not taken "on the basis of" the output of the system.

However, regardless of the limited scope of the right-based obligations provided by the AI Act, it is worth noting that the providers and deployers are still subject to the right-based obligations that derive from the principles and rights provided under the GDPR.[92] In this sense, the EDPB has warned that the AI Act should not jeopardize the application of the right to data erasure/correction, the right to the restriction of processing, the right not to be subject to an automated individual decision, and the right to receive an explanation.[93]

[91] In the sense that such decision produces legal effects or similarly significantly affects that person in a way that they consider having an adverse impact on their health, safety or fundamental rights.
[92] *Supra*, section 3.1.
[93] EDPB-EDPS, *supra*, note 73.

c) Implications for the use of AI in tax administration

Since the AI Act adopts a risk-based approach, its scope of application is influenced by the risk categorization of the target AI system. The majority of the risk management obligations apply to high-risk AI systems, which are subject to the specific requirements and risk management measures set out in Chapter III. In the tax domain, the extension of such provisions upon tax authorities depends on whether their systems qualify as high risk for the purposes of the AI Act.

In principle, an AI system qualifies as "high-risk" when *(a)* it is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonization legislation, and *(b)* the product, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonization legislation.[94]

Still, an AI system may qualify as "high-risk" in the absence of the former requirements only when applied in specific sensitive domains, including access to public services, law enforcement, and the administration of justice.[95]

The inclusion of law enforcement and public service systems into the "high-risk" category ensures that such systems meet adequate requirements in terms of design, testing, performance, and accuracy, in order to prevent discrimination or violations of the fundamental rights provided under the CFREU.[96] However, not every use of AI in law enforcement or public service qualifies as high-risk. The AI Act conceives two fundamental exceptions that directly impact the categorization of AI systems in the field of public law and, specifically, tax administration.

[94] Art. 6, AI Act.
[95] These and the other sensitive areas are listed under Annex III, paragraphs 2 to 8, of the AI Act, and should be read in conjunction with Recitals 54 to 60.
[96] See Recitals 55 and 56.

First, under Recital 59, AI systems explicitly intended to be used for administrative proceedings by tax and customs authorities as well as by financial intelligence units carrying out administrative tasks analyzing information pursuant to Union anti-money laundering law should not be classified as high-risk AI systems used by law enforcement authorities for the purpose of prevention, detection, investigation, and prosecution of criminal offenses.[97] A similar exception is provided under Recital 58, with regard to the AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services.

Secondly, AI systems do not qualify as high-risk, regardless of the area of application, when they are implemented to perform preparatory tasks in the decision-making process.[98] Similarly, a system does not qualify as high risk when it is intended to perform a preparatory task to an assessment in the specific sensitive domains listed above unless the system performs profiling of individuals.[99]

In light of these exceptions, the use of AI by tax authorities is unlikely to be subject to the obligations provided for high-risk systems. In the *rationale* of the AI Act, this limitation is meant to prevent further burdens on administrative authorities, in order to facilitate the implementation of advanced technologies in the public domain.

However, this exclusion might create an overall incoherent risk categorization between high-risk and non-high-risk AI systems, and most importantly, it might neglect the application of specific requirements that may facilitate, rather than hinder, the application of AI in the field of tax and public administration.

---

[97] The risk qualification of tax systems under the AI Act has also been addressed by Peeters, B. (2024) 'European Law Restrictions on Tax Authorities' Use of Artificial Intelligence Systems: Reflections on Some Recent Developments' 2 *EC Tax Review*. p. 5, and by Hadwick, D. (2024) 'Slipping Through the Cracks, the Carve-outs for AI Tax Enforcement Systems in the EU AI Act', *Jean Monnet Network on EU Law Enforcement Working Paper*, available at https://jmn-eulen.nl/wp-content/uploads/sites/575/2023/06/8.-WP-Hadwick.pdf [accessed 15 September 2024].

[98] Art. 6(3)(a), AI Act.

[99] Art. 6(3)(d), AI Act.

3.3. Focus: the interplay between the GDPR and the AI Act

The AI Act and the GDPR do not regulate the same objects and do not require the same approach.[100]

The scope of application of the GDPR extends to the processing of personal data belonging to natural persons. Under Art. 3, the GDPR applies either "in the context of the activities of an establishment of a controller or a processor in the Union" (Art. 3(1) GDPR – sc. "*establishment criterion*") or, in specific cases[101], "to the processing of personal data of data subjects who are in the Union", (Art. 3(2) GDPR – "*targeting criterion*").[102]

On the contrary, the obligations of the AI Act apply to the providers of AI systems "*irrespective of whether they are established within the Union or in a third country*",[103] if the output of the system is intended to be used in the EU.[104] The obligations that fall upon the deployers only apply if the deployer has a place of establishment or is located within the EU.[105]

Furthermore, the GDPR primarily adopts a rights-based approach, although it provides a set of provisions that may significantly impact the risk management framework adopted by data controllers and public authorities. By contrast, the AI Act notably adopts a risk-based approach, which consists of imposing specific risk management obligations to AI systems based on their risk-categorization, in order to achieve compliance.

---

[100] See CNIL, *Entry into force of the European AI Regulation: the first questions and answers from the CNIL* (12 July 2024), available at https://www.cnil.fr/en/entry-force-european-ai-regulation-first-questions-and-answers-cnil [accessed 15 September 2024].

[101] Namely when the processing of data relates to: *(a)*" *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union*"; or *(b)* "*the monitoring of their behavior as far as their behavior takes place within the Union".* (Art. 3(2), GDPR).

[102] See EDPB, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*, (12 November 2019) available at https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf [accessed 15 September 2024].

[103] Recital 21, AI Act.

[104] See Recital 22, AI Act, which also provides that the AI Act "*should not apply to public authorities of a third country and international organizations when acting in the framework of cooperation or international agreements concluded at Union or national level for law enforcement and judicial cooperation with the Union or the Member States, provided that the relevant third country or international organization provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals*."

[105] Art. 2(2)(b), AI Act.

However, there are cases where the scope of application of the GDPR and AI Act might overlap. In principle, an AI system that falls under the scope of the AI Act may be subject to the GDPR if it involves a component of data processing. In turn, an AI system that does not involve data processing may only be subject to the AI Act, the processing of data by AI systems that are not covered by the AI Act may only be subject to the GDPR.[106] Generally, the use of AI systems in the public sector involves a strong component of data processing. For this reason, public authorities could be subject, in principle, to the obligations provided both by the GDPR and the AI Act. Notably, the use of AI systems for public purposes could be labeled as high-risk for the purposes of both the GDPR and the AI Act. In this scenario, public authorities would be bound to comply with the risk management framework set for high-risk processing under the GDPR along with the risk-based requirements and obligations set under Chapters 2 and 3 of the AI Act.

