



**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. 157

**E-Compliance and Emerging Technologies
in Tax Law: A Comparative Legal Inquiry
between the E.U. and the U.S.**

Amedeo Rizzo

2026

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://ttlfs.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://ttlfs.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 Author

Amedeo Rizzo, MCI Arb, AFHEA, is a Doctor of Philosophy (DPhil) Candidate in Law at the University of Oxford, Exeter College, and Tutor at St Catherine's College, Hertford College, and Oriel College (Oxford) in the UK. He works as an Academic Fellow at Bocconi University and SDA Bocconi School of Management in Italy, where he coordinates the LLM in Global Tax Law and Governance and several research centers, including the Accounting & Tax Policy Observatory (OFC), the AI & Tax Platform, the Transfer Pricing Forum, and the Tax Strategies Project. He is also a Member of the Register of Experts for the course 'International Tax Planning' at Sapienza University of Rome in Italy. He has been a Visiting Scholar of law and technology at the Singapore Management University, Yong Pung How School of Law, and at the University of California, Los Angeles (UCLA).

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. He has previously worked for the European Commission, DG ECFIN, the Centre for Budget and Governance Accountability in New Delhi, India, and several other private and public institutions.

Before earning his D.Phil. in Law from the University of Oxford, Amedeo obtained an M.Sc. in Taxation from the University of Oxford (with distinction), an M.Sc. in Business Administration and Law (summa cum laude) and a B.Sc. in Business Administration and Economics, both from Bocconi University.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:

Amedeo Rizzo, E-Compliance and Emerging Technologies in Tax Law: A Comparative Legal Inquiry between the E.U. and the U.S., Stanford-Vienna TTLF Working Paper No. 157, <http://ttlfs.stanford.edu>.

Copyright

© 2026 Amedeo Rizzo

Abstract

Tax administration increasingly operates through large amounts of data, including structured invoices, third-party reports, platform information, and automated risk analysis. This article defines electronic compliance (e-compliance) as the legally structured use of digital infrastructure to generate, transmit, verify, analyze, and act upon tax-relevant data where the system affects the taxpayer's legal or procedural position. It compares the European Union and the United States through a functional and institutionally sensitive method. The EU analysis combines the supranational framework created by the VAT in the Digital Age package, the Directive on Administrative Cooperation, the GDPR, the Charter of Fundamental Rights and the AI Act with an overview of electronic-invoicing and reporting models across all 27 Member States. The US analysis examines federal information reporting, IRS automation and AI governance, tax confidentiality, the Privacy Act, tax procedure and the continuing diversity of state sales-tax systems.

The comparison shows that the conventional contrast between a rights-oriented EU and an efficiency-oriented United States is too simplistic. EU law provides a more explicit horizontal and *ex ante* framework, but its practical operation varies across national systems and does not protect companies as such under the GDPR. US law contains strong tax-specific protections for confidentiality, notice and adjudication, but its safeguards for upstream data analytics are more fragmented and often more remedial than preventive.

The article identifies three principal developments: enforcement is moving closer to the taxable event; administrative savings may coexist with transferred software, correction and evidential costs; and the central measure of taxpayer protection can be identified with the practical ability to understand, challenge, and correct consequential uses of data. It concludes by proposing a model of accountable compliance by design based on four connected requirements: clear authority and purpose, reliable data and infrastructure, meaningful contestability, and effective oversight and remedy.

Keywords: e-compliance; digital tax administration; taxpayer rights; electronic invoicing; artificial intelligence; data protection; institutional contestability; comparative tax law.

Table of Contents

1.	INTRODUCTION.....	2
2.	LEGAL FOUNDATIONS OF E-COMPLIANCE IN TAXATION.....	7
2.1	DEFINITION OF E-COMPLIANCE.....	7
2.2	E-COMPLIANCE AS A REGULATORY TOOL IN TAX LAW.....	9
2.3	LEGAL PRINCIPLES AND CHALLENGES	11
(i)	<i>Proportionality and Legal Certainty</i>	<i>11</i>
(ii)	<i>Protection of Taxpayer Rights and Data Privacy</i>	<i>13</i>
(iii)	<i>Transparency and Accountability of Tax Administration.....</i>	<i>14</i>
3.	E-COMPLIANCE IN THE EUROPEAN UNION	15
3.1	EU-LEVEL INSTRUMENTS AND COMPETENCES	15
3.2	NATIONAL IMPLEMENTATIONS: AN EU-27 OVERVIEW.....	18
(i)	<i>The Current Implementation Map</i>	<i>19</i>
(ii)	<i>Points of Convergence.....</i>	<i>22</i>
(iii)	<i>Divergence and Peculiar National Configurations.....</i>	<i>24</i>
3.3	INTERACTION WITH THE GDPR AND FUNDAMENTAL RIGHTS.....	26
4.	E-COMPLIANCE IN THE UNITED STATES	30
4.1	LEGAL BASIS IN FEDERAL TAX LAW AND THE INSTITUTIONAL FRAMEWORK	30
4.2	STATE-LEVEL LEGAL APPROACHES TO DIGITAL TAX COMPLIANCE	35
4.3	ABSENCE OF A UNIFIED DATA-PROTECTION REGIME AND LEGAL CONSEQUENCES	37
5.	COMPARATIVE LEGAL ANALYSIS: EUROPEAN UNION AND UNITED STATES	40
5.1	STRUCTURAL AND INSTITUTIONAL DIFFERENCES	40
5.2	LEGAL INSTRUMENTS AND ENFORCEMENT MECHANISMS	42
5.3	TAXPAYER-ORIENTED DESIGN AND PROCEDURAL RIGHTS	43
5.4	ROLE OF E-GOVERNMENT IN REDUCING COMPLIANCE COSTS AND TAX EVASION	47
5.5	LEGAL CHALLENGES AND POLICY PERSPECTIVES.....	49
(i)	<i>Balancing Administrative Efficiency with Taxpayer Rights</i>	<i>49</i>
(ii)	<i>Data Protection and Trust in Digital Tax Administration</i>	<i>50</i>
(iii)	<i>Political Will and Institutional Capacity</i>	<i>51</i>
(iv)	<i>Accountable Compliance by Design</i>	<i>52</i>
6.	CONCLUSION.....	54

1. Introduction

Modern tax administration runs on data. The return remains important, but it no longer monopolises the administration's view of taxable activity. Structured invoices, third-party reports and transactional records increasingly flow through systems capable of validating information, detecting discrepancies and directing scrutiny before a conventional audit begins. This tendency moves tax administration away from episodic, taxpayer-initiated procedures and into the “natural systems” through which individuals and businesses transact, with compliance built into those systems and brought closer to the taxable event. E-compliance is both the vehicle and the accelerator of that transformation. The legal consequence should be a tax system whose accuracy, coercive reach and legitimacy increasingly depend on who controls the data, how those data are interpreted, and whether taxpayers can identify and challenge the conclusions drawn from them.¹

E-compliance is defined in this article as the legally structured use of digital infrastructures to generate, standardize, transmit, verify, match, infer from and act upon tax-relevant data, where the design or mandatory use of that infrastructure affects the timing or content of compliance, the allocation of responsibilities and costs, the taxpayer's informational or evidential position, or the availability of correction and review.²

¹ OECD, *Tax Administration 3.0: The Digital Transformation of Tax Administration* (OECD Publishing 2020) 7, 9-17 and 41-53; OECD, *Tax Administration 3.0 and Electronic Invoicing: Initial Findings* (OECD Publishing 2022) 10-17. The first report articulates the movement towards tax processes embedded in taxpayers' natural systems, built-in compliance and taxation closer to taxable events; the second examines electronic invoicing and continuous transaction reporting as concrete, data-intensive manifestations of that model.

² Roland Ismer, 'Tax Technology for the European Union!' (2023) 32 *EC Tax Review* 234, 235-238; Bruno Peeters, 'Editorial: European Law Restrictions on Tax Authorities' Use of Artificial Intelligence Systems: Reflections on Some Recent Developments' (2024) 33 *EC Tax Review* 54, 54-57.

The practical importance of the category has grown with the movement from periodic returns towards structured invoices, near-real-time reporting, platform reporting, crypto-asset information exchange and large-scale analytics. The European Union's VAT in the Digital Age (ViDA) package now supplies a staged framework for structured electronic invoicing and digital reporting, while DAC8 extends automatic exchange to reportable crypto-assets. In the United States, electronic information reporting has become mandatory at a much lower aggregate threshold, and the Internal Revenue Service has formalized agency-wide rules for the development, procurement and use of artificial intelligence.³ These developments show that legal obligations and administrative knowledge are increasingly embedded in technical systems before a conventional assessment or appeal arises.

The central question is accordingly this: how do the European Union and the United States authorize, structure, constrain and render contestable digital tax-compliance infrastructures, and under what legal and institutional conditions can the movement from episodic, *ex post* enforcement towards continuous, data-driven control improve tax administration without transferring disproportionate informational, evidential, procedural or economic risks to taxpayers and intermediaries?

The proposal from which this article proceeds posited a relatively rights-oriented EU model and a decentralized, efficiency-oriented United States model. However, a close examination supports only a part of that contrast. EU law gives privacy and personal-data protection a constitutional and horizontal form through articles 7 and 8 of the

³ Council Directive (EU) 2025/516 of 11 March 2025 amending Directive 2006/112/EC as regards VAT rules for the digital age [2025] OJ L 2025/516; Council Regulation (EU) 2025/517 of 11 March 2025 amending Regulation (EU) No 904/2010 as regards the VAT administrative cooperation arrangements needed for the digital age [2025] OJ L 2025/517; Council Directive (EU) 2023/2226 of 17 October 2023 amending Directive 2011/16/EU on administrative cooperation in the field of taxation [2023] OJ L 2023/2226; Treas Reg § 301.6011-2; Internal Revenue Service, Internal Revenue Manual 10.24.1, 'IRS Policy for Artificial Intelligence (AI) Governance' (10 August 2026), superseding the revision dated 10 February 2026.

Charter of Fundamental Rights and the General Data Protection Regulation (GDPR). It also subjects Member State action within the scope of EU law to proportionality and effective judicial protection.⁴ Yet tax administration remains predominantly national; article 23 GDPR permits carefully framed fiscal restrictions; data protection does not protect legal persons as such; and rights of access or explanation are of limited practical value when the administration cannot reconstruct the role of a model in a particular case.⁵

The United States has no federal omnibus statute equivalent in architecture to the GDPR. That absence matters, particularly for *ex ante* governance of lawful internal analytics, purpose limitation and model-specific transparency. It is nevertheless inaccurate to treat federal tax administration as an informational free zone. Section 6103 of the Internal Revenue Code begins from the confidentiality of returns and return information; the Privacy Act regulates federal systems of records; section 7803(a)(3) directs the Commissioner to ensure that IRS employees are familiar with and act in accord with taxpayer rights afforded elsewhere in the Code; and deficiency procedure generally interposes notice and a route to pre-payment adjudication before collection of disputed income-tax deficiencies.⁶ These safeguards are sectoral and fragmented. Some are strongest against unauthorized disclosure but weaker where the alleged harm is an inaccurate, opaque or inadequately reviewable use of information within government.

⁴ Amedeo Rizzo and Giorgio Hassan, ‘Proportionate Risk Management for Tax-Related AI Systems: Analysis and Implications under EU and US Law’ (2026) 18 World Tax Journal, no 1, DOI 10.59403/560kfb; Amedeo Rizzo and Giorgio Hassan, ‘Addressing the Use of AI by EU Tax Authorities: Towards a Common Framework of Taxpayer Protection’ (2025) 65 European Taxation 15, 15-29.

⁵ Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, arts 7, 8, 47 and 52; Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1, recital 14 and arts 5, 12-15, 22 and 23.

⁶ 26 USC §§ 6103, 6212, 6213 and 7803(a)(3); Privacy Act of 1974, 5 USC § 552a.

