Aalto University

POLICY BRIEF
11 November 2026

AI-Driven RegTech for the EU's Digital Rulebook: Large Language Models Powering Compliance Capabilities

Nomi Byström and Adam Leon Smith

Abstract

The surge in the European Union's digital laws has created for companies a legal burden with high compliance costs, straining in particular the capacity of small and medium-sized enterprises (SMEs) to adapt and ensure regulatory compliance. Furthermore, despite the Omnibus simplification packages, the rapid increase in new legislation continues. This Policy Brief studies AI-driven regulatory technology (RegTech) solutions that leverage large language models (LLMs) to support companies' compliance burden with the digital legislation. The Brief is an outcome of the research project AI-Driven Compliance Capabilities: The Impact and Risks of Artificial Intelligence in RegTech and SupTech Solutions (CCRS-AI) which is carried out at Aalto University and funded by the Research Council of Finland, formerly Academy of Finland.

Recommendations to address challenges

1. To support companies with the digital legislation's regulatory burden, the European Union and member states should provide in-depth guidance on the advantages and risks of RegTech tools, in particular those that employ artificial intelligence technologies – from large language models and federated learning to descriptive AI and computer vision. There should also be updated information on available solutions to support Europe's RegTech industry.
2. Addressing hallucinations and leakage of data, for example of trade secrets, requires attention, first, to the kind of platform to be used: when available, a RegTech tool leveraging a purpose-built LLM is recommended. Furthermore, mitigating data leakage and hallucinations requires employment of not only prompt engineering but also broad security guardrails.
3. To support compliance with the GDPR, the European Data Protection Board has published a comprehensive risk management guide with tools to identify, evaluate and mitigate data protection and privacy risks. Moreover, the EDBP has recently released guidelines on anonymisation. Secure IT infrastructure as well as employing privacy enhancing technologies (PETs) also contribute to upholding data protection and privacy.
4. Of paramount significance for companies that utilise LLM-based RegTech solutions is effective – not merely nominal – human oversight of the tools and verification of their outputs.

Keywords: EU's digital legislation, AI-driven RegTech solutions, large language models (LLMs), general-purpose large language models, purpose-built LLMs

Policy briefs offer decision-makers solutions based on research evidence for topical issues in our society. The solutions are recommendations made by the researchers in their role as experts.

Introduction

In the past decade, the increase in the digital legislation of the European Union (EU) has been nothing short of dramatic: from the regulation of cybersecurity and data (personal as well as non-personal information) to online platforms, electronic communications and artificial intelligence (AI). While Regulation 2016/679,[1] better known as the General Data Protection Regulation (GDPR) needs no introduction, of the more recent laws suffice to mention the Cyber Resilience Act,[2] European Health Data Space[3] and Artificial Intelligence Act.[4]

A change to the regulatory surge was anticipated after the 2024 Draghi report and Budapest Declaration, followed by the Competitiveness Compass in January of the following year, all of which paved the way to the European Commission's Omnibus simplification packages.

Significantly, on 19 November 2025, the Commission adopted the Omnibus package VII on Digital. Of the two law proposals included in it, the Digital Omnibus on AI is already law.[5] It introduces amendments first and foremost to the Artificial Intelligence Act, but also to Regulations 2018/1139 and 2023/1230. Changes include new prohibited AI practices, extended timelines, regulatory relief to small mid-cap companies and reducing sectoral overlap.

The second law draft for a Regulation on the Digital Omnibus seeks amendments to the Union's digital acquis with proposed alterations inter alia to the regulation of data, reporting of security incidents and cookie rules.[6] A host of laws are targeted, including the GDPR; Data Act (2023/2854); NIS2 Directive (2022/2555); Platform-to-Business Regulation (2019/1150), Data Governance Act (2022/868) and ePrivacy Directive (2002/58/EC). At the time of writing, the pertinent law proposal is under the co-legislative process.

Furthermore, more changes beyond the Omnibus packages can be expected as on 28 April 2026, the European Commission introduced its Regulatory Deep Cleaning Action Plan.[7]

Nevertheless, at the same time, the surge in new digital legislation has not gone away, on the contrary. Even after the 19 November 2025, there is already a flood of law drafts the development of which will require companies' attention, such as the proposals for a Regulation on Digital Networks;[8] Cloud and AI Development Act[9] and EU Kids Act.[10] And yet more legislation is planned, beginning with the Digital Fairness Act and European Product Act.