In principle, the overlap between the GDPR and the AI Act could increase uncertainty[107] and administrative burdens for the users of AI systems.[108] However, in some cases, compliance with the GDPR could prepare, or facilitate, compliance with the AI Act, [109] while in other cases, the AI Act might provide the standards for interpreting the scope of the GDPR in the field of artificial intelligence. Particularly, the GDPR and the AI Act share several obligations, transparency measures,

---

[106] CNIL, *supra,* note 100.

[107] Furthermore, it could be difficult to establish who are the actors subject to compliance under the AI Act (i.e., the providers and deployers) and the GDPR (i.e., the data controllers and data processors). In this regard, see Paolucci, F., 'Shortcomings of the AI Act - Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights', *Verfassungsblog on Matters Constitutional* (14 March 2024), available at https://verfassungsblog.de/shortcomings-of-the-ai-act/ [accessed 15 September 2024].

[108] These concerns have also been shared in the recent Report on European Competitiveness. See Draghi, M. (2024), 'The future of European competitiveness Part B | In-depth analysis and recommendation', p. 79, available at https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en#paragraph_47059 [accessed 15 September 2024].

[109] Considering the risk of overlap with other sources of data protection law, several provisions of the AI Act contain a "without prejudice clause" clarifying that the AI Act does not seek to affect the application of EU data protection law (see Art. 2(5)(a), Art. 4(a)(1)(c), Art. 68(c)(3), and Recital 2(a) of the AI Act). With regard to the relationship between the AI Act and the GDPR, see Barezzani, S (2024). 'Artificial Intelligence Act (AI Act) and the GDPR', in Sushik J., Samarati P., Young M. (eds.) *Encyclopedia of Cryptography, Security and Privacy*, Springer; CEDPO AI Working Group, *AI and Personal Data A Guide for DPOs "Frequently Asked Questions",* (6 June 2023); available at https://cedpo.eu/ai-and-personal-data-a-guide-for-dpos-frequently-asked-questions/ [accessed 15 September 2024]; Future of Privacy Forum, *GDPR and the AI Act interplay: Lessons from FPF's ADM Case-Law Report* (03 November 2022), available at https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/ [accessed 15 September 2024].

and human oversight requirements that apply to high-risk processing and AI systems, as we have illustrated in the previous sections.[110]

However, it is worth noting that some of the risk-based obligations provided under the AI Act do not find perfect correspondence in the GDPR. These provisions concern, respectively, the area of risk assessment (particularly, right-impact assessment) and the area of risk mitigation (particularly, bias mitigation).

a) Risk assessment under the GDPR and the AI Act

Both the GDPR and the AI Act provide specific transparency requirements concerning AI risk assessment. While Art. 35 GDPR provides that the data controller should perform a DPIA when performing a form of high-risk data processing, Art. 27 AI Act provides that the deployers[111] of high-risk systems shall perform a fundamental rights impact assessment (FRIA) on the risks that the system may produce after deployment.

The content of the impact assessment required by the two provisions is similar. The GDPR-based DPIA requires *(a)* a description of the purpose and envisaged operations; *(b)* an assessment of the necessity and proportionality of such operation in relation to the purpose of data processing; *(c)* an assessment of the risks to the rights and freedoms of data subjects; and *(d)* the measures (such as safeguards, security measures, and other mechanisms) envisaged to address the risks assessed under point (c)[112]. Likewise, the AI Act-based FRIA requires (i) a description of the operations and time of operation of the system in light of its intended purpose; (ii) the identification of the categories of the natural persons and groups likely to be affected by the system, and the specific risks of harm; (iii) the

[110] *Supra*, sections 3.1. and 3.2.
[111] This obligation generally applies to the deployers of high-risk AI system (with the exception of high-risk systems used for critical infrastructure) that are public bodies or private entities providing public services. By contrast, private bodies are only subject to Art. 27 AI Act if they deploy one of the high-risk systems included in point 5, letters (b) or (c), of Annex III AI Act.
[112] See Art. 35(7) FDPR.

human oversight and risk-mitigating measures applied by the provider to mitigate such risks of harm.[113]

However, the FRIA outlined by Art. 27, AI Act, has a somewhat broader scope compared to the DPIA provided in Art. 35, GDPR. In fact, the FRIA covers a wider range of fundamental rights compared to the DPIA, which is primarily focused on the privacy rights that fall under the scope of the GDPR.[114]

In this regard, Mantelero [2024] has pointed out that DPIAs may "*lead to the use of data protection categories to justify the final decision, which largely obscures the rationale behind the assessment in relation to* [those] *rights*", while the FRIA " *entails specific consideration of each relevant fundamental right, as defined in doctrine and case law, with more accurate and transparent results in terms of assessment.* [Furthermore,] *looking at DPIA practice, it is evident that attention given to rights other than data protection is minimal and usually not well elaborated*."[115]

From this perspective, the AI Act poses a higher burden, in terms of risk assessment, compared to the GDPR. Particularly, the FRIA encourages the deployers to perform a "comprehensive" impact assessment that entails specific considerations of each relevant fundamental right that may be put at risk by the AI system, without limiting the scope of such impact assessment to the protection of personal data.[116]

In our view, the differences between GDPR-based and AI Act-based risk assessment do not necessarily translate to higher uncertainty or compliance costs. Rather, when an AI system is subject

[113] In the context of the FRIA, the information provided by the deployer may fall directly from the provider.
[114] In this regard, Art. 35 GDPR expressly states that the DPIA is meant to assess the impact of high-risk processing on the protection of personal data. On the role of fundamental rights (or "human rights") impact assessment in targeting the risks of AI, see Janssen H., Lee M.S.A., Singh J. (2022) 'Practical fundamental rights impact assessments' 30 *International Journal of Law and Information Technology,* pp. 200-232; Montelero A. and Esposito M.S., 'An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems' 41 *Computer Law and Security Review*, No. 105561; Stahl C.B. *et al.,* 'A systematic review of artificial intelligence impact assessments', 56 *Artificial Intelligence Review*, pp. 12799-21831; de Hert, P. (2013) 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments', in de Hert P. and D Wright D. (eds.) *Privacy Impact Assessment*, Springer.
[115] Mantelero, A. (2024), 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template' 54 *Computer Law and Society Review*, No. 106020.
[116] *Id*.

to both the GDPR and the AI Act, the controllers/deployers of the system would be bound to perform a "reinforced" impact assessment[117] that gives equal attention to the protection of personal data and the risk of harm to the other fundamental rights enshrined in the CFREU.

At the same time, when a certain AI system is not covered by the high-risk obligations of the AI Act, the DPIA carried out by the controller may nevertheless provide a description of the specific risks of harm to the fundamental rights of data subjects (meaning, other than data protection), and envisage risk mitigating measures appropriate to such risk of harm.[118]

b) Risk mitigation under the GDPR and the AI Act

In terms of risk mitigation, the AI Act provides specific risk-mitigating measures that do not find a counterpart under the provisions of the GDPR.