The comparison is therefore organized around institutional contestability, understood as the practical ability of a taxpayer to challenge the role that data or automated systems have played in their case. A system is contestable where the taxpayer can identify that automated processing has influenced the outcome, access and understand the relevant information, correct errors, obtain genuine human reconsideration, and seek an effective remedy where necessary. Contestability does not require complete transparency, such as disclosure of source code or every enforcement criterion. It requires sufficient information and review to ensure that automated outcomes can be meaningfully questioned rather than merely accepted.⁷

Two further analytical tools guide the comparison. First, the article follows tax data through its full lifecycle: generation, transmission, integration, inference, decision, enforcement and redress. This matters because important legal effects can arise before a formal decision is taken. Technical rules may determine which information can be submitted, validation systems may turn data errors into compliance problems, and automated matching or risk-scoring may influence which taxpayers receive further scrutiny.⁸ Secondly, the article examines how the costs and risks of digitalization are distributed. A system may reduce administrative costs while transferring implementation, correction, security or evidential burdens to taxpayers and intermediaries. Administrative savings therefore do not necessarily amount to overall savings.

The comparison is functional, but it remains sensitive to institutional differences. It does not treat the EU and the IRS as equivalent institutions, distinguishing between EU

⁷ Danielle Keats Citron, 'Technological Due Process' (2008) 85 *Washington University Law Review* 1249, 1278-1304; Cary Coglianese and David Lehr, 'Transparency and Algorithmic Governance' (2019) 71 *Administrative Law Review* 1, 42-49.

⁸ Susan C Morse, 'When Robots Make Legal Mistakes' (2020) 72 *Oklahoma Law Review* 213, 217-229; Joshua D Blank and Leigh Osofsky, *Automated Agencies: The Transformation of Government Guidance* (CUP 2025) 47-76.

and US federal rule-making, national tax administrations and the IRS, differences among EU Member States and US states, and the different legal protections that constrain tax administration in each system. This approach allows similar functions to be compared without ignoring the institutional and constitutional settings in which they operate.⁹

The analysis also distinguishes between different types of evidence. Legislation and case law establish legal powers and formal rights. Administrative guidance and technical specifications explain how systems are designed, but do not necessarily create enforceable rights. Oversight reports provide evidence of how institutions operate, while empirical claims about compliance, costs or error require greater caution. Changes in tax gaps or enforcement outcomes cannot normally be attributed to a single technology without considering other legal, economic and institutional factors. This is particularly important in a field that is still evolving: ViDA is subject to staged implementation, the AI Act was amended in July 2026, the IRS adopted new AI-governance rules in February 2026, and Direct File was suspended for the 2026 filing season.¹⁰

The article proceeds in five substantive stages. Part 2 defines e-compliance and identifies the legal principles that should govern it. Parts 3 and 4 examine the EU and US frameworks, including differences among EU Member States and selected US state-level examples. Part 5 compares the two systems directly and develops a model

⁹ Ralf Michaels, 'The Functional Method of Comparative Law' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (2nd edn, OUP 2019) 345, 369-383; Mathias Siems, *Comparative Law* (3rd edn, CUP 2022) 13-25; Jaakko Husa, *A New Introduction to Comparative Law* (Hart 2015) 103-118; Günter Frankenberg, 'Critical Comparisons: Re-thinking Comparative Law' (1985) 26 *Harvard International Law Journal* 411, 411-455.

¹⁰ Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence [2026] OJ L 2026/1744; US Government Accountability Office, *U.S. Department of the Treasury, Internal Revenue Service – Applicability of the Congressional Review Act to the Suspension of Direct File* B-337954 (12 May 2026).

of accountable compliance by design. Part 6 concludes that the initial contrast between a rights-oriented EU and an efficiency-oriented United States is too simple. The more useful distinction concerns where legal safeguards are located and whether they remain effective throughout the lifecycle of tax data.

2. Legal Foundations of E-Compliance in Taxation

2.1 Definition of E-Compliance

“Electronic compliance” may have several interpretations: sometimes it denotes little more than the online fulfilment of an obligation whose legal content remains unchanged; at other times it is used to describe a far more ambitious administrative programme in which tax becomes integrated into accounting, payroll, payment and platform systems. The OECD’s Tax Administration 3.0 project deliberately imagines tax processes that are increasingly embedded in taxpayers’ “natural systems”.¹¹ That vision is important evidence of institutional direction, but it is not a legal definition. “Seamlessness” describes an administrative aspiration: it says little about authority, the incidence of duties, the legal significance of technical rejection, or the route by which a taxpayer may contest an embedded rule.

A useful definition of e-compliance must distinguish digitization, digitalization and infrastructural regulation. Digitization converts existing information into digital form, while digitalization reorganizes administrative processes around digital tools. Infrastructural regulation goes further: the technical system itself becomes part of how tax-relevant information is created, transmitted or acted upon. ViDA illustrates this

¹¹ OECD, *Tax Administration 3.0: The Digital Transformation of Tax Administration* (OECD Publishing 2020) 15-22; OECD, *Tax Administration 3.0 and Connecting with Natural Systems: Initial Findings* (OECD Publishing 2022) 11-19.

distinction by defining an electronic invoice as one issued, transmitted and received in a structured format capable of automated processing, rather than simply as a digital copy of a paper invoice.¹² Structure therefore matters because it allows information to be validated, matched and processed automatically, while also determining which information can be expressed within the system.¹³

E-compliance can therefore be understood as the legally structured use of digital infrastructure to generate, transmit, verify, analyze or act upon tax-relevant data where that process affects a taxpayer's legal or procedural position. This includes electronic filing and payment, electronic invoicing, real-time reporting, third-party reporting, automated matching, risk scoring and automated administrative action. A digital tool used only for convenience falls outside this stronger definition unless law gives it a formal role or attaches consequences to its use.

These forms of e-compliance differ in intensity. Filing portals principally affect how taxpayers communicate and comply. Electronic invoicing and transaction reporting move data collection closer to the underlying economic event and may make technical validation part of legal compliance. Third-party reporting allows information supplied by employers, banks, platforms or other intermediaries to be compared automatically with taxpayer data, raising questions about which source receives practical priority when the information conflicts.¹⁴

A further step occurs when administrations use data to generate inferences. Automated matching, rules engines, statistical risk models and machine-learning tools may all influence which cases receive attention. They should not be treated as a single category

¹² Council Directive (EU) 2025/516, art 5(4), substituting Directive 2006/112/EC art 217.

¹³ Citron, 'Technological Due Process' 1258-1278; Coglianese and Lehr, 'Regulating by Robot' 1189-1203. The graded taxonomy in the text is the article's synthesis.

¹⁴ Leandra Lederman, 'Reducing Information Gaps to Reduce the Tax Gap: When Is Information Reporting Warranted?' (2010) 78 *Fordham Law Review* 1733, 1736-1746; Shu-Yi Oei and Diane M Ring, 'Can Sharing Be Taxed?' (2016) 93 *Washington University Law Review* 989, 1036-1056.

of “AI”: their legal significance depends on what they do, how transparent they are and what consequences follow from their output. The same applies to automated notices, refund holds, assessments or penalties. Even where a system does not formally determine liability, it may materially shape the administrative process and the burdens imposed on the taxpayer.¹⁵ The same applies to automated notices, refund holds, assessments or penalties. Even where a system does not formally determine liability, it may materially shape the administrative process and the burdens imposed on the taxpayer.

The concept is therefore deliberately functional. It does not cover the substantive taxation of the digital economy, nor every proposed use of technologies such as blockchain.¹⁶ Its purpose is narrower: to identify the point at which digital design acquires legal significance. The more a system determines the form of data, accelerates compulsory reporting, produces administrative inferences or generates legal consequences, the stronger the need for clear legal authority, sound data governance and meaningful contestability.

2.2 E-Compliance as a Regulatory Tool in Tax Law

Traditional tax administration separates compliance from enforcement: taxpayers report their liabilities, while the administration audits and assesses where necessary. E-compliance weakens that distinction. Electronic invoices may be validated before delivery, payroll systems can calculate and transmit tax automatically, platforms may

¹⁵ David Freeman Engstrom and others, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies* (Administrative Conference of the United States 2020) 9-18, 75-88; Cary Coglianese and David Lehr, ‘Transparency and Algorithmic Governance’ (2019) 71 *Administrative Law Review* 1, 19-41.

¹⁶ I Lazarov, Q Botha, NO Costa and J Hackel, ‘Reporting of Cross-Border Transactions for Tax Purposes via DLT’ in G Kotsis and others (eds), *Database and Expert Systems Applications – DEXA 2022 Workshops* (Springer 2022) 282-293.

report independently of taxpayers, and risk models can determine which cases receive scrutiny. Compliance is therefore increasingly shaped by digital infrastructure as well as by legal obligations addressed directly to taxpayers.

Technical design consequently acquires regulatory significance. Data formats determine what information can be submitted, validation rules determine what is accepted, and interfaces govern how private systems communicate with tax authorities. These mechanisms can improve accuracy and reduce manual processing,¹⁷ but they are not merely technical details. Where their use is mandatory, they help determine how legal obligations are performed and should therefore be treated as part of the regulatory framework.¹⁸

E-compliance also changes the timing and allocation of administrative functions. Real-time reporting and electronic invoicing bring tax authorities closer to the underlying transaction, while employers, banks, platforms and software providers increasingly perform reporting and compliance functions previously associated with public administration.¹⁹ This may improve efficiency, but it can also shift responsibility and error risk. A taxpayer confronted with incorrect third-party data, for example, may have to resolve an error originating outside their control.

For this reason, claims that digitalisation reduces compliance costs require qualification. A system may save administrative resources while transferring software, reconciliation, correction or evidential costs to taxpayers and intermediaries. The same applies to risk-based enforcement. Algorithms can make case selection more systematic, but their results depend on the data, criteria and priorities on which they

¹⁷ OECD, *Tax Administration 3.0 and Electronic Invoicing* 18-30.

¹⁸ Lawrence Lessig, *Code and Other Laws of Cyberspace, Version 2.0* (Basic Books 2006) 120-137; Citron, 'Technological Due Process' 1258-1264.

¹⁹ Oei and Ring, 'Can Sharing Be Taxed?' 1036-1056; Lederman, 'Reducing Information Gaps to Reduce the Tax Gap' 1773-1791.

are built.²⁰ Even where a risk score does not determine liability, it may determine who bears the burdens of investigation.

It follows that e-compliance should be interpreted as a form of regulatory design operating throughout the tax-data lifecycle. Its principal legal challenge is to preserve the benefits of earlier and more efficient compliance without allowing technical systems to determine obligations, allocate risks or direct enforcement without adequate legal authority, correction mechanisms and meaningful contestability.

2.3 Legal Principles and Challenges

(i) Proportionality and Legal Certainty

Digital tax administration requires a clear legal basis. Reporting duties must be authorised by law, the use of collected data must remain within the permitted purpose, and taxpayers must be able to foresee the legal consequences of non-compliance.²¹ The more intrusive or consequential the system, the stronger the need for specific legal authority. A general power to require electronic filing, for example, should not automatically justify indefinite data retention, reuse for unrelated purposes or fully automated adverse decisions.

EU law expresses this problem through legality, legal certainty and proportionality. A restriction on Charter rights must be provided for by law, respect their essence and, subject to proportionality, be necessary and genuinely meet an objective of general

²⁰ Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 *Georgetown Law Journal* 1147, 1167-1188; David Freeman Engstrom, Daniel E Ho, Catherine M Sharkey and Mariano-Florentino Cuéllar, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies* (Administrative Conference of the United States 2020) 35-54.

²¹ Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, art 52(1); Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1, art 23; 5 USC § 706(2)(C); 26 USC §§ 6001 and 6011; Duncan Bentley, *Taxpayers' Rights: Theory, Origin and Implementation* (Kluwer Law International 2007) 221-246.

interest or protect the rights of others.²² GDPR article 23 similarly permits legislative restrictions for important economic or financial interests, including taxation, but requires a measure which respects the essence of fundamental rights and is necessary and proportionate, accompanied by specific safeguards. In *Valsts ieņēmumu dienests*, the Court did not deny the legitimacy of tax authorities obtaining data from an online advertising service. It insisted that the request remain tied to specified purposes, relevant categories and proportionality rather than becoming an unlimited demand.²³

US law approaches these questions through several overlapping doctrines rather than a single principle. Statutory authority, fair notice, due process and judicial review under the Administrative Procedure Act all help determine whether a digital tax measure is lawful. The central question is whether the law clearly authorizes the obligation and gives the taxpayer a meaningful way to challenge its application. Legislation need not specify every technology used, but it should define the purpose of the system, the consequences it may produce, the responsible authority and the safeguards that apply. Legal certainty also requires clear rules for system failure. Mandatory digital processes can reject filings, record incorrect timestamps or accept technically valid but substantively inaccurate data. The law should therefore determine who bears the consequences of outages, authentication problems and other technical errors. Where electronic compliance is compulsory, alternative channels, safe harbors and reliable audit trails are part of the legal safeguards of the system, rather than matters of administrative convenience.

²² Charter, art 52(1).

²³ Case C-175/20 *SIA 'SS' v Valsts ieņēmumu dienests* EU:C:2022:124, paras 64-66, 70-84.

(ii) Protection of Taxpayer Rights and Data Privacy

Taxpayer protection extends beyond privacy. It also includes data protection, tax secrecy, commercial confidentiality, professional privilege, access to information, correction, reason-giving and effective review. These safeguards protect different interests and are not interchangeable. The GDPR, for example, protects personal data relating to natural persons, not companies as such.²⁴ Yet business tax data may still reveal sensitive information about individuals or commercially valuable information about firms. Where the GDPR does not apply, protection may instead depend on fiscal secrecy, trade-secret law and administrative procedure.

Data protection contributes a set of *ex ante* disciplines. Purpose limitation asks why information is collected and when reuse requires a further legal basis. Data minimization asks whether the fields, population and period are adequate, relevant and limited to what is necessary. Accuracy and storage limitation address error and temporal accumulation. Privacy by design, security and impact assessment translate general principles into system architecture.²⁵ These duties are particularly important in tax systems because data are collected under compulsion and may expose financial, familial and professional relationships. Consent is rarely the relevant legal basis; public-law necessity must carry the justificatory burden.

Confidentiality addresses who may access or disclose tax information. Section 6103 of the Internal Revenue Code provides a strong sector-specific rule, but it does not by itself govern every internal use of data, analytical model or correction process. The GDPR regulates processing more broadly, although its protections may be restricted

²⁴ GDPR, recital 14 and art 4(1).

²⁵ GDPR, arts 5, 25, 32 and 35.

for fiscal purposes and generally do not apply to companies as such. Neither regime therefore provides a complete framework on its own.

Taxpayer protection also includes equality and digital accessibility. Mandatory online systems may disadvantage taxpayers with limited connectivity, disabilities or low digital literacy, while algorithmic tools may produce unequal effects through indirect proxies such as location or occupation. The appropriate response is not to prohibit all differentiation, but to require sound data, accessible alternatives, effective review and evidence that the system serves a legitimate administrative purpose.

(iii) Transparency and Accountability of Tax Administration

Transparency can be interpreted in different forms. Legal transparency concerns the rules authorising and limiting a digital system. Process transparency concerns its general functions, data and institutional responsibilities. Decision-specific explanation tells the taxpayer which facts or inferences materially affected the outcome. Institutional auditability allows an independent body to examine the system's data, performance and safeguards.

This distinction avoids two common mistakes. Publishing source code is not always necessary or sufficient, because the key issue may instead be the data, thresholds or workflow. At the same time, enforcement secrecy cannot justify the absence of accountability. Sensitive risk criteria can remain confidential while still being subject to independent review by courts, supervisory authorities or inspectors.

EU case law gives increasing substance to decision-specific intelligibility. *SCHUFA* treats a score as potentially falling within article 22 GDPR where a third party gives it a determining role in a decision. *Dun & Bradstreet Austria* holds that meaningful information about the logic involved must describe the procedure and principles

actually applied so that the person can understand which data were used and how; the mere provision of an algorithm is not enough, and trade-secret claims do not eliminate review.²⁶ These cases arose outside taxation, and their application to audit selection or decision-support cannot be assumed. They nevertheless support a broader concept of decisional traceability.

Accountability also depends on records. A human official cannot explain or reconsider a system output if the relevant inputs, model version, validation result and intervention are not retained. Procurement contracts should preserve audit access and prevent trade-secret claims from disabling public-law duties. Responsibility must remain allocated even when a vendor supplies the model or an intermediary transmits the data. A public authority may outsource computation; it cannot outsource legality.

Meaningful human review requires more than formal approval of an automated recommendation. The reviewer must be able to access the relevant evidence, understand the system's role and depart from its output where appropriate. Effective review therefore depends on institutional capacity as well as legal rights: safeguards remain largely formal where an administration lacks the staff, records or technical competence needed to apply them in practice.

3. E-Compliance in the European Union

3.1 EU-Level Instruments and Competences

The European Union does not operate a single tax administration or generally control domestic tax procedure. Its e-compliance framework instead combines several areas of EU law, including VAT harmonisation, administrative cooperation, public procurement, data protection, fundamental rights and AI governance. EU law therefore

²⁶ Case C-634/21 *SCHUFA Holding (Scoring)* EU:C:2023:957, paras 56-73; Case C-203/22 *Dun & Bradstreet Austria* EU:C:2025:117, paras 38-50, 56 and 67-76.

sets important common rules and standards, while Member States remain responsible for most digital systems, validation procedures, sanctions and remedies.²⁷

Directive 2014/55/EU provides the EU baseline for electronic invoicing in public procurement. It requires covered public authorities to receive and process invoices that comply with the European standard, but it does not itself require all suppliers to issue electronic invoices. Member States may impose broader supplier-side obligations. EN 16931 therefore creates a common semantic standard, while leaving national transmission systems and mandate design largely separate.²⁸

The VAT in the Digital Age package introduces a clearer path towards EU-wide convergence. It defines electronic invoices as structured data capable of automated processing and requires digital reporting based on e-invoicing for intra-EU B2B transactions from 1 July 2030. Member States with existing domestic real-time reporting systems must align them with the EU framework by 1 January 2035. Hence, ViDA does not immediately replace national systems, but establishes the common model towards which they must progressively converge.²⁹

Three different functions should be distinguished within electronic invoicing. Invoice exchange concerns the structured document sent between supplier and customer; reporting concerns the transmission of invoice or transaction data to the tax authority; and clearance makes the authority or an authorized infrastructure part of the validation

²⁷ Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47, arts 16, 113 and 115; Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, art 51.

²⁸ Directive 2014/55/EU of the European Parliament and of the Council on electronic invoicing in public procurement [2014] OJ L 133/1, arts 3 and 7; Commission Implementing Decision (EU) 2017/1870 on the publication of the reference of the European standard on electronic invoicing and the list of syntaxes [2017] OJ L 266/19. Article 7 imposes the receiving and processing duty on contracting authorities and entities; it does not create an EU-wide supplier issuance duty.

²⁹ Council Directive (EU) 2025/516 amending Directive 2006/112/EC as regards VAT rules for the digital age [2025] OJ L 2025/516, arts 1-7; Council Regulation (EU) 2025/517 [2025] OJ L 2025/517; Council Implementing Regulation (EU) 2025/518 [2025] OJ L 2025/518; European Commission, ‘VAT in the Digital Age (ViDA)’ <https://taxation-customs.ec.europa.eu/taxation/vat/vat-digital-age-vida_en> accessed 10 August 2026.

or issuance process. Member States combine these functions differently. Belgium's decentralized exchange model, Hungary's reporting system and Italy's state-mediated architecture therefore represent distinct forms of e-compliance rather than variations of a single model.

The Directive on Administrative Cooperation adds a separate layer. DAC6, DAC7 and DAC8 extend automatic information exchange to cross-border arrangements, digital platforms and crypto-assets. They do not generally determine whether an invoice is legally valid. Instead, they require intermediaries and service providers to generate information that can be exchanged between national tax authorities, expanding the role of third-party data in tax administration.³⁰

These sectoral rules operate within the wider framework of EU fundamental rights and data protection. The GDPR governs the processing of personal data through principles such as legality, purpose limitation, accuracy, security and rights of access and correction, while the Charter protects privacy, personal data and effective judicial protection. These safeguards constrain digital tax systems, although their application remains subject to the scope of personal-data law, fiscal restrictions and national procedural rules.³¹

The AI Act adds further governance requirements where a tax-administration system falls within its classifications, but it does not create a complete regime for tax analytics. Tax systems are not a separate high-risk category under Annex III, and

³⁰ Council Directive 2011/16/EU on administrative cooperation in the field of taxation [2011] OJ L 64/1; Council Directive (EU) 2018/822 (DAC6) [2018] OJ L 139/1; Council Directive (EU) 2021/514 (DAC7) [2021] OJ L 104/1; Council Directive (EU) 2023/2226 (DAC8) [2023] OJ L 2023/2226; Anne Van de Vijver, Luisa Scarcella and Alessia Tomo, 'DAC8: Track and Exchange of Information on Crypto-Assets as a New Tool to Achieve Tax Compliance' in Marina Serrat Romaní, Jasper Korving and Mariolina Eliantonio (eds), *Exchange of Information in the EU: Taxpayers' Rights, Transparency and Effectiveness* (Edward Elgar 2024) 338-355.

³¹ Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1, arts 5, 6, 12-16, 23, 25, 32 and 35; Charter, arts 7, 8, 47 and 52.

classification depends on the system's intended use. For many validation, matching and risk-selection tools, tax law, the GDPR, the Charter and national administrative law will therefore remain the principal sources of protection.³² The EU model is consequently best understood as common norm-setting combined with decentralized implementation: EU law creates shared standards and safeguards, while Member States retain substantial control over the systems through which they operate.

3.2 National Implementations: An EU-27 Overview

The classification below uses the operative legal effect of each regime, relying on the European Commission country factsheets, which provides a harmonised baseline.³³

Table 1. EU-27 national e-invoicing position in 2026

Status category	Member States	Current legal position	Principal distinguishing feature
Active broad B2B	Belgium; Italy; Poland; Romania	A broad domestic structured-invoice duty is in force.	Decentralized exchange, central transmission, phased national platform and state platform with separate B2C reporting.
Active phased or partial B2B	Croatia; Germany; Greece	The private-sector obligation is operative, but receipt, issuance, taxpayer groups or transactions are phased.	Transition rules form part of the legal architecture, not merely technical grace periods.
Conditional / right to require	Estonia; Finland	No universal issue duty; a qualifying or registered recipient may demand a compliant e-invoice.	Interoperability is organized through a private entitlement.
Future enacted	France; Latvia; Slovakia; Slovenia; Spain	A broad obligation has been enacted but was not yet generally operative at the cut-off.	Dates range from 2026 to 2028; Spain's periods depend on a future ministerial order.
B2G supplier mandate	Austria; Denmark; Lithuania; Luxembourg; Portugal; Sweden	Suppliers must issue structured invoices in covered public procurement; no broad B2B duty.	Federal, threshold, foreign-supplier and transition rules diverge.

³² Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L 2024/1689, recital 59 and annex III; Regulation (EU) 2026/1744. The classification of a tax use remains dependent on the system's intended purpose and function.

³³ European Commission, 'eInvoicing Country Factsheets for each Member State and other countries' (2025-26) <<https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467108874/eInvoicing%2BCountry%2BFactsheets%2Bfor%2Beach%2BMember%2BState%2Band%2Bother%2Bcountries>> accessed 10 August 2026.

Status category	Member States	Current legal position	Principal distinguishing feature
Public bodies receive only	Bulgaria; Cyprus; Czechia; Hungary; Ireland; Malta; Netherlands	Authorities receive/process compliant invoices; no general statutory supplier or B2B mandate.	Contractual duties and tax-data reporting may exist without universal invoice exchange.

The categories do not necessarily constitute a maturity ranking. A State in the public-body-receipt group may have sophisticated tax reporting or digital bookkeeping, while a State with an active B2B mandate may still preserve substantial transitional exceptions. Nor are the categories mutually exclusive in every functional sense: all Member States implement the public-procurement receiving baseline, and many B2B States also maintain separate B2G rules. The classification identifies the additional legal obligation that most clearly distinguishes each system at the cut-off.