Particularly, Art. 10(5) of the AI Act provides that high-risk AI systems can rely on personal data concerning "sensitive" information about data subjects – in derogation of Art. 9 GDPR[119] – in order to detect biases in the training of the model and, as a consequence, prevent discrimination among different classes of data subjects.[120]

---

[117] The overlap between DPIA and FRIA is expressly contemplated by the AI Act, which provides that the FRIA shall "complement" the DPIA carried out in accordance with Art. 35 GDPR (see At. 27(5), AI Act), Consistently with this approach, the CNIL suggests that "*since the common objective is to enable all necessary measures to be taken to limit the risks to the health, safety and fundamental rights of persons likely to be affected by the AI system, these analyses can even be brought together in the form of a single document to avoid overly burdensome formalism*". CNIL, supra, note 100.

[118] In this regard, the CNIL suggests that the deployers of AI systems shall conduct a DPIA that addresses, *inter alia*, the following risks: the risks related to the confidentiality of data that can be extracted from the AI system; the risks to data subjects linked to misuse of the data contained in the training dataset; the risk of automated discrimination caused by training biases; the risk of automated decision-making; the risk of users losing control over their data published and freely accessible online; the risks related to known attacks (*e.g.* data poisoning attacks); the systemic and serious ethical risks related to the deployment of the system. See CNIL, *AI system development: CNIL's recommendations to comply with the GDPR* (07 June 2024), available at https://www.cnil.fr/en/ai-system-development-cnils-recommendations-comply-gdpr [accessed 15 September 2024].

[119] Art. 9(1) GDPR provides that "*processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited*".

[120] In this regard, Recital 67 of the AI Act requires that "*the data sets should also have the appropriate statistical properties, including as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used, with specific attention to the mitigation of possible biases in the data sets, that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations (feedback loop)".*

The GDPR does not expressly include bias-detection mechanisms among the risk management measures that apply to data processors under Art. 35 GDPR. Rather, the implementation of de-biasing mechanisms in data processing systems is prohibited, since de-biasing constitutes a form of processing of sensitive data for the purposes of Art. 9(1) GDPR.

Nevertheless, paragraph 2 of Art. 9 GDPR also provides that data controllers may use sensitive data, thereby wavering the prohibition set under paragraph 1, for matters of social security, social protection law, and reasons of substantial public interest.[121] Yet, this exception only applies when expressly implemented under domestic law, and no EU country has yet resorted to this exception.[122]

For this reason, the GDPR currently provides uncertainty as to whether data providers – such as, hypothetically, tax authorities – could lawfully conduct bias assessments in accordance with the indications of the AI Act. To prevent uncertainty and regulatory burdens in relation to this problem, lawmakers should resort to the exception clause set by Art. 9(2) GDPR and authorize AI providers – such as, hypothetically, tax authorities – to rely on sensitive data to perform bias-mitigation and prevent any risk of discrimination.

c) Implications for the use of AI in tax administration

Although the overlap between the GDPR and the AI Act can potentially increase the uncertainty and costs of compliance, the combined application of these regulations could also bring substantial benefits in the field of high-risk AI. In both the fields of risk assessment and risk mitigation, compliance with the GDPR could foster compliance with the AI Act, while the provisions of the AI Act could complement the risk management framework of the GDPR. Nonetheless, it is harder to reach similar conclusions in cases where AI systems are not intended as high-risk for the purposes of

[121] Particularly, Art. 9(2)(g) GDPR provides an exemption on the prohibition of Art. 9(1) when "*processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*".
[122] Bekkum V.M. and Borgesius F.Z. (2023) 'Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?' 48 *Computer Law and Security Review*, No. 105770.

the AI Act. In all these cases, AI systems that perform high-risk processing are only subject to the obligations provided under the GDPR, while they are exempted from the obligations that apply to high-risk AI, excluding the transparency obligations provided under Art. 50, if applicable in the case at hand.

As we have previously mentioned, this is the case of tax authorities and financial institutions, along with law enforcement authorities (or private bodies involved in high-risk AI systems) that use AI as a preparatory task for the overall decision-making process.[123] These inconsistencies affect not only compliance with the obligations that apply in both systems – i.e., documentation, human oversight, explainability – but also the provisions that are "peculiar" to the AI Act, such as comprehensive impact assessments and bias mitigation measures. Without resorting to these measures, public bodies such as tax authorities would be forced to adopt a less efficient risk management framework compared to law enforcement authorities or social security services (along with other high-risk categories), thus potentially exposing taxpayers to higher risks of harm.

4. The US perspective: the Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI

The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (hereinafter, EO 14110) was signed into order on October 30th, 2023.[124] The intended purpose of E.O 14110 is to harness the potential of AI "for good", by promoting a common endeavor from the government, the sector, academia, and civil society in identifying and mitigating the risks associated with AI.[125]

[123] *Supra*, section 3.2.
[124] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO 14110, 30 October 2023), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [accessed 15 September 2024].
[125] EO 14110, section 1, paragraph 1.

E.O 14110 follows the prior America's strategy for AI innovation, which was enacted in 2020 to address the use of AI by the Government through three pillar regulations – the AI in Government Act of 2020,[126] Executive Order 13859 on AI Leadership,[127] and Executive Order 13960 on AI in Government.[128] EO 14110 does not intend to overlap or supersede the requirements provided in these regulations,[129] although it is meant to address the difficulties in their implementation.[130]

The approach of E.O 14110 is that AI should primarily be "safe" and "secure" through the adoption of "robust, reliable, repeatable, and standardized evaluations", along with policies, institutions, and other appropriate mechanisms to manage the risks associated with AI.[131] From this perspective, the presidential action adopts a risk-management approach that places a primary focus on risk management and human oversight over the functioning of AI. The evaluation and assessment of AI systems lays the groundwork for a responsible and human-centered development of AI, which takes into account the core principles of equality, justice and non-discrimination, privacy, civil liberties, and consumer protection.[132]

In this regard, section 10 of EO 14100. – "*Advancing Federal Government Use of AI*" – specifically addresses the use of AI by Federal Agencies, providing detailed measures to coordinate the use of AI among the Federal Government and increasing AI talent in the Government.

---

[126] H.R.2575 - AI in Government Act of 2020

[127] Executive Order on Maintaining American Leadership in Artificial Intelligence (EO 13859, 19 February 2019).

[128] Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government (EO 13960, 03 December 2020).

[129] In this regard, the O.M.B. guidance issued in application of the EO provides that "*the practices in this section also do not supersede, modify, or direct an interpretation of existing requirements mandated by law or governmentwide policy, and responsible agency officials must coordinate to ensure that the adoption of these practices does not conflict with other applicable law or governmentwide guidance*."

[130] The Stanford Centre for Human Centered Artificial Intelligence (HAI) found that 88% had failed to submit Agency AI Plans under the AI Leadership Order, 76%of 220 agencies had failed to submit AI use case inventories, and more generally, fewer than 40% of all requirements provided under the Three Pillars of the American Strategy were implemented. See Lawrence C., Cui I., Ho D.E. (2022), 'Implementation Challenges to Three Pillars of America's AI Strategy', Stanford RegLab Policy White Paper, available at https://hai.stanford.edu/sites/default/files/2022-12/HAIRegLab%20White%20Paper%20-%20Implementation%20Challenges%20to%20Three%20Pillars%20of%20America%E2%80%99s%20AI%20Strategy.pdf [accessed 15 September 2024].