(i) The Current Implementation Map

By August 2026, four Member States had broad B2B structured-invoicing mandates in force. Belgium requires domestic VAT-taxable businesses to exchange structured invoices through a decentralised Peppol-based model from 1 January 2026, with ordinary PDFs generally insufficient.³⁴ Italy uses the central *Sistema di Interscambio*, which plays a direct role in transmitting in-scope invoices.³⁵ Poland introduced KSeF progressively in 2026, with temporary relief for the smallest invoice volumes.³⁶ Romania requires B2B invoices to pass through *RO e-Factura* and also imposes

³⁴ Peppol (originally Pan-European Public Procurement On-Line) is an international network and set of technical standards that allows businesses and government organizations to exchange electronic documents – such as invoices, purchase orders, and shipping notices – safely and securely. Belgian legislation: Law of 6 February 2024 amending the Belgian VAT Code, including art 53 §2bis; Belgian Federal Government, ‘Structured electronic invoices between companies are compulsory since 2026’ <<https://einvoice.belgium.be/en/article/structured-electronic-invoices-between-companies-are-compulsory-2026>> accessed 10 August 2026

³⁵ Italian legislation: decreto legislativo 5 agosto 2015, n 127, art 1; Council Implementing Decision (EU) 2024/3150 [2024] OJ L 2024/3150.

³⁶ Poland: ustawa z dnia 5 sierpnia 2025 r, Dz U 2025 poz 1203; Ministry of Finance, ‘Krajowy System e-Faktur’ <<https://www.podatki.gov.pl/ksef/>> accessed 10 August 2026.

separate B2C reporting obligations.³⁷ These systems share a move towards structured transaction data, but differ significantly in architecture, timing and the role assigned to the tax authority.

Croatia, Germany and Greece formed a second group in which the private-sector obligation was operative but phased or partial.³⁸ Croatia's 2026 first stage requires VAT-registered domestic businesses to issue and receive structured invoices, while non-VAT businesses must initially be able to receive them and move to issuance in 2027. Germany adopted an unusual receive-before-issue transition: domestic businesses have had to be capable of receiving a structured invoice since 1 January 2025, but issuers may use transitional alternatives through 2026 and, for smaller businesses, through 2027. Greece introduced mandatory electronic invoicing in stages during 2026, using authorized providers or the *AADE timologio* application and linking exchange to the myDATA environment.

Estonia and Finland do not impose a universal B2B issuance duty. They instead make the recipient's entitlement central. Since July 2025, an Estonian entity registered as an e-invoice recipient may require a compliant electronic invoice. Finnish law gives qualifying businesses a right to request a European-standard electronic invoice, subject to the statutory turnover and transaction conditions. These regimes are important from a legal perspective because they organize interoperability as a private right rather than a universal public order. The supplier's obligation is activated by the recipient's status

³⁷ Romania: Ordonanța de urgență a Guvernului nr 120/2021, as amended; Ministry of Finance, 'RO e-Factura' <<https://mfinante.gov.ro/web/efactura>> accessed 10 August 2026.

³⁸ Croatia: Zakon o fiskalizaciji, Narodne novine 89/2025, especially arts 33-40 and 80; Croatian Tax Administration, 'Fiskalizacija 2.0 / eRačun' <<https://porezna.gov.hr/fiskalizacija/bezgotovinski-racuni/eracun>> accessed 10 August 2026. Germany: Umsatzsteuergesetz, § 14, as amended by the Wachstumschancengesetz; Bundesministerium der Finanzen, 'Fragen und Antworten zur Einführung der obligatorischen E-Rechnung' (March 2026) <<https://www.bundesfinanzministerium.de/Content/DE/FAQ/e-rechnung.html>> accessed 10 August 2026. Greece: Law 4308/2014, art 14, as amended; AADE Decisions A.1128/2025 and A.1044/2026.

or request, and the compliance burden therefore follows commercial relationships rather than a single nationwide commencement date.³⁹

Five Member States had enacted a future broad obligation. France requires all businesses to be able to receive electronic invoices from 1 September 2026; large enterprises and intermediate-sized enterprises issue and e-report from that date, while SMEs and microenterprises follow on 1 September 2027.⁴⁰ Slovakia's domestic VAT mandate begins on 1 January 2027, Latvia's broad B2B date is 1 January 2028, and Slovenia has enacted a 1 January 2028 exchange obligation.⁴¹ Spain has enacted and regulated its architecture, but not a fixed calendar date: businesses above the statutory turnover threshold comply 12 months after the ministerial order governing the public solution enters into force, and others after 24 months.⁴² No final order was identified at the cut-off, so a claimed universal Spanish date would be premature.

Austria, Denmark, Lithuania, Luxembourg, Portugal and Sweden impose supplier-side electronic invoicing in public procurement without a broad private-sector mandate.⁴³ Their scope is not uniform. Austria's longstanding duty is principally federal; Denmark's model rests on *NemHandel* and OIOUBL; Lithuania moved public exchange to SABIS; Luxembourg and Sweden include foreign suppliers to covered

³⁹ Estonia, Accounting Act, as amended with effect from 1 July 2025, provisions on the registered e-invoice recipient's right to require an e-invoice <<https://www.riigiteataja.ee/en/akt/516062025001>> accessed 10 August 2026; Finland, Act on Electronic Invoicing of Contracting Entities and Traders 241/2019 <<https://www.finlex.fi/en/legislation/2019/241>> accessed 10 August 2026.

⁴⁰ French legislation: art 26, loi n° 2022-1157 du 16 août 2022 and art 91, loi n° 2023-1322 du 29 décembre 2023; Direction générale des Finances publiques, 'Facturation électronique' <<https://www.impots.gouv.fr/facturation-electronique-et-plateformes-agreees>> accessed 10 August 2026.

⁴¹ Latvia: Accounting Law amendments of 31 October 2024 and 5 June 2025. Slovakia: Act No 385/2025 amending Act No 222/2004 <<https://static.slov-lex.sk/static/SK/ZZ/2025/385/>> accessed 10 August 2026. Slovenia: Zakon o izmenjavi elektronskih računov in drugih elektronskih dokumentov, Uradni list RS 83/2025, item 3032.

⁴² Spanish legislation: Law 18/2022, final provision 8; Real Decreto 238/2026, final provision 4.

⁴³ European Commission country factsheets for Austria, Denmark, Lithuania, Luxembourg, Portugal and Sweden, cited in n 33; Austria, E-Rechnungsverordnung, BGBl II 505/2012; Denmark, Act No 1203 of 27 December 2003 and Executive Order No 991 of 7 October 2004; Luxembourg, Law of 13 December 2021; Portugal, Decreto-Lei 111-B/2017 and Lei 73-A/2025, art 95; Sweden, Act (2018:1277) on electronic invoices resulting from public procurement.

public bodies; Portugal already covers large suppliers but extends the transition for SMEs, microenterprises and public co-contractors through 31 December 2026. These systems show why Directive 2014/55 cannot be read as the source of one uniform supplier obligation.

Bulgaria, Cyprus, Czechia, Hungary, Ireland, Malta and the Netherlands had transposed the public authority's duty to receive and process compliant invoices but had no general statutory supplier-side or private B2B mandate.⁴⁴ Contract terms may nevertheless require electronic invoicing, especially in central-government procurement. The Netherlands is a clear example: public bodies possess the required receiving capability, while supplier issuance is often generated by procurement conditions rather than a universal legislative command. Hungary is distinctive for the opposite reason. Its NAV Online Invoice system supplies the tax administration with extensive real-time invoice data, yet that reporting architecture must not be misclassified as universal customer-to-customer structured exchange.

(ii) Points of Convergence

The first convergence is semantic. EN 16931 supplies a common data model, while the system implemented by some Member States (UBL, CII, national Core Invoice Usage Specifications, and Peppol) provide recurring implementation routes. Peppol appears in decentralised national networks, public-procurement systems and private-provider ecosystems. It is not, however, an EU clearance platform. Its presence says little by itself about whether a tax authority receives the invoice, whether the invoice is legally

⁴⁴ European Commission country factsheets for Bulgaria, Cyprus, Czechia, Hungary, Ireland, Malta and the Netherlands, cited in n 33; Hungary, NAV, 'Online Invoice' <<https://nav.gov.hu/ado/online-szamla>> accessed 10 August 2026; Ireland, European Union (Electronic Invoicing in Public Procurement) Regulations 2019, SI 258/2019.

valid only after a platform event, or whether a private access point bears responsibility for failed delivery.⁴⁵

A second convergence concerns scope. Most current B2B mandates focus on domestic transactions involving businesses established, resident or fixed in the Member State. Ordinary B2C delivery is usually excluded, although Romania requires B2C data transmission and Italy's infrastructure captures invoiced consumer transactions. Non-established traders often fall outside domestic issuance duties unless they possess a relevant fixed establishment, while foreign suppliers may remain within B2G procurement rules in States such as Luxembourg and Sweden. ViDA's 2030 layer concerns intra-EU transactions; it does not transform trade between the Union and the United States into an EU e-invoicing mandate.⁴⁶

A third convergence is the use of staged implementation. Legislatures distinguish receipt from issuance, large from small businesses, VAT-registered from non-registered persons, or public from private transactions. Transitional rules can prevent sudden exclusion and allow software adaptation. They can also generate legal uncertainty where dates depend on turnover history, invoice volume, future technical measures or repeated postponement. Portugal's succession of public-sector extensions and Spain's order-dependent commencement demonstrate why a current-law account must identify the event which activates the obligation, not merely repeat an announced year.

⁴⁵ Directive 2014/55/EU, arts 3 and 7; Commission Implementing Decision (EU) 2017/1870; European Commission country factsheets, cited in n 33. National Core Invoice Usage Specifications and Peppol profiles implement or constrain the common semantic standard but do not create a single Union clearance network.

⁴⁶ Council Directive (EU) 2025/516; Belgian Federal Government guidance, cited in n 34; France, Direction générale des Finances publiques guidance, cited in n 40; Greece, Decisions A.1128/2025 and A.1044/2026; Luxembourg Government, 'Electronic invoicing' <<https://efacturation.public.lu/en.html>> accessed 10 August 2026; Swedish Public Procurement Agency, 'E-invoicing for suppliers to the public sector' <<https://www.upphandlingsmyndigheten.se/en/public-procurement/e-commerce/e-invoicing-for-suppliers-to-the-public-sector/>> accessed 10 August 2026.

Across the Union, electronic invoicing is consequently moving from bilateral consent towards legally prescribed interoperability. The convergence is, however, bounded. Member States increasingly require structured data and machine processability; they do not yet agree on a single platform, on the degree of tax-authority intermediation, on the relation between invoice exchange and fiscal reporting, or on the territorial and personal scope of domestic rules.

(iii) Divergence and Peculiar National Configurations

The sharpest divergence concerns architecture. Italy, Poland and Romania operate central public infrastructures, although their validation and legal effects differ. Belgium instead uses a decentralised Peppol network in which invoices move between business software systems and the 2026 exchange obligation is not itself a clearance regime. These models all produce structured data, but they allocate outage risk, vendor responsibility, data concentration and correction in different places.⁴⁷

Germany's sequence is peculiar because the duty to receive precedes the universal duty to issue. From 2025 a domestic business must provide at least a technically usable receiving channel, while paper and unstructured invoices remain available under transitional rules for issuers. That structure separates market readiness from full compulsion. It may reduce the coordination problem which arises when an issuer is required to send a structured invoice to a recipient which cannot process it; it also creates a period in which the legal category of invoice varies according to the issuer's size and the transitional date.⁴⁸

⁴⁷ Italy, decreto legislativo n 127/2015; Poland, Act of 5 August 2025, Dz U 2025 poz 1203; Romania, OUG 120/2021, as amended; Croatia, Zakon o fiskalizaciji, Narodne novine 89/2025; Belgium, Law of 6 February 2024 and official guidance, cited in n 34.

⁴⁸ Umsatzsteuergesetz, § 14; Bundesministerium der Finanzen, 'Fragen und Antworten zur Einführung der obligatorischen E-Rechnung' (March 2026), especially questions 2, 11 and 12

Greece departs from the ordinary territorial pattern. Its implementing decisions cover domestic B2B transactions and certain supplies to entities in third countries outside the Union, while excluding intra-EU B2B transactions from the domestic mandate. The system uses authorized electronic-invoicing providers or the public *Timologio* application and connects the invoice process with myDATA. The configuration warns against treating “cross-border” as a single category: third-country sales, intra-EU supplies and domestic supplies can be assigned different transmission rules for reasons which reflect both VAT competence and the anticipated ViDA transition.⁴⁹

France and Spain illustrate two different paths towards platform-based e-invoicing. France has fixed statutory start dates and relies on accredited private platforms linked to the public infrastructure, alongside separate reporting duties for certain B2C and cross-border transactions. Spain also provides for private platforms and a free AEAT solution, but its 12- and 24-month implementation periods depend on a ministerial order that was not yet final at the research cut-off. The Spanish framework is therefore enacted, but its effective dates remain conditional.⁵⁰

Estonia and Finland follow a different model based on the recipient’s right to request a structured invoice. Rather than imposing an immediate universal mandate, these systems give legal significance to the ability to receive machine-readable data and can encourage wider adoption through commercial demand. The trade-off is greater

<<https://www.bundesfinanzministerium.de/Content/DE/FAQ/e-rechnung.html>> accessed 10 August 2026.

⁴⁹ Law 4308/2014, art 14, as amended by Law 5222/2025, art 239; AADE Decision A.1128/2025, arts 1-2; AADE Decision A.1044/2026. The decisions distinguish domestic B2B, specified third-country supplies and intra-EU B2B transactions.

⁵⁰ France, Direction générale des Finances publiques, ‘Facturation électronique’, cited in n 40; Real Decreto 238/2026, arts 7 and 11 and final provisions 3-4; Law 18/2022, final provision 8. The Spanish periods run from the entry into force of the ministerial order governing the public solution, not from the date of the Royal Decree.

complexity for suppliers, which must determine when a recipient is entitled to a structured invoice and which format applies.⁵¹

Finally, invoice exchange must not be inferred from tax reporting. Hungary's NAV system, Spain's SII and VeriFactu rules, and Portugal's SAF-T and invoice-data requirements can give the administration detailed or rapid information without obliging the customer to receive the same structured object. Conversely, Belgium's B2B exchange duty is not yet a near-real-time VAT clearance system. The distinction affects taxpayer rights. A reporting error is contested against the administration; an exchange failure may also disrupt payment, contractual performance and input-tax evidence between private parties.⁵²

The EU-27 landscape therefore seems to reflect a layered rather than uniform process of integration. Public-procurement rules created a common baseline, while Member States adopted different models based on central platforms, decentralised networks, recipient rights, reporting systems and phased mandates. ViDA provides a future point of convergence, but national differences remain important during the transition. Businesses operating across borders must still determine the relevant transaction, parties, establishment rules, format, transmission channel and reporting obligation in each Member State.

3.3 Interaction with the GDPR and Fundamental Rights

The diversity of national systems also affects how common EU rights operate in practice. A lawful basis under the GDPR is only the starting point. Tax authorities and

⁵¹ Estonia, Accounting Act, as amended, and Finland, Act 241/2019, cited in n 39; European Commission country factsheets for Estonia and Finland, cited in n 33.

⁵² Hungary, NAV Online Invoice guidance, cited in n 44; Spain, Real Decreto 596/2016, Orden HFP/417/2017 and Real Decreto 238/2026; Portugal, Decreto-Lei 198/2012, Portaria 31/2019, Decreto-Lei 111-B/2017 and Lei 73-A/2025, art 95; Belgium official guidance, cited in n 34.

their intermediaries must still define the purpose of processing, limit data collection, ensure accuracy and security, assess high-risk processing, and provide rights of information, access and correction subject to lawful restrictions. Where Member States implement EU law, the Charter further requires proportionality and effective judicial protection.⁵³

The object of such protection needs to be precise to be effective. A corporate invoice can contain personal data concerning sole traders, employees, customers or contact persons, but the GDPR does not protect a company as such. Commercial confidentiality, tax secrecy, professional privilege and business autonomy therefore remain necessary alongside data protection. This is especially important in centralized systems which receive line-level descriptions, bank information or commercial relationships at scale. A general statutory power to administer VAT does not answer every question about retention, secondary analysis or access by vendors.

The Italian *Garante*'s 2018 intervention remains a peculiarly instructive case within the wider map. Before general B2B implementation, the authority objected to systematic and generalized processing, excessive storage and the inclusion of information which could reveal health, legal and other sensitive matters. The subsequent measures altered storage and consultation arrangements. The episode does not prove that the final architecture is proportionate in every use. It does show that horizontal supervision can intervene at the level of infrastructure before individual assessments or penalties are issued.⁵⁴

⁵³ GDPR, arts 5, 6, 12-16, 23, 25, 32 and 35; Charter, arts 7, 8, 47 and 52; Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 71-118.

⁵⁴ Garante per la protezione dei dati personali, 'Il Garante privacy all'Agenzia delle entrate: la fatturazione elettronica va cambiata' (16 November 2018) <<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9059957>> accessed 10 August 2026; Garante, Provvedimento n 511, 'Provvedimento in tema di fatturazione elettronica' (20 December

CJEU tax cases reinforce the need to examine the whole information chain. *Valsts ieņēmumu dienests* applies necessity and proportionality to extensive requests for platform data.⁵⁵ *Ispas* requires observance of rights of defense in VAT procedures, while *Berlioz* and the joined Luxembourg information-order cases connect administrative cooperation with effective judicial review.⁵⁶ These authorities do not require disclosure of every anti-fraud technique. They reject the proposition that fiscal purpose places data collection or information orders outside review.

Automated processing creates a further issue: Article 22 GDPR concerns decisions based solely on automated processing which produce legal or similarly significant effects. The SCHUFA case shows that a score can fall within that framework where a recipient gives it a determining role.⁵⁷ At the same time, the Austrian case *Dun & Bradstreet* requires information which makes the procedure and principles actually applied intelligible, rather than source code or a generic description.⁵⁸ In taxation, an audit-selection score may remain upstream of a legal decision, while an automated refund hold, assessment or penalty may be more directly consequential. In line with the substance over form principle, classification must follow function and workflow, not the software's label.⁵⁹

Fiscal secrecy and article 23 restrictions can qualify transparency, access and other rights. The restriction itself must be legislative, necessary and proportionate, and it

2018) <<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069072>> accessed 10 August 2026.

⁵⁵ Case C-175/20 SIA 'SS' v Valsts ieņēmumu dienests EU:C:2022:124, paras 64-66 and 79-84.

⁵⁶ Case C-298/16 *Ispas v Direcția Generală a Finanțelor Publice Cluj* EU:C:2017:843, paras 26-39; Case C-682/15 *Berlioz Investment Fund SA v Directeur de l'administration des contributions directes* EU:C:2017:373, paras 55-59 and 84-86; Joined Cases C-245/19 and C-246/19 *État luxembourgeois v B and Others* EU:C:2020:795, paras 57-79 and 98-112.

⁵⁷ Case C-634/21 *SCHUFA Holding (Scoring)* EU:C:2023:957, paras 56-73.

⁵⁸ Case C-203/22 *Dun & Bradstreet Austria* EU:C:2025:117, paras 38-50, 56 and 67-76.

⁵⁹ Lee A Bygrave, 'Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision-Making' in Karen Yeung and Martin Lodge (eds), *Algorithmic Regulation* (OUP 2019) 248-262.

must satisfy the Regulation's safeguards. Operational confidentiality cannot serve as an excuse for neglecting these principles, as a taxpayer does not need to receive the full risk model to contest an incorrect invoice record or decisive inference: the authority must at least preserve enough data and decisional history for competent administrative, supervisory or judicial review.

Effective remedy is the final safeguard. The *Puškár* case confirms that tax-related data processing can engage privacy and data-protection rights, and that prior administrative remedies cannot make access to judicial protection excessively difficult.⁶⁰ Article 47 of the Charter likewise requires effective review of measures affecting taxpayers. In digital tax systems, that review must also be timely: a later judgment may not fully remedy a rejected invoice, delayed payment or blocked deduction.

The EU is therefore rights-oriented in constitutional form but heterogeneous in operational design, supplying a strong *ex ante* vocabulary: legal basis, purpose, minimization, security, supervision and remedy. However, it does not guarantee equivalent contestability in all 27 systems. Article 23 restrictions, the limited personal scope of the GDPR, divergent technical records, private-platform dependence and unequal institutional capacity can separate rights in law from rights in use.

Overall, it provides the impression that a common rights framework is only effective and evenly applied when each architecture preserves traceable data, correction, meaningful reconsideration, and timely relief.⁶¹

⁶⁰ Case C-73/16 *Puškár v Finančné riaditeľstvo Slovenskej republiky* EU:C:2017:725, paras 62-76 and 89-113; Charter, art 47; *Berlioz Investment Fund*, paras 84-86; *État luxembourgeois*, paras 98-112.

⁶¹ GDPR, art 23; Charter, arts 47 and 52; *Valsts ieņēmumu dienests*, paras 79-84; Bruno Peeters, 'Editorial: European Law Restrictions on Tax Authorities' Use of Artificial Intelligence Systems: Reflections on Some Recent Developments' (2024) 33 EC Tax Review 54, 54-58.

4. E-Compliance in the United States

4.1 Legal Basis in Federal Tax Law and the Institutional Framework

The federal system presents a different legal pattern. Congress has not enacted a single law of digital tax administration. Governance of electronic systems of tax administration arise from separate statutes and administrative instruments.

The Internal Revenue Code begins with broad record-keeping and return obligations. Section 6001 authorizes records and statements required by the Secretary, while section 6011 governs returns and regulations concerning form and manner. Electronic filing mandates have developed through specific statutory authority and Treasury regulations. Final regulations issued in 2023 generally require electronic filing when a person must file at least ten covered returns in the aggregate, replacing the former 250-return threshold measured by return type.⁶² The rule demonstrates a familiar feature of e-compliance: a lower threshold makes digital infrastructure a routine obligation for relatively small filers.

Federal income-tax administration has also long depended on third-party information. Employers, financial institutions, businesses, brokers and payment settlement entities report specified payments under provisions including sections 6041, 6045 and 6050W. Withholding and information reporting reduce the administration's dependence on self-declared data and permit automated matching.⁶³ This is preventive enforcement in an established form. Modern systems increase the speed and scale of matching, but the main legal challenges have been around long before the age of machine learning:

⁶² 26 USC §§ 6001 and 6011; Treas Reg § 301.6011-2; TD 9972, 88 Fed Reg 11754 (23 February 2023).

⁶³ 26 USC §§ 6041, 6045 and 6050W.

reporting thresholds, data accuracy, duplicate or corrected forms, recipient notice and the consequence of inconsistency.

The evidence supporting third-party reporting is stronger than the evidence supporting “AI” as a generic compliance tool. IRS tax-gap studies have repeatedly associated higher reporting visibility and withholding with lower misreporting, supporting the proposition that independent information can materially change compliance incentives and detection capacity.⁶⁴

The statutory confidentiality rule is central in this process. Section 6103 provides that returns and return information shall be confidential except as authorized by the Code. “Return information” is defined broadly and includes data received, recorded, prepared or collected regarding liability and investigation. Civil damages and criminal penalties can apply to specified unlawful disclosures and inspections.⁶⁵ This framework supplies quite a strong tax-specific protection, constraining disclosure to other agencies, private persons and contractors through detailed exceptions and safeguards.

Formal assessment procedure provides another set of safeguards. The IRS is authorized to determine and assess tax, but deficiency procedures generally require notice and allow a timely petition to the United States Tax Court before assessment and collection of the disputed deficiency.⁶⁶ The Independent Office of Appeals is placed on a statutory footing in section 7803(e) of the Internal Revenue Code. Section 7803(a)(3) requires the Commissioner to ensure that IRS employees are familiar with and act in accord with taxpayer rights afforded by other provisions of the Code,

⁶⁴ Internal Revenue Service, *Federal Tax Compliance Research: Tax Gap Projections for Tax Year 2022*, Publication 5869 (Rev 10-2024) (October 2024), 4-5; Leandra Lederman, ‘Reducing Information Gaps to Reduce the Tax Gap: When Is Information Reporting Warranted?’ (2010) 78 *Fordham Law Review* 1733, 1736-1746. The IRS publication reports an association between visibility, withholding and compliance; it does not predict the effect of every additional reporting mandate.