[131] EO 14110, section 2(a).

[132] EO 14110, section 2, letters (d) to (f).

To address the use of AI by federal agencies, the Government entrusts the White House Office of Management and Budget (OMB) to issue guidance to agencies to strengthen the effective and appropriate use of AI, advance AI innovation, and manage risks from AI in the Federal Government.[133] More specifically, the guidance of the OMB should cover, *inter alia*, the following areas:

(i) *Strengthening AI governance*.[134] To this end, the OMB should provide guidance to agencies for designating a Chief Artificial Intelligence Officer who is responsible for coordinating the use of AI, promoting AI innovation, and managing risks from the use of AI.[135]

(ii) *Implementing required minimum risk-management practices for Government uses of AI that impact people's rights or safety*.[136] To this end, the OMB shall provide guidance to agencies in adopting a risk management framework in accordance with the National Institute of Standards and Technology (NIST) AI Risk Management Framework[137] and Blueprint for an American Bill of Rights.[138]

(iii) *Monitoring the implementation of AI by federal agencies.*[139] To this end, the OMB shall develop a method for agencies to track and assess their ability to adopt AI into their programs and operations, manage its risks, and comply with Federal policy on AI.

---

[133] EO14100 section 10(1)(b).
[134] EO 14100 section 10(1)(b)(i).
[135] The CAIO should also comply with the obligations provided under section 8(c) of Executive Order 13960 and section 4(b) of Executive Order 14091 on "Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government".
[136] EO 14100 section 10(1)(b)(iv).
[137] The NIST AI Risk Management Framework released on 26 January 2023 (NIST, *Artificial Intelligence Risk Management Framework* [AI RMF 1.0] – NIST-AI 100-1),, was developed by the NIST together will private and public stakeholders in order to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems. On 26 July 2024, the NIST released another framework addressing the risks of generative AI, as required under section 4.1(a)(i)(A) of EO 14110. See NIST, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* – NIST AI 600-1, available at https://doi.org/10.6028/NIST.AI.600-1 [accessed 15 September 2024].
[138] On the Blueprint, see *infra.*
[139] EO 14100 section 10(1)(c).

On the 28th of March 2024, the Director of the OMB released a memorandum (hereinafter, the "OMB Memorandum") directing agencies to advance AI governance and innovation while managing the risks that lie within the use of AI in Government.[140]

The Memorandum applies to all agencies defined in 44 USC. § 3502(1),[141] with the exception of the cases where AI systems are used as a component of a National Security System,[142]or, in some cases, when AI systems are used by elements Intelligence Community.[143] Particularly, section V of the Memorandum outlines a set of minimum risk management practices to manage risks related to agency information and systems, in accordance with section 10(1)(b)(ii) of the EO. The scope of section V aligns with the purpose of this paper, as it provides specific risk-management obligations that extend, among others, to tax authorities.

a) Risk-based obligations

The risk-based obligations set out under Section V of the Memorandum are meant to address the risks for the rights and safety of the public. Accordingly, these obligations only apply to the extent that the AI system qualifies as "safety-impacting" or "right-impacting" pursuant to the definitions provided in Section VI of the memorandum.

---

[140] Young S.D., *Memorandum for the Heads of Executive Departments and Agencies* (M-24-10, March 2024), available at https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf [accessed 15 September 2024],

[141] Under 44 USC. § 3502(1), the term "agency" includes "*any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government […], or any independent regulatory agency*" that is not expressly excluded thereinunder.

[142] On the use of AI in the field of national security, see Shasha Y. and Carroll F. (2022) 'Implications of AI in national security: understanding the security issues and ethical challenges', in Montasari R. and Jahankhani A. (eds.) *Artificial intelligence in cyber security: Impact and implications: Security challenges, technical and ethical issues, forensic investigative challenges*, Springer International Publishing, pp. 157-175, and Sayler, K.M. 'Artificial intelligence and national security" (2020) *Congressional Research Service* R-45178.

[143] The bodies of the US "Intelligence Community" are indicated under paragraph 4 of 50 US Code § 3003.

Safety-impacting AI refers to AI whose output produces an action or serves as a principal basis for a decision that has the potential to significantly impact the safety of: *(1)* human life or well-being; *(2)* climate or environment; *(3)* critical infrastructure; *(4)* strategic assets or resources.[144]

Right-impacting AI refers to AI whose output serves as a principal basis for a decision or action concerning a specific individual or entity that has a significant effect on that individual's or entity's: *(1)* civil rights, civil liberties, or privacy; *(2)* equal opportunities; *(3)* access to or the ability to apply for critical government resources or services.[145]

In order to establish whether an AI system is subject to the risk-based obligations set under Section V, federal agencies shall determine, in coordination with the Chief AI Officer (CAIO), whether the system is safety or rights-impacting based on the former definitions. In doing so, the Agency should place particular focus on whether the output of the AI system serves as the principal basis for a decision or action.[146]

When a system qualifies as safety or right impacting under the OMB memorandum, the relevant Agency should adopt specific measures at different stages of the functioning of the AI systems. Particularly:

1. *Before implementing the system,* the Agency should *(i)* conduct – and periodically update – an impact assessment on the risks associated with the AI; *(ii)* conduct adequate testing to ensure that the system will perform in a real-world context; *(iii)* conduct an independent evaluation over the functioning of the system, which should be performed by the CAIO together with an AI oversight board or another appropriate agency that has not been involved in the development of the system.[147] When a system qualifies as rights-impacting, the impact

[144] OMB Memorandum, section 6. Note that the first paragraph of the Appendix to the Memorandum includes a list of practices that are presumed to be "safety-impacting" for the purposes of section 5(c).
[145] *Id*. The practices that are presumed to be "rights impacting" are included in the second paragraph of the Appendix to the Memorandum.
[146] OMB Memorandum, section 5(b).
[147] OMB Memorandum, section 5(c)(iv), letters (a) to (c).

assessment and subsequent monitoring activities should address the impact of AI on equity and fairness, and foresee appropriate measures to prevent unlawful discrimination, harmful bias, or inequality, including incorporating feedback from the public.[148]

2. *While using the system,* the Agency should: *(i)* conduct ongoing monitoring and regularly evaluate risks from the use of AI; *(ii)* mitigate emerging risks to rights and safety; *(iii)* ensure adequate human training, and provide additional human oversight, intervention, and accountability as part of decisions or actions that could result in a significant impact on rights or safety; *(iv)* provide public notice and plain-language documentation on the functioning of the system.[149] When a system qualifies as rights-impacting, the Agency should conduct ongoing monitoring and mitigation for AI-enabled discrimination. Furthermore, when possible, the Agency should implement appropriate mechanisms to notify negatively affected individuals and maintain human review or output options for AI-enabled decisions.[150]

b) Right-based obligations (reference to the Blueprint for an AI Bill of Rights)

In defining the minimum practices for safety and rights impacting AI systems, the Memorandum states that agencies are encouraged to incorporate, as appropriate, additional risk management practices to address context-specific risks associated with certain uses of AI. According to the OMB, the agencies shall draw best practices from domestic and international standards, including the NIST AI Risk Management Framework and, most importantly, the Blueprint for an AI Bill of Rights.[151]

[148] OMB Memorandum, section 5(c)(v), letters (a) and (b).
[149] OMB Memorandum, section(c)(iv), letters (d) to (l).
[150] OMB Memorandum, section (c)(v), letters (c) to (e).
[151] White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights*, available at https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [accessed 15 September 2024].

The Blueprint for an AI Bill of Rights (hereinafter, Blueprint) is a non-binding[152] whitepaper, published by the White House in October 2022, which aims at supporting the development of policies and practices for the building, deployment, and governance of AI in accordance with the civil rights and democratic values of the United States.[153]

The rights provided under the Blueprint translate to specific risk-based obligations for federal agencies, which should implement them considering the extent and nature of the risk of harm that the system poses to people's rights and opportunities.[154]

The core right provided by the Blueprint is the right to be protected from unsafe and ineffective AI systems. The wording of this provision echoes the fundamental principles of "safety and trustworthiness" provided under Art. 1 of the EO 14100.[155] In this sense, the right to safety requires the adoption of a comprehensive risk management system to prevent any foreseeable risk of harm against the addressees of AI.[156]

The Blueprint further provides that individual citizens should not be subject to algorithmic discrimination. The right not to be discriminated against implies further risk management obligations,

---

[152] Accordingly, the Blueprint itself does not "*create any legal right, benefit, or defense, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person*". Blueprint, page 2.

[153] On the limited scope of the Blueprint in the work of Federal Agencies, see Hine E and Floridi L. (2023) 'The blueprint for an AI bill of rights: in search of enaction, at risk of inaction' (33) *Minds and Machines*, pp. 285-292; Lage, D., Pruitt R., and Arnold J.R. (2024) 'Who Followed the Blueprint? Analyzing the Responses of US Federal Agencies to the Blueprint for an AI Bill of Rights' arXiv preprint, p. 2404, available at https://arxiv.org/abs/2404.19076#:~:text=Through%20an%20analysis%20of%20publicly%20available%20records%20across,aligned%20with%20one%20or%20more%20of%20its%20principles. [accessed 15 September 2024].

[154] However, the Blueprint itself recognizes that in some cases, exceptions to the principles there described may be necessary to comply with existing law, conform to the practicalities of a specific use case, or balance competing public interests. *Id.,* page 9.

[155] Accordingly, the Blueprint refers to E.O 14110 as one of the fundamental measures that were taken to address the risks of safety and effectiveness in the use of AI by the Government. *Id*., p. 16.

[156] As an example of the risks associated with unsafe and ineffective AI systems, the Blueprint mentioned an incorrect AI system that, due to feedback loops, suggested performing police visits in neighborhood with comparatively low crime rates. See Mattu S. and Gilbertson A., *Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them* (02 December 2021) https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them [accessed 15 September 2024]

such as testing and risk mitigation before deployment, equity impact assessments, continuous monitoring, and clear organizational oversight.[157] [158]

The Blueprint also conceives a right to data privacy, which is also intended as a right to be free from abusive practices in AI profiling. To this end, the users of AI systems should provide default protections that prevent such abusive practices and implement enhanced protection in sensitive domains such as law enforcement or mass surveillance.

Lastly, the Blueprint provides that US citizens shall have a right to receive notice when an AI system has contributed to a decision that adversely impacts them, and how and why it contributed to the decision-making process. Furthermore, the addressees of AI profiling should have, when possible, the right to opt out in favor of a human alternative, and – in any case – the right to appeal the decision and subject it to human considerations and fallback. These obligations call on the providers of AI systems to adopt specific measures to ensure transparency, explainability, and human intervention in individual decision-making processes.

The combined application of these rights further emphasizes, from a right-based perspective, the relevance of AI risk management in the public domain. Although these provisions are intentionally overlapping,[159] the recurrent aspects addressed in the Blueprint – risk assessment, risk mitigation, privacy, transparency, and human intervention – largely align with the scope of the risk management framework developed by the O.M.B.

---

[157] The problem of AI-enabled discrimination has had relevant impact in the field of crime-forecasting, especially in the assessment of the risk of recidivism. See National Institute of Justice, *2021 Review and Revalidation of the First Step Act Risk Assessment Tool* (NCJ 303859, December 2021) available at https://www.ojp.gov/pdffiles1/nij/303859.pdf [accessed 15 September 2024].

[158] A set of risk management measures to address discrimination in AI can be found in NIST (2022). *NIST Special Publication 1270: Towards a Standard for Identifying and Managing Bias in Artificial Intelligence* (15 March 2022) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf [accessed 15 September 2024].

[159] As stated in the Blueprint, "*considered together, the five principles and associated practices of the Blueprint for an AI Bill of Rights form an overlapping set of backstops against potential harms. This purposefully overlapping framework, when taken as a whole, forms a blueprint to help protect the public from harm". Id.,* p. 8.

Accordingly, the Blueprint provides valuable guidance – although non-binding – as to the priorities that federal agencies should seek when implementing appropriate risk management measures in accordance with the EO and Memorandum.

c) Implications for the use of AI in tax administration

As we have previously mentioned, the EO and the Memorandum, as inspired and integrated by the Blueprint for an AI Bill of Rights apply to 44 USC. § 3502(1), are binding upon all the federal agencies listed under 44 USC. § 3502(1), including but not limited to, the IRS.

Accordingly, the IRS recently released an interim guidance[160] for the implementation of the requirements set under the Memorandum (hereinafter, Interim Guidance). The Interim Guidance follows and complements the previous "IRS AI Strategy",[161] which was implemented by the IRS in 2020 pursuant to Executive Order 13960.

The first part of the guidance focuses on AI governance.[162] In order to comply with the obligations, set under section 10.1 of the EO, the IRS has designed a governance structure that has the power to intervene in the implementation of the system, to ensure compliance with the applicable regulations.[163]

The second part of the guidance focuses on extending the risk-based obligation provided by the OMB. In this regard, the risk management measures described by the IRS coincide with the recommendations provided under section 5 of the Memorandum.