⁶⁵ 26 USC §§ 6103, 7213, 7213A and 7431.

⁶⁶ 26 USC §§ 6201, 6212 and 6213.

including rights to be informed, challenge the IRS’s position, appeal an IRS decision in an independent forum, privacy and confidentiality.⁶⁷

These protections are important but limited. The Taxpayer Bill of Rights does not itself create a general damages remedy for every violation of its principles.⁶⁸ Existing tax procedures are strongest once a formal liability is proposed, but they are less well suited to earlier burdens such as audit selection, refund delays, identity-verification holds or erroneous classifications. As a result, a system focused on reviewing final liability may not expose the data or automated processes that caused the taxpayer to be selected in the first place.

The Administrative Procedure Act (APA) and constitutional due process provide a general public-law background. Judicial review under the APA requires courts to decide relevant questions of law and set aside agency action that is arbitrary, capricious, contrary to law or adopted without required procedure, subject to statutory limits and doctrines specific to taxation.⁶⁹ Pre-enforcement relief can be limited by the Anti-Injunction Act, although the *CIC Services* case confirms that not every challenge to a reporting requirement is a prohibited suit to restrain tax assessment or collection.⁷⁰ Due process can be satisfied by meaningful post-deprivation or pre-payment procedures depending on the tax and context.

The Privacy Act of 1974 regulates federal agency records about individuals maintained in a “system of records” and retrieved by a personal identifier. It limits disclosure, requires agencies to maintain records with appropriate accuracy, relevance, timeliness

⁶⁷ 26 USC § 7803(a)(3) and (e).

⁶⁸ *Moya v Commissioner* 152 TC 182, 196-197 (2019); National Taxpayer Advocate, *Toward a More Perfect Tax System: A Taxpayer Bill of Rights as a Framework for Effective Tax Administration* (2013) 3-18; cf 26 USC § 7803(a)(3).

⁶⁹ Administrative Procedure Act, 5 USC §§ 701-706; *Loper Bright Enterprises v Raimondo* 603 US 369, 391-412 (2024).

⁷⁰ 26 USC § 7421(a); *CIC Services LLC v Internal Revenue Service* 593 US 209, 216-226 (2021).

and completeness when used to make determinations, and provides access and amendment procedures, subject to statutory exceptions and exemptions.⁷¹ Its narrower definitions, exemptions and remedial doctrine prevent it from operating as a US counterpart to the GDPR. In particular, an analytical environment may contain data concerning a person without every model feature or output being retrieved in the manner required by the definition. The Act nevertheless supplies a legal language of record accuracy and correction that is directly relevant to automated administration.

The E-Government Act adds privacy-impact assessment requirements for certain new or substantially changed information systems, while the Federal Records Act and federal cybersecurity law address documentation and security.⁷² OMB memoranda govern agency AI management and procurement across the executive branch, but expressly state that they do not create rights or obligations for the public.⁷³ So, while they are useful to shape inventories, risk management, acquisition and internal accountability, their enforceability by an individual taxpayer remains a separate question governed by other law.

The IRS's current AI-governance policy, IRM 10.24.1, took effect on 10 February 2026 and replaced the March 2025 interim guidance. It applies across the agency and to employees, contractors, vendors and outsourcing providers whose systems process IRS information or connect to IRS systems. It addresses inventories, high-impact AI,

⁷¹ 5 USC § 552a(a)(4)-(5), (b), (d) and (e)(5).

⁷² E-Government Act of 2002, Pub L 107-347, § 208, 116 Stat 2899; Federal Records Act, 44 USC chs 29, 31 and 33, especially § 3101; Federal Information Security Modernization Act of 2014, Pub L 113-283, 128 Stat 3073.

⁷³ Office of Management and Budget, Memorandum M-25-21, 'Accelerating Federal Use of AI through Innovation, Governance, and Public Trust' (3 April 2025) 1-2; Office of Management and Budget, Memorandum M-25-22, 'Driving Efficient Acquisition of Artificial Intelligence in Government' (3 April 2025) 1. Both memoranda state that they do not create rights or obligations for the public.

generative AI, record keeping, taxpayer rights, privacy and security.⁷⁴ The manual is important evidence of the agency's governance structure.

A March 2026 GAO report found 126 active IRS AI use cases in the agency inventory as of June 2025, of which 65 were sensitive or research-and-development uses exempt from public reporting.⁷⁵ Sixty-one per cent were recorded as in development. The report identified weaknesses in inventory quality, skills, coordination and strategic management. Those findings show why institutional capacity is part of legal protection. An agency cannot reliably provide explanation, preserve records, supervise vendors or assess disparate effects if it cannot maintain a complete inventory or retain the necessary expertise.

Different AI uses should be assessed according to their function. Public-facing bots, internal drafting tools, anomaly detection and audit-selection models do not create the same legal risks. A generative tool used to prepare an internal summary may raise confidentiality or accuracy concerns without affecting liability, while a fraud-detection model can influence which taxpayers receive scrutiny. A rules engine that produces a mismatch notice may create an immediate burden even if human review is available later. Treating all 126 IRS AI use cases as one system would therefore obscure important differences in purpose, consequence and required safeguards.

Private vendors may provide models, infrastructure and technical support to the IRS. Section 6103, contractual safeguards and IRS governance rules regulate access to taxpayer information, but confidentiality alone is insufficient. Public accountability also requires documentation, audit access and the ability to explain taxpayer-specific

⁷⁴ Internal Revenue Service, IRM 10.24.1.1-.10 (10 August 2026).

⁷⁵ US Government Accountability Office, *Artificial Intelligence: IRS Actions Needed to Address Skills Gaps, Information Quality, and Strategic Management* GAO-26-107522 (24 March 2026) 17-31, 50-62.

outputs. Proprietary systems should not prevent the IRS, Appeals or a court from examining how a material inference was produced.

The suspension of Direct File illustrates another feature of digital tax administration: political reversibility. Treasury suspended the program in 2025, leaving it unavailable for the 2026 filing season. GAO concluded that the suspension concerned agency organization, procedure or practice rather than changing taxpayers' underlying rights or obligations under the Congressional Review Act.⁷⁶ The episode nevertheless shows that digital services depend on several dimensions, including in particular funding, executive policy, administrative continuity, and legal authority.

The US model is therefore neither purely efficiency-oriented nor comprehensively rights-based. It combines strong tax-specific protections for confidentiality and formal liability with less developed *ex ante* controls over internal analytics. The principal weakness is often limited visibility into upstream automated processes rather than an absence of downstream procedural rights.

4.2 State-Level Legal Approaches to Digital Tax Compliance

State sales-tax administration exposes the decentralised side of the US system. *South Dakota v Wayfair* overruled the physical-presence rule that had prevented states from imposing collection duties on many remote sellers. The Court did not create a national digital compliance system. It restored the ordinary *Complete Auto* framework and emphasised features of South Dakota's law that reduced burdens, including a safe

⁷⁶ US Government Accountability Office, *U.S. Department of the Treasury, Internal Revenue Service – Applicability of the Congressional Review Act to the Suspension of Direct File B-337954* (12 May 2026) 1-13.

threshold, prospective application and participation in the Streamlined Sales and Use Tax Agreement.⁷⁷

Post-*Wayfair* rules vary in thresholds, tax bases, local rates, registration, filing frequency, marketplace-facilitator duties and software architecture. South Dakota currently uses a sales threshold exceeding \$100,000, after removing its transaction-count test. California applies a higher economic-nexus threshold of \$500,000 and is not a full member of the Streamlined Sales Tax project.⁷⁸ These differences can increase compliance cost where sellers must translate similar transactions into multiple legal and technical classifications.

Marketplace-facilitator statutes shift collection and remittance from individual sellers to platforms for covered transactions.⁷⁹ This can reduce the number of small sellers required to interact separately with each state and exploit the platform's existing data. It also creates concentrated private governance, as the platform determines whether a transaction falls within the statute, applies product taxability rules, and reports the result. Sellers may be relieved of one duty while becoming dependent on the platform's classification and records.

The Streamlined Sales and Use Tax Agreement represents a form of “coordinated simplification”. Participating states adopt common definitions and administrative features, provide central registration and support certified service providers.⁸⁰ This arrangement shows that decentralization can lead in some cases to bottom-up standardization. However, this kind of standardization has its limits: participation is

⁷⁷ *South Dakota v Wayfair Inc* 585 US 162, 173-189 (2018); *Complete Auto Transit Inc v Brady* 430 US 274, 279 (1977).

⁷⁸ SD Codified Laws § 10-64-2; Cal Rev & Tax Code § 6203(c)(4).

⁷⁹ See, e.g., SD Codified Laws ch 10-65; Cal Rev & Tax Code §§ 6041-6049.5.

⁸⁰ Streamlined Sales Tax Governing Board, *Streamlined Sales and Use Tax Agreement* (as amended through 14 May 2026), arts III-VIII.

voluntary, major states remain outside, and certified software transfers some costs to private providers rather than abolishing them.

State consumer-privacy statutes do not supply a simple answer to revenue-department data use. Many exclude state agencies or information governed by other laws. Revenue confidentiality and state administrative procedure must be examined jurisdiction by jurisdiction. It would therefore be misleading to infer that the spread of general state privacy legislation has produced a consistent taxpayer-data regime. Federalism supports innovation, but it can also fragment safeguards and remedies.

The state comparison has a close EU analogue: both Member States and US states retain operational autonomy within wider constitutional orders. However, EU VAT harmonization and horizontal data-protection law are more extensive than US coordination of sales taxes, while the Streamlined Agreement can standardize practical administration without a federal tax directive. Therefore, the most relevant comparison is not about what system is centralized or decentralized, as it would be too simplistic. The main comparator is what specific layer is centralized, while also capturing what dimensions are converging and what are diverging.

4.3 Absence of a Unified Data-Protection Regime and Legal Consequences

The absence of an omnibus federal data-protection statute has three principal consequences for e-compliance.⁸¹ First, principles such as purpose limitation, minimisation, and data protection by design do not apply through a single generally applicable taxpayer-facing instrument. Secondly, rights depend on the classification and location of information: return information under section 6103, a record in a

⁸¹ Privacy Act, 5 USC § 552a; Internal Revenue Code, 26 USC § 6103; Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 11-35.

Privacy Act system, material in an administrative file, or evidence relevant to a deficiency. Thirdly, oversight is widely dispersed among different actors, including the IRS, Treasury, OMB, the National Taxpayer Advocate, the Treasury Inspector General for Tax Administration (TIGTA), GAO, Congress, and the courts.

This fragmentation does not necessarily imply weak protection. Section 6103 offers detailed and enforceable confidentiality. The Privacy Act gives individuals access and amendment rights in defined systems. Tax procedure can provide notice and independent adjudication. Inspector-general and congressional oversight can expose institutional failure without requiring an individual lawsuit. A horizontal statute may articulate principles more elegantly, but enforcement depends on institutions and remedies.

The gaps are most visible where processing is lawful, internal, and consequential without becoming the formal basis stated in a notice. Suppose a third-party information return contains an error, a model treats it as a risk indicator and a refund is held for identity or fraud review. Section 6103 prevents unauthorized disclosure but does not itself require a taxpayer-specific explanation. The Privacy Act may help if the relevant record falls within its definitions and no exemption applies, but model features and internal deliberation can complicate access. Deficiency procedure may never arise. The taxpayer experiences a real burden without a single doctrinal pathway matching the entire chain.

Audit selection illustrates the tension between enforcement secrecy and accountability. Tax authorities may legitimately protect detailed selection criteria, but secrecy should not prevent correction of inaccurate data or independent review of unlawful or discriminatory design. A useful distinction is therefore between information that should be public, information that should be explained to the affected taxpayer, and

information that may remain confidential but must be available to a court or oversight body.

US protection is also more remedial than preventive in several respects.⁸² Taxpayers often obtain procedural protection once a notice, assessment or other formal action has occurred. By contrast, the GDPR places greater emphasis on *ex ante* duties such as data minimization, impact assessment and governance. IRS and OMB AI policies move US practice in a similar direction, but their administrative character makes them less durable than statutory safeguards.