Particularly, the IRS expects to apply appropriate risk management measures both before the implementation of the system (i.e., performing an impact assessment, conducting real-world testing,

---

[160] Johnson, Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles (20 May 2024), available at https://www.irs.gov/pub/foia/ig/spder/interim-guidance-raas-10-0524-0001-artificial-intelligence-governance-and-principles-redacted.pdf [accessed 15 September 2024].
[161] Interim Guidance, 10.24.1.1(2).
[162] Interim Guidance, 10.24.1.5.
[163] The governance structure of the IRS includes, together with the CAIO, The Chief Data and Analytics Officer (CDAO), the Data and Analytics Strategic Integration Board (DASIB), the AI Governance Project Management Office (PMO), AI Assurance Team, AI Project Teams.

and independently evaluating the functioning of the system)[164] and during its use (i.e., conducting ongoing monitoring and regularly evaluating the risks of AI; mitigating the risks to rights and safety; ensuring sufficient human training and human oversight in the decision-making process; providing documentation on the functioning of the system).[165]

Furthermore, when using rights-impacting AI systems, the IRS expects to adopt the additional risk management measures required under section 5 of the Memorandum.[166]

Lastly, the IRS has implemented the provisions of the OBM memorandum regarding the disclosure of the functioning of their systems to the Government and the public.[167] In accordance with the Memorandum, the IRS has reaffirmed that the disclosure of data to the public will only happen to the extent that it does not undermine the interests pursued by the IRS.[168]

The overall risk management framework developed by the IRS ensures compliance with the principles of EO 14100 and with the provisions set out in the Memorandum. Furthermore, the risk management framework designed by the IRS might show consideration for the right-based obligations stemming from the Blueprint for an AI Bill of Rights. In this regard, the Interim Guidance provides that the implementation of AI in the tax domain should, in any case, "emphasize the protection and prioritization of taxpayer rights", by complying with the principles of safety and trustworthiness set under the EO.[169]

Since the IRS expressly advocates for a rights-oriented approach to the use of AI in tax administration, the Blueprint might provide the groundwork for extending the framework of taxpayer protection to the AI domain and address the use of automated decision-making in individual tax proceedings.

---

[164] Interim Guidance, 10.24.1.8, numbers 1 to 3.
[165] Interim Guidance, 10.24.1.8, numbers 4 to 8.
[166] Interim Guidance, 10.24.1.8, numbers 9 to 14.
[167] Interim Guidance, 10.24.1.6.
[168] Interim Guidance, 10.24.1.6.1(d), In accordance with section 4(d)(i) of the Memorandum.
[169] Interim Guidance, 10.24.1.9.

5. Comparing the EU and US approaches to AI risk regulation in tax administration

In the previous sections, we have broadly addressed the AI risk management obligations that fall upon the subjects of the GDPR and AI Act, and upon the Federal Agencies addressed by EO 14110.

This analysis clearly shows that the US is addressing the use of AI in the public domain through a risk-based approach that is partly consistent with the scope and requirements of the AI Act. In turn, the risk management framework provided by the AI Act operates in conjunction with the GDPR, by providing a set of risk management measures aimed at preventing any risk of harm to the rights of EU citizens.

In the field of tax law, the risk management obligations stemming from the GDPR, the AI Act, and the EO could lay the groundwork for a safe and effective implementation of AI in tax audits, both in the EU and the US.

Nevertheless, as we have previously pointed out, the extension of such risk-based obligations to tax authorities largely depends on whether the use of AI in tax proceedings qualifies as high-risk (or rights-impacting) for the purposes of the three regulations.

The risk categorization of tax-related AI systems is not only a matter of consistency in the application of the three regulations but also a fundamental pre-requisite to subject tax authorities to the risk management framework provided therein. In turn, the adoption of such a risk management framework would enable tax authorities to better address the risks of using AI in the tax administration, ensuring higher standards of protection and enhancing the effectiveness of tax audits.

Accordingly, we now provide a comparison of the risk management framework provided under the GDPR, the AI Act, and the EO by primarily focusing on the risk categorization of tax-related AI systems in each regulation. Based on such initial comparison, we then proceed to compare the risk

management obligations provided in each regulation to address the risks of AI in tax, by focusing on the risks related to algorithmic discrimination, human/AI interaction, and data security.[170]

5.1. Assessing the risk of AI in tax administration

The EU and the US adopt a different approach in determining what constitutes high-risk AI or the use of AI for the purposes of risk management regulation.

The AI Act pre-determines what constitutes a high-risk AI system in the realm of public law, by expressly including a set of high-risk domains – namely law enforcement, social assistance, and administration of justice – under the scope of Annex III. As we have previously noted, the AI Act expressly excludes tax authorities from the high-risk AI domains, as clarified under Recital 59.

Under the GPDR, data processing is labeled as high-risk when it is likely to result in a high risk to the rights and freedoms of individuals. In principle, this definition could fit the use of tax-related AI systems, due to their potential impact on the rights and freedoms of taxpayers.

Under the Memorandum, an AI system may qualify as rights-impacting to the extent that its output influences a decision that targets civil rights, equal opportunities, or access to government services of US citizens. From this perspective, the categorization of tax-related AI systems under the rights-impacting domain seems uncertain.

Compared to the others, the risk assessment procedure of the AI Act seems to provide an increased level of certainty, since it expressly states what constitutes a high-risk system and what does not.[171]

By contrast, the GDPR and the Memorandum encompass a wide definition of high-risk processing or rights-impacting AI for the purposes of each regulation. The inclusion of tax scoring systems in such categories is not apparent but rather depends on whether those systems, respectively, *(i)* result in high

[170] *Supra,* section 2.
[171] Novelli C. et *al*. (2024), 'AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act' 3 *Digital Society*, published online, available at file:///C:/Users/giorg/Downloads/s44206-024-00095-1.pdf [accessed 15 September 2024].

risks to the rights and freedoms of natural persons or *(ii)* target the civil rights equal opportunities, or access to government services of US citizens.

From this perspective, the risk categorization of tax-related AI systems remains uncertain. In our view, lawmakers should address this uncertainty by harmonizing this approach to AI risk assessment in the tax domain. In fact, both in the EU and the US, there might be several reasons to argue that the progressive implementation of AI in tax administration calls for a uniform and precautionary approach to risk regulation.

On the one hand, the risk categorization of AI systems influences the risk management framework they should apply. In the case of the GDPR, high-risk processing triggers specific risk management obligations, including but not limited to the obligation to perform a DPIA.[172] In the case of the AI Act and the Memorandum, AI systems that do not qualify as high-risk or rights/safety impacting are *de facto* exempt from a large part of the risk management obligations provided in both regulations. For this reason, labeling tax-related AI systems as high-risk would translate into higher standards of protection for taxpayers.

On the other hand, the use of tax scoring systems might expose taxpayers to a significant risk of harm to their fundamental rights, such as the right not to be discriminated against.[173] Notably, this risk of harm does not differ from the potential risks that may apply to data subjects in other fields, such as law enforcement, social security, or credit scoring, which are all defined as high-risk or rights-impacting fields under the GDPR, AI Act, and EO 14100.

Based on these considerations, we reaffirm that tax-related AI systems should be uniformly considered high-risk (or rights-impacting, in the case of EO 14100) under the standards of AI regulation in the EU and the US. This approach would ensure consistency in the application of AI

[172] *Supra*, section 3.2.
[173] As provided, for instance, by Art. 21 CFREU.

risk management obligations across the public domain and provide a comprehensive framework for addressing the risk of AI, for the benefit of tax authorities and taxpayers alike.