Constitutional privacy and due process provide additional protection, but they do not amount to a comprehensive data-governance framework. The strength of the US system instead lies in tax-specific rules on confidentiality, notice and adjudication. Its main form of weakness is that these protections are strongest once a dispute has taken a recognized legal form and less developed during earlier stages such as data collection, risk scoring and automated prioritization.

The initial contrast between an efficiency-oriented United States and a rights-oriented EU seems therefore too simplistic. US law contains significant taxpayer protections, but they are dispersed across different statutes and procedures. The more important problem is fragmented contestability: taxpayers may possess several rights without a clear way to connect them to the data or automated inference that produced the burden.

⁸² Amedeo Rizzo and Giorgio Hassan, ‘On the Distinction Between Tort-Based and Risk-Based AI Regulation: A Transatlantic Perspective’ (Stanford-Vienna Transatlantic Technology Law Forum, TTLF Working Paper No 131, 2025).

5. Comparative Legal Analysis: European Union and United States

5.1 Structural and Institutional Differences

The comparison between the European system and the American shows how each order centralizes different layers. The EU increasingly centralizes legal standards for VAT data, administrative cooperation, personal-data protection and, in some uses, AI governance, while leaving operation and most remedies to Member States. The United States tends to centralize federal income-tax administration in the IRS, but state sales-tax systems remain legally and technically fragmented. Centralization of rules, data, and administration must therefore be assessed separately.

First, this distinction affects accountability. Under ViDA and DAC, the Union legislature can define common reporting structures while national authorities collect, exchange and act upon information. A taxpayer may confront a national portal implementing a Union duty, a data-protection authority applying national law within the GDPR, and national courts capable of referring questions to the CJEU. Responsibility is legally distributed but not necessarily transparent to the user. At federal level in the United States, Congress, Treasury and the IRS occupy a more continuous chain for federal taxes, subject to review by Appeals, the Tax Court and federal courts. That continuity can facilitate standardized operation. It does not eliminate opacity inside a large agency or dependence on contractors.

The horizontal location of rights is another structural difference. EU data-protection principles apply across public and private processing within their scope. Their breadth encourages attention to purpose, minimization and design before an adverse tax decision exists. US safeguards attach more often to a sector or procedural event:

disclosure of return information, maintenance of a system of records, issuance of a deficiency notice or final agency action. The former risks obtaining only formal rights, without proper implementation; the latter might lead to procedural gaps between legal categories.⁸³

Federalism and national autonomy can both generate experimentation. Member States have developed central clearance systems, decentralized Peppol exchange, recipient-entitlement models and reporting-only architectures before ViDA supplies a common future layer. US states developed economic-nexus and marketplace rules after Wayfair, with voluntary coordination through the Streamlined Agreement. Experimentation is valuable when it generates evidence and transferable standards. It can be costly when taxpayers must maintain parallel systems and no institution is responsible for learning across them. The major risk is connected to a lack of overall evaluation, interoperability, and limitation of duplicated burdens.

Institutional capacity is required for an effective implementation of both systems. EU rights require technically capable national administrations and supervisory authorities, while IRS confidentiality and AI policy require accurate inventories, trained staff, and contract oversight. In both orders, legal safeguards can fail through underinvestment. Capacity therefore can determine whether the administrative duties of accuracy, security, reasons, and timely review can be performed.

⁸³ Regulation (EU) 2016/679, arts 5, 12-15 and 25; 26 USC §§ 6103, 6212-6213 and 7522; Privacy Act, 5 USC § 552a; Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 *International Data Privacy Law* 233, 238-242; Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 243, 254-264.

5.2 Legal Instruments and Enforcement Mechanisms

The EU and US systems converge functionally around data-rich preventive enforcement, although they reach it through different taxes and instruments. EU VAT policy increasingly relies on structured transaction data and cross-border exchange. US federal income taxation relies heavily on withholding and third-party information returns, with automated comparison against returns. Both reduce the administration's dependence on a taxpayer's uncorroborated account and move control earlier than a traditional audit.

The difference lies partly in granularity and legal timing. An annual information return supplies a later summary of a payment relationship. Near-real-time VAT ledgers and electronic invoices supply transaction records close to the event. Greater timeliness can improve intervention and make pre-filled or reconciled returns possible. It also increases the number of compliance moments and the possibility that a technical error disrupts ordinary business. The legal system must decide whether rejection, correction and late transmission are administrative events or substantive failures.

Both systems delegate informational functions. DAC7 and DAC8 place due-diligence and reporting obligations on platforms and crypto-asset service providers. US law places information-reporting duties on employers, brokers, payment entities and marketplaces; states often make marketplace facilitators collectors and remitters. Delegation can exploit data already held by sophisticated intermediaries and reduce enforcement cost. It can also transform private classification into public consequence. A platform's error may become the administration's mismatch, while neither institution offers a complete correction route.

The form of legal authority is also important. EU legislation generally specifies who must report, which data are required and how information is exchanged, while technical details are left to implementation. US filing and reporting duties are likewise based on statute and regulation, but AI-assisted selection often relies more heavily on general administrative authority and internal policy. In both systems, transaction reporting is therefore more clearly legislated than inferential enforcement.

Taxpayers may be penalized for failing to transmit information in the required form or time even where the underlying tax is correct. Such penalties may be justified where structured reporting is necessary, but they should not treat outages, technical complexity or vendor failures as equivalent to deliberate non-compliance. EU proportionality and US reasonable-cause or due-process protections provide mechanisms for distinguishing avoidable failure from circumstances outside the taxpayer's control.

Automated administration should also be distinguished from automated enforcement. Field validation, automated matching and audit prioritization all use automation, but they do not have the same legal effect. Safeguards should therefore depend on consequence. Routine validation mainly requires accuracy, notice and easy correction, whereas systems that materially influence adverse outcomes require stronger protections, including traceable records, reasons, meaningful human reconsideration and effective review.

5.3 Taxpayer-Oriented Design and Procedural Rights

A proper way to compare taxpayer protection in the two system might be by following the six-link contestability chain: awareness, access, comprehension, correction, reconsideration and remedy. A system may perform well at one link and fail at

another. The chain is cumulative because a remedy cannot be used effectively where the taxpayer does not know what must be challenged.⁸⁴

Awareness

Transparency differs between the two systems, but the underlying issue is similar. EU law can require information about data processing and certain automated decisions, although fiscal restrictions and investigation secrecy may limit disclosure. US tax procedure often provides detailed notice once an adjustment is proposed, but taxpayers may not know that an automated model influenced audit selection or another preliminary measure.

Neither system should require disclosure of every internal enforcement priority. A stronger rule is to require notice where an automated classification itself creates a significant burden or becomes an important basis for adverse action. At that point, the taxpayer should receive enough information to understand and challenge the role played by the system.

Access

GDPR article 15 provides broad access to personal data and specified information, subject to restrictions and competing rights. CJEU case law on tax files and information orders supports effective access and review in appropriate stages. The Privacy Act provides access to records in covered systems, while tax procedure and discovery can reveal evidence relevant to a dispute. EU access is conceptually broader, but it does not protect a company as such and may not identify the model's role. US access is more fragmented and may depend on whether information is part of a defined record or formal case.

⁸⁴ Citron, 'Technological Due Process' 1278-1304; *Dun & Bradstreet Austria* paras 46-50.

Comprehension

Dun & Bradstreet Austria rejects both a bare algorithm and an unintelligible technical description as sufficient explanation. US law lacks an equivalent generally applicable doctrine for automated tax decisions, but reasoned agency action, statutory notices and evidential fairness can require an intelligible account of the factual and legal basis. In both systems, the correct object is not source code in the abstract. It is the procedure, data and factors that materially affected the individual outcome.

Correction

Data quality is where e-compliance often imposes its heaviest hidden burden. A third-party return, invoice record or identity indicator may be wrong. GDPR rights of rectification and the principle of accuracy supply a general framework, while national tax systems provide correction mechanisms. The Privacy Act has an amendment procedure, and information-return systems allow corrected forms. These routes may be too slow or institutionally divided where one actor created the error and another acted on it. A rights-preserving system should allow the taxpayer to initiate a correction that is propagated to all consequential uses, with a visible status and interim protection against avoidable harm.⁸⁵

Reconsideration

Human intervention is meaningful only if the reviewer can inspect the relevant data, understand the model's function, receive the taxpayer's evidence and depart from the output. EU article 22 GDPR safeguards refer to human intervention in defined cases. The IRS manual requires protection of taxpayer rights and governance for high-impact uses, while Appeals supplies independent review of many tax controversies. The legal

⁸⁵ GDPR, arts 5(1)(d), 16 and 19; Privacy Act, 5 USC § 552a(d)(2)-(3) and (e)(5).

title of the reviewer matters less than the actual capacity and authority. Rubber-stamping can therefore make a formally human process functionally automated.

Remedy

The EU combines data-protection supervision with national administrative and judicial remedies, reinforced by CJEU case law under article 47 of the Charter. The US relies more heavily on tax-specific remedies, including administrative appeals, Tax Court review, refund litigation and Privacy Act procedures. Both systems offer meaningful protection but at different stages. EU law provides stronger ex ante and supervisory safeguards, while US tax procedure offers developed adjudication once a formal dispute arises. Their weaknesses also differ: responsibility may be fragmented across EU institutions and Member States, whereas US remedies can be limited by procedural barriers such as the Anti-Injunction Act, sovereign immunity and classification rules.

This comparison shows why formal data-protection rights are only part of the picture. A right of access has limited value if the administration has not preserved records linking an automated system to the taxpayer's case. Likewise, a well-reasoned final notice may come too late where an automated hold has already caused serious delay. Institutional contestability therefore depends on data protection, tax procedure, record-keeping and technical design working together.

The strongest objection is enforcement secrecy. Tax authorities may reasonably withhold detailed risk indicators where disclosure would facilitate avoidance. The appropriate response is calibrated transparency.⁸⁶ Public information can describe the system's purpose and governance; affected taxpayers should receive enough

⁸⁶ Coglianese and Lehr, 'Transparency and Algorithmic Governance' 42-55; Engstrom and others, *Government by Algorithm* 84-92.

information to understand and challenge the material basis of an adverse action; and courts or oversight bodies should be able to examine sensitive details confidentially. Secrecy may limit disclosure, but it should not prevent independent scrutiny.

5.4 Role of E-Government in Reducing Compliance Costs and Tax Evasion

Efficiency should be assessed across several dimensions: administrative cost, taxpayer compliance cost, speed, detection and substantive accuracy. A digital measure may improve one while worsening another.⁸⁷ Electronic filing can reduce manual processing but increase software costs; real-time reporting can speed up matching while creating more frequent obligations; and AI may improve case selection without improving the accuracy of the final assessment.

The strongest evidence concerns the value of independent information rather than technology itself. Withholding and third-party reporting are associated with higher compliance because tax authorities can compare taxpayer declarations with external data. That does not mean every additional reporting duty is justified. New data requirements should be assessed against their total public and private costs, including implementation, correction, and security.

EU and national authorities identify administrative, interoperability, and anti-fraud benefits from structured invoicing and digital reporting, and ViDA is based on similar expectations.⁸⁸ These materials are useful evidence of policy objectives, legal design

⁸⁷ OECD, *Tax Administration Digitalisation and Digital Transformation Initiatives* (OECD Publishing 2025) 24-36.

⁸⁸ European Commission, 'eInvoicing Country Factsheets for each Member State and other countries', cited in n 33; European Commission, Directorate-General for Taxation and Customs Union, *VAT Gap in Europe: Report 2025* (Publications Office 2025) 16-26; Council Directive (EU) 2025/516, relevant recitals on digital reporting, evaluation and proportionality. These sources establish policy design, legal architecture and reported administrative experience; they do not establish that any particular national system caused a change in the VAT gap.

and reported administrative experience, but they do not prove that a particular system caused an improvement in tax compliance.

Compliance costs are also unevenly distributed. Common standards can reduce cross-border complexity, and ViDA may lower costs by limiting divergent national requirements. During implementation, however, firms must update software, train staff, and manage parallel processes. These fixed costs are easier for large businesses to absorb than for SMEs, which may depend more heavily on external vendors. Therefore, thresholds, phased implementation, and free compliance tools can produce important distributive effects.