5.2. Addressing the risk of discrimination

Both in the EU and the US, the risk of discrimination arising from the use of AI in public administration has been addressed with great concern. The respect for the rights enshrined in the CFREU, including the right not to be discriminated against, is at the core of the rights-based approach of the GDPR.[174] Similarly, the AI Act qualifies systems as high- or non-high-risk by considering the impact of the system on the protection of the rights provided under the Charter, including the right not to be discriminated against.[175] In turn, the EO takes a clear stand against discrimination in public administration, consistently with the scope of the Blueprint for an AI Bill of Rights. However, when it comes to managing the risk of discrimination, the AI Act and Memorandum seem to take a more effective approach compared to the GDPR.

On the EU side, as we have emphasized in the previous sections, the AI Act expressly allows the use of sensitive data to perform bias detection in the training of the dataset, in order to minimize the risk of misrepresentation and discrimination in the output of the model.

On the US side, the Memorandum, in accordance with the EO and the AI Bill of Rights, provides a set of additional risk-mitigating measures addressing equity and fairness in the development and implementation of safety-or-rights-impacting AI systems. The IRS has expressly planned to adopt such measures with its risk management framework, thus emphasizing its effort to mitigate any risk of discrimination in AI-led tax administration.

---

[174] See Recital 4, GDPR.

[175] See Recital 48, AI Act: "*the extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high risk*".

Although the GDPR repeatedly addresses the risk of discrimination in the realm of high-risk data processing, it does not explicitly conceive measures such as the bias-detection system of the AI Act or the reinforced risk management process provided by the Memorandum.

In the EU, the lack of equivalent measures for bias mitigation under the GDPR could expose taxpayers to a higher risk of discrimination. In fact, the bias-detection measures provided under Art. 10 of the AI Act do not apply to tax authorities (as they do not qualify as high-risk for the purposes of the AI Act), meaning that the only source of risk management that applies to tax authorities is the GDPR itself.

In order to address this problem, we believe that EU Member States should favor the adoption of bias-mitigating measures by public authorities, by providing an express exemption on the prohibition set by Art. 9 GDPR. As we have previously emphasized, this exception would be consistent with the scope of Art. 9(2)(g) GDPR, which allows the use of sensitive data for matters of public interest.

Furthermore, this approach would ensure that the exemption of tax authorities from the scope of the AI Act does not translate to less adequate risk mitigating measures for taxpayers, but rather enhances the risk management standard of the GPDR to the level of the other EU and US sources of AI risk regulation.

5.3. Preventing automated decision-making in tax proceedings

As public authorities increasingly rely on AI systems to perform their daily tasks, automated decision-making becomes a matter of great concern for domestic legal systems.

As we have emphasized in section 2, the use of AI in the public domain could lead to forms of "human overreliance" on the outcome of the system, due to the lack of appropriate training and individual responsibility on public officials. In this scenario, the amount of human oversight and decision-making power in tax proceedings would decrease in favor of automated decision-making, leaving no guarantee of human oversight to the data subjects.

In this regard, the GDPR, AI Act, and EO 14110. address the matter of automated decision-making quite diversely.

Primarily, the GDPR addresses automated decision-making through a rights-based approach. In Art. 22, the GDPR provides that data subjects shall have a right not to be subject to automated individual decisions. Yet, in the realm of public law, the right not to be subject to an automated individual decision does not necessarily limit the scope of work of public administrations. Indeed, public authorities may be lawfully exempted by the prohibition set under Art. 22 GDPR, insofar as the exemption constitutes a necessary and proportionate measure for pursuing the public interest.

However, even when authorized to perform automated decision-making under the GDPR, public authorities would still be subject to the rights-based obligations that apply to the addressees of automated decision-making, as provided under Articles 15 and 22(3) of the GDPR.

Ensuring the rights provided to the subjects of automated decision-making may be particularly burdensome upon public authorities.[176] Particularly, public authorities might have difficulties in safeguarding the right to receive an explanation of the logic behind automated decision-making, as there might be technical issues or other reasons that prevent the provision of detailed explanations for automated tax controls.[177]

---

[176] In his opinion on the SCHUFA ruling, Adv. Gen. Pikamae specifically addressed the scope of the right to receive an explanation on the outcome of an automated individual decision – as provided by Art. 15(h) GDPR – by stating that it "*must be understood to include sufficiently detailed explanations of the method used to calculate the score and the reasons for a certain result. In general, the controller should provide the data subject with general information, notably on factors taken into account for the decision-making process and on their respective weight on an aggregate level, which is also useful for him or her to challenge any 'decision' within the meaning of Article 22(1) of the GDPR*". See *Opinion of Advocate General Pikamae on Case C-634/21*, EU:C:2023:220, para. 58.

[177] Amongst the others, there can be technical issues in explaining models that make use of machine learning. For a thorough analysis of explainability in machine learning models, see Rudin C. (2019), 'Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead', 1 Natural Machine Intelligence, p. 206. See also Bell A. et *al*. (2022), 'It's Just Not That Simple: An Empirical Study of the Accuracy-Explainability Trade-off in Machine Learning for Public Policy', in 2*022 ACM Conference on Fairness, Accountability, And Transparency,* p. 248; Sokol K. & Vogt J.E (2023)., '(Un)Reasonable Allure of Ante-Hoc Interpretability for High-Stakes Domains: Transparency Is Necessary but Insufficient for Comprehensibility', in Workshop on Interpretable Machine Learning in Healthcare, available at http://arxiv.org/abs/2306.02312 [accessed 15 September 2024]; Keenan B. & Sokol K. (2024), 'Mind the Gap! Bridging Explainable Artificial Intelligence and Human Understanding with Luhmann's Functional Theory of Communication', available at http://arxiv.org/abs/2302.03460 [accessed 15 September 2024]; Amarasinghe K. et *al*. (2023),' On the Importance of Application-Grounded Experimental Design for Evaluating Explainable ML Methods', available at http://arxiv.org/abs/2206.13503 [accessed 15 September 2024].

For this reason, EU public authorities, and tax authorities specifically, must adopt adequate safeguards in order to prevent automated decision-making and, as a consequence, the application of the right-based obligations that relate to automated decision-making under the GDPR.

Based on the indications of the EDPB,[178] an individual decision supported by an automated system does not constitute automated decision-making insofar as the data controller, or the processor on his behalf, applies "meaningful" human intervention in the decision-making process.

By contrast, the AI Act conceives human oversight as a requirement for high-risk systems and as an obligation for AI deployers, which stems from the Art. 14 AI Act.