The burden-displacement analysis makes these differences visible. Decentralized networks can reduce format fragmentation but increase dependence on software providers; central platforms can simplify transmission while concentrating outage and validation risk; recipient-right models avoid universal mandates but require suppliers to determine when structured invoicing is required. Similarly, US marketplace-facilitator rules may reduce compliance duties for small sellers while transferring significant classification power to platforms. Digitalization rarely eliminates compliance burdens altogether, but it clearly affects who bears them and in what form. Errors should be treated as part of the cost of digital tax administration.⁸⁹ False mismatches, rejected invoices, identity holds, and misclassifications can generate delay, professional fees, as well as liquidity problems. Efficiency assessments should therefore take metrics such as correction times and false positives into account.

Digital exclusion belongs in the same analysis. A mandatory portal may reduce average costs while imposing serious burdens on taxpayers with limited digital access

⁸⁹ Morse, 'When Robots Make Legal Mistakes' 217-229; Citron, 'Technological Due Process' 1264-1278.

or accessibility needs. Assisted services, exemptions and alternative channels should therefore be treated as part of system design rather than as secondary accommodations. The same caution applies to AI. GAO found that many IRS AI use cases were intended to improve efficiency or compliance, but most were still in development and the report identified weaknesses in governance and information quality.⁹⁰ It did not establish the accuracy or distributional effects of individual models. Claims of efficiency should therefore account for error rates, verification costs and whether automation merely shifts work from initial processing to the correction of unreliable outputs. E-government can reduce both compliance burdens and evasion where reliable data support pre-filled obligations, early correction, and common standards. Nonetheless, it can produce the opposite effect where fragmented rules, system errors or opaque models create new costs.

5.5 Legal Challenges and Policy Perspectives

(i) Balancing Administrative Efficiency with Taxpayer Rights

Efficiency and taxpayer rights should not be interpreted as conflicting variables. Clear authority, accurate data, timely correction, and reason-giving can reduce both administrative error and the cost of disputes. Data minimisation may also improve system quality by limiting irrelevant information, while independent review can identify recurring problems before they spread.

Some trade-offs remain. Greater transparency may weaken enforcement, individual review requires resources, and data collected for one purpose may reveal other forms

⁹⁰ US Government Accountability Office, *Artificial Intelligence: IRS Actions Needed to Address Skills Gaps, Information Quality, and Strategic Management* GAO-26-107522 (24 March 2026) 17-31. GAO assessed inventory and governance; it did not assess the accuracy or distributional effects of individual models.

of non-compliance. The law should therefore require authorities to define the objective, use a proportionate design, document remaining risks and provide effective remedies. EU proportionality offers a clear framework for this analysis, while US statutory interpretation and due process can perform a similar function, although less consistently.

Safeguards should be consequence-sensitive and graduated depending on the risk.⁹¹ This prevents procedural protection from making high-volume administration unworkable while refusing to treat scale as a justification for unreviewable harm.

(ii) Data Protection and Trust in Digital Tax Administration

Trust in digital tax administration depends on different factors, which are often only indirectly connected to legislative *dictat*. These factors include institutional competence, predictability, security and effective correction. Confidentiality is essential because taxpayers disclose information under legal compulsion, but it is not enough where data are inaccurate or used opaquely. Likewise, transparency cannot compensate for insecure systems or ineffective remedies.

The EU supports trust through horizontal data-governance rules and independent supervision, while the US relies more heavily on tax confidentiality, procedural safeguards and oversight. Both systems should provide clear information about consequential automated uses, performance and correction mechanisms without revealing sensitive enforcement methods.

Security is therefore fully part of accountability. Centralised tax data and cross-border exchange require strong access controls, incident response, contractor responsibility

⁹¹ Regulation (EU) 2024/1689, arts 6, 9 and 14; OMB M-25-21 6-17.

and effective remedies. A system that is secure but unreviewable is not legitimate; one that is transparent but insecure is not trustworthy.

(iii) Political Will and Institutional Capacity

Political willingness to adopt technology is not equivalent to willingness to finance safeguards. Legislatures often support new reporting powers because expected revenue is visible, while inventories, documentation, accessibility, independent review and legacy-system replacement appear as overhead. That imbalance can produce a system which collects more data than the institution can govern.

The EU's decentralized operation makes capacity uneven. A common Directive can mandate structured data, but Member States differ in procurement, digital identity, staffing, judicial speed and supervisory resources. Harmonized rights do not automatically harmonize implementation. EU evaluation should therefore look beyond formal transposition and consider how digital tax systems operate in practice, including correction times, system reliability, and the effectiveness of available remedies.

The IRS example makes the same point within a central administration. GAO's 2026 findings on inventory quality, skill gaps and coordination show that governance must keep pace with expansion. IRM 10.24.1 supplies an institutional framework, but it will protect taxpayers only if offices identify use cases, classify risk, preserve records and enforce vendor obligations. Direct File's suspension shows that service-oriented systems are politically reversible even where taxpayer duties remain stable.

Institutional capacity also determines whether human review is meaningful. A formal requirement to reconsider an automated output has little value if staff lack the time, access or technical understanding needed to question it. Review must therefore be

properly designed and resourced. The same applies to data-protection authorities, inspectors and courts: independent oversight is effective only where those bodies have sufficient technical expertise to examine how the system actually operates.

(iv) Accountable Compliance by Design

The comparative analysis supports a hybrid model, but not a transplant of one legal order into the other. Importing the GDPR wholesale would not reproduce EU constitutional structure or solve US tax-procedure questions. Importing IRS operational centralisation would not fit the allocation of fiscal competence in the Union. The transferable element is functional: a set of legal gates that must be passed as data move from obligation to consequence.⁹²

- **Gate I: authority and purpose.** Consequential digital systems should rest on sufficiently clear legal authority. Legislation needs not prescribe technical architecture, but it should identify the foundational elements, such as fiscal purpose, persons and data affected, permissible uses, responsible authority and principal safeguards. The greater the scale and consequence of processing, the more specific the legal basis should be. Authorities should also assess whether the data or automation are necessary and whether a less intrusive design could achieve the same objective.
- **Gate II: data and infrastructure.** Tax data should be subject to clear rules on provenance, accuracy, retention, security and correction. Information supplied by third parties should remain contestable, and corrections should reach systems that rely on the same data. Interoperability can reduce compliance

⁹² Michaels, 'The Functional Method of Comparative Law' 369-383; Siems, *Comparative Law* 271-286; Pierre Legrand, 'The Impossibility of "Legal Transplants"' (1997) 4 *Maastricht Journal of European and Comparative Law* 111, 111-124.

costs, but it should be accompanied by limits on access and reuse. Where private vendors are involved, contracts should preserve documentation, audit access, portability and responsibility for error.⁹³ Simplified tools, phased implementation, and assisted channels may also be necessary where uniform digital obligations impose disproportionate burdens on SMEs or vulnerable taxpayers.

- **Gate III: decision and contestability.** Where automated processing materially affects a taxpayer, the administration should preserve enough information to reconstruct how the outcome arose. Notice and explanation should depend on consequence: a routine validation error may require only rapid correction, while a refund denial, penalty or assessment based substantially on automated processing requires clearer reasons and genuine human reconsideration.⁹⁴ Human review must allow the decision-maker to depart from the system's output. Risk scores, third-party reports and technical validation should inform administration without becoming conclusive proof of liability.
- **Gate IV: oversight and remedy.** Digital systems should be subject to inventories, risk assessment, performance testing, incident reporting and periodic review.⁹⁵ Independent oversight bodies must have sufficient technical access to examine consequential systems. Remedies should also match the harm: rapid administrative correction may be necessary where waiting for ordinary litigation would leave a taxpayer with a rejected invoice, delayed refund or continuing data error.

⁹³ OMB M-25-22 5-16; Internal Revenue Service, IRM 10.24.1.4-.10.

⁹⁴ Case C-634/21 *SCHUFA Holding (Scoring)* EU:C:2023:957, paras 60-73; *Dun & Bradstreet Austria* paras 46-50; 26 USC §§ 6212-6213 and 7522(a).

⁹⁵ Internal Revenue Service, IRM 10.24.1.3-.10; OMB M-25-21 6-17; GAO-26-107522 50-62.

The four gates are interdependent. Clear authority cannot compensate for inaccurate data, and accurate data cannot justify an opaque or unreviewable decision. Rights-preserving e-compliance therefore requires legality, data governance, contestability and remedy to be built into the system from the outset. This does not require individual review of every automated transaction. Stronger safeguards should arise where automation begins to produce material legal or economic consequences.

6. Conclusion

Once law makes e-compliance part of administration, its technical design has the potential to reallocate legal power. It may move control closer to the transaction, transfers work to taxpayers and intermediaries, gives practical authority to particular data sources, and dissolve a visible administrative act into a chain of operations. The main question is whether the institutional architecture preserves legality and an effective route to identify and correct consequential error.

From the analysis conducted in this article, the European Union seems to possess a more explicit rights-oriented constitutional framework. The Charter and GDPR supply horizontal principles of proportionality, purpose limitation, minimization, access, security and effective judicial protection. ViDA and the DAC framework also demonstrate a capacity to standardize data and cooperation across national systems. Yet formal rights do not necessarily guarantee effective protection. In the EU, fiscal restrictions, national procedural differences, uneven institutional capacity, and the exclusion of companies as such from GDPR protection leave important gaps. For example, the Italian e-invoicing episode illustrates how independent supervision can shape digital tax infrastructure before individual enforcement occurs. The *Garante*'s

intervention was followed by changes to the storage, consultation, and retention of invoice data.

The United States is more fragmented, but it is not indifferent to taxpayer rights. Section 6103 provides strong confidentiality rules, the Privacy Act governs federal records, and tax procedure offers notice, administrative review and adjudication once a dispute becomes a formal liability. The main weakness seems to lie earlier in the process, where rules on data use, model governance and taxpayer visibility are spread across statutes, OMB policies, the Internal Revenue Manual and oversight mechanisms.

The three main comparative findings can be summarized as follows. First, the timing of enforcement is moving from occasional *ex post* investigation towards infrastructural control, although the extent differs by tax and system. Secondly, apparent administrative savings do not necessarily eliminate costs; they may instead shift them into the design and maintenance of software, the correction of inaccurate information, delays caused by automated checks and the production of evidence needed to challenge an adverse result. Thirdly, the most revealing distinction between legal systems is not the quantity of data collected, but rather the continuity of institutional contestability from source data to remedy.

The broader lesson is that formal rights matter only when they operate together within an institutional process that allows taxpayers to understand, challenge, and correct consequential uses of their data. A right to information is of limited value if the administration cannot identify the data or reasoning behind a decision, just as human review offers little protection if reviewers lack the authority or capacity to question an automated result. Effective accountability therefore requires a continuous route from the initial collection and use of data to explanation, correction and remedy. That route

need not require the public disclosure of sensitive enforcement methods. It requires instead that the administration be able to give affected taxpayers intelligible reasons and that independent bodies be able to examine the system sufficiently to determine whether it is lawful, reliable and fair.

The proposed model of accountable compliance by design therefore contains four gates. Authority and purpose require specific legal power, bounded use and periodic reconsideration. Data and infrastructure require provenance, minimization, quality, security, bounded interoperability and vendor accountability. Decision and contestability require traceability, consequence-sensitive notice, intelligible reasons, genuine human reconsideration and rules on evidential weight. Oversight and remedy require inventories, technical audit, incident accountability, rapid correction and independent relief. These gates should be adapted to the relevant tax and institutional order, not applied as a uniform technological blueprint.

In light of the analysis, legislatures should state more clearly when automated systems may produce or materially influence adverse tax consequences, while administrations should preserve taxpayer-specific decision records and publish correction routes and aggregate performance. At the same time, procurement should guarantee public audit access, and evaluation should measure false positives, correction time, distributional burden, and security as well as revenue and processing speed. EU and US institutions should also separate low-risk service automation from systems that direct investigation or liability, so that safeguards respond to consequence rather than rhetoric about AI.

The trend that is recommended in this article is to build accountability into infrastructure before path dependence turns convenience into unreviewable power, as e-compliance constitutes a sensible path when it improves compliance, enforcement, and the overall relationship between administrations and taxpayers.