The approach of the Memorandum is consistent with the approach of the AI Act. Particularly, under section v(c) of the Memorandum, the OMB expressly includes a requirement for "human oversight", "human review", and "opt/out options" among the minimum risk management practices to be adopted by federal agencies pursuant to section 10 of the EO. As we have previously pointed out, the IRS planned to implement these requirements, as resulting from its Interim Guidance.[179]

In the EU, the detailed provisions of the AI Act concerning human oversight might help tax authorities reach the threshold for "meaningful human intervention" in AI-led tax proceedings and, consequently, prevent the application of Art. 22 GDPR and the right-based obligations related to automated decision-making.

Although in the US there is no equivalent provision as Art. 22 GDPR, the right-based obligations relating to automated decision-making – including, particularly, the right to receive notice and explanation on the outcome of an automated individual decision – find correspondence in the principles of US administrative and tax law,[180] and in the Blueprint for an AI Bill of Rights.

---

[178] EDBP, *supra, note 37*.
[179] *Supra*, section 4.
[180] See Deeks, A.S. (2019) 'The Judicial Demand for Explainable Artificial Intelligence' 119 *Columbia Law Review*, pp.1829–1850.

For this reason, the indications provided in the Memorandum, similarly to the AI Act, may provide guidance to the IRS in implementing appropriate risk management measures to prevent, or otherwise control, the scope of automated decision-making in tax proceedings.

In this regard, it is worth noting that neither the Memorandum nor the AI Act clarify at what stage a person affected by a high-risk AI system could request human intervention. Naturally, this determination depends on the context and scope of application of the system, since some use cases may require a human-in-the-loop sort of intervention, while others may require *post-hoc* review or opt-out mechanisms.[181]

In the realm of tax scoring, we believe that taxpayers should be entitled to request human intervention *during* tax proceedings (*i.e.,* human in the loop), rather than in the form of a subsequent review or preventive opt-out mechanism. In fact, this approach would balance the interests of tax authorities in implementing AI in tax audits, while allowing taxpayers to exercise the right to be heard and receive an explanation on the outcome of their act of assessment.[182]

Furthermore, this approach would be consistent with the recent developments of the CJEU concerning the interpretation of risk-scoring systems under the GDPR. As we have pointed out in section 3, the CJEU recognized that relying on an algorithmic risk score as part of a complex procedure may still be considered automated decision-making, insofar as the recipient of the risk score "*draws strongly*

[181] It was argued that opt-out procedures could prevent risks of a "digital divide", *i.e*. differences in the ability to communicate with tax authorities based on one's digital skills. Accordingly, it was suggested that legal systems should provide taxpayers with a right to engage with tax authorities in non-digital formats when taxpayers do not possess adequate means to be involved in digital interactions. See Contrino, A. (2023) 'Digitalizzazione dell'Amministrazione Finanziaria e Attuazione del Rapporto Tributario: Questioni Aperte e Ipotesi di Lavoro nella Prospettiva dei principi generali' 2 *Rivista DIiritto Tributario*, pp. 116-117, See also De la Feria, R., and Ruiz, M.A.G., (2022) 'The Robotisation of Tax Administration', in Ruiz M.A.G. (eds.), *Interactive Robotics: Legal, Ethical, Social and Economic Aspects*, Springer, p. 115: "*for most – young, higher-income, highereducated, tech-savvy, individuals – AI can be a convenient alternative to bureaucracy; but for the less tech-savvy elderly, or for those who lack the income to access digital services, or the language skills to understand them, the robotisation of life can have dehumanising effects. Tax compliance technology is particularly susceptible to these risks, and there is already evidence of divides emerging in countries, like the US, where compliance AI has been used the most",*

[182] See Art. 41 CFREU.

on that probability value to establish, implement or terminate a contractual relationship with that person."[183]

Accordingly, based on the indications provided by the CJEU in the SCHUFA ruling, human in the loop seems to constitute a minimum requirement for the implementation of AI in tax proceedings. Furthermore, this minimum requirement does not automatically outweigh the application of Art. 22, unless the decision-maker draws on other elements compared to the risk score.

Similar considerations could apply to the I.R.S, under the risk management framework provided under EO 14100. In this case, human in the loop would constitute a necessary requirement to enhance the rights of taxpayers in AI-led tax proceedings[184] and enforce the right to receive notice and explanation on the decision made upon them, in accordance with the AI Bill of Rights.

6. Conclusion

In this paper we have addressed the AI risk management regulations that applies to public bodies in the EU and in the US, emphasizing their impact on tax authorities and on the risks concerning the use of AI in tax proceedings.

In the EU, the risk management obligations that apply to tax authorities are found within the GDPR and the AI Act. Although the GDPR and the AI Act have a different approach and scope of application, both regulations require the implementation of a risk management framework to address the risks relating to high-risk processing and high-risk AI system.

[183] CJEU*, Schufa Holding* (supra, note 43)
[184] *Supra*, note 169.

In the US, the Government has implemented a new comprehensive regulation on AI risk management in the public domain – EO 14100 –, which was followed by an OMB Memorandum that addresses, inter alia, the required risk management measures for public authorities implementing AI.

The three regulations similarly address the risks concerning the implementation of AI in tax administration. Particularly, the risks relating to algorithmic discrimination, human/AI interaction, and data security, find appropriate consideration in specific provisions of the GDPR, the AI Act, and the Memorandum.

In some cases, the standards and requirements stemming from one of these three regulations provide valuable guidance for implementing the risk management measures provided by the other.

With regard to the risk of discrimination, the risk management framework envisioned by the AI Act and the Memorandum encompasses additional measures to prevent, detect, and mitigate biases on the output of algorithmic profiling, being one of the main causes of discrimination in the realm of AI. In turn, these risk management measures could also benefit compliance with the requirements of the GDPR, although appropriate legislative measures are needed to integrate such measures into the scope of the GDPR.

With regard to the risks concerning human/AI interaction, the recent developments in the interpretation of the GPDR could provide a standard for complying with the human oversight requirements set by the AI Act and the Memorandum, in order to prevent automated decision-making in individual proceedings.

Based on this comparison, the risk management framework provided by the three regulations has a shared concern for all the risks that may concern the use of tax-related AI systems, emphasizing the progressive alignment in the EU and US approach to AI regulation in the public domain.

However, there are still fundamental inconsistencies – both in the EU and US approaches – concerning the application of AI risk regulation to tax administrations. Particularly, the AI Act

excludes tax-related AI systems from the requirements and obligations that concern high-risk systems. Similarly, the OMB Memorandum encompasses a notion of rights-impacting AI systems that does not seem to include tax scoring or equivalent systems.

As we have extensively pointed out, the disharmony in the risk classification of tax-related AI systems might create imbalances in the application of the three regulations, and lower the standards of protection for taxpayers in the US and the E.U. Accordingly, we believe that lawmakers should adopt a precautionary and uniform approach to AI regulation in the tax domain, by placing tax-related AI systems among the pool of high-risk and rights-impacting systems for the purposes of the AI Act and EO 14100. By harmonizing the risk class of tax-related AI systems, lawmakers would ensure higher standards of taxpayer protection and the uniform application of AI risk regulations across the EU and the US for the benefit of tax authorities and taxpayers alike.