To support companies with their compliance burden, there are regulatory technology (RegTech) solutions. A game changer for these tools has been the employment of artificial intelligence in general, and for digital laws, solutions leveraging large language models (LLMs) in particular.

Trained on vast amounts of text, LLMs are deep learning models that generate human-like language.[11] For RegTech purposes, it is useful to distinguish between general-purpose LLMs and purpose-built LLMs. While the former, trained on diverse public texts, offer greater versatility but lower precision; the latter provide limited versatility yet greater area-specific expertise.

For businesses, advantages of employing LLM-based RegTech tools include a major speeding up of compliance, continuous regulatory ingestion, cross-document reasoning as well as a reduction in human effort.

Optimisation of LLM-based RegTech solutions for supporting digital laws requires, first, that their use itself complies with the relevant legislation, notably the Artificial Intelligence Act, and when personal data is processed, the General Data Protection Regulation. Furthermore, the type of LLM that the RegTech tool employs is significant, with purpose-built LLMs standing out at an advantage due to auditability and greater expertise. Additionally, they can be configured to be deterministic to ensure repeatable results. Last but not least, there are risks in the leveraging of the LLM-based RegTech solutions that need to be addressed and mitigated in order for the tools to deliver the sought-after regulatory compliance.

Material and methods

The material for this Policy Brief comes from both published and event sources. The first-mentioned include the EUR-Lex database with access to the authentic Official Journal of the European Union as well documents and publications, first and foremost by the European Commission and the European Data Protection Board (EDPB). The event sources comprise two international roundtable discussions held in spring and summer 2026 with contributions ranging from AI scientists, law professors and lawyers to specialists from the European Commission, representatives of SME organisations and civil servants; and a wide range of businesses: SMEs, large companies and RegTech providers. The roundtable discussions and this policy brief are part of the research project AI-Driven Compliance Capabilities: The Impact and Risks of Artificial Intelligence in RegTech and SupTech Solutions (CCRS-AI) that is carried out at Aalto University and funded by the Research Council of Finland.

Insights

Challenge 1:
There prevails a lack of knowledge of RegTech solutions providing compliance with digital legislation. Companies seeking regulatory support may not even know that such tools exist. And even when businesses are aware of pertinent RegTech solutions, they may have major concerns over the use of these tools due to lack of sufficient and up-to-date knowledge in order to be able to make an informed decision.

Recommendation 1:
To support companies with the digital legislation's regulatory burden, the European Union and member states should provide in-depth guidance on the advantages and risks of RegTech tools, in particular those that employ artificial intelligence technologies – from large language models and federated learning to descriptive AI and computer vision. There should also be updated information on available solutions to support Europe's RegTech industry.

Challenge 2:
RegTech solutions employing LLMs entail risks, such a leakage of data and hallucinations.

Recommendation 2:
Addressing hallucinations and leakage of data, for example of trade secrets, requires attention, first, to the kind of platform to be used: when available, a RegTech tool leveraging a purpose-built LLM is recommended. Furthermore, mitigating data leakage and hallucinations[12] requires employment of not only prompt engineering but also broad security guardrails.

Challenge 3:
The use of RegTech solutions leveraging large language models can also risk data protection and privacy, including by means of data breaches and prompt-based leakages of personal information, leading to non-compliance with the General Data Protection Regulation.

Recommendation 3:
To support compliance with the GDPR, the European Data Protection Board has published a comprehensive risk management guide with tools to identify, evaluate and mitigate data protection and privacy risks.[13] Moreover, the EDBP has recently released guidelines on anonymisation.[14] Secure IT infrastructure as well as employing privacy enhancing technologies (PETs) also contribute to upholding data protection and privacy.[15]

Challenge 4:
Lack of robust human-in-the-loop frameworks is a major risk for companies that use LLM-enabled RegTech tools.

Recommendation 4:
Of paramount significance for companies that utilise LLM-based RegTech solutions is effective – not merely nominal – human oversight of the tools and verification of their outputs.

A warm thank you to all roundtable participants from around Europe and beyond as well as the CCSR-AI team: Professor Robin Gustafsson, Dr. Åke Freij and Doctoral Researcher Anita Golzarjannat.

Contact

Dr. Nomi Byström
Staff Scientist, Project Manager
Aalto University, Department of Industrial Engineering and Management
P.O. Box 15500, 00076 AALTO
nomi.bystrom@aalto.fi

Professor Robin Gustafsson
Aalto University, Department of Industrial Engineering and Management
P.O.Box 15500, FI-00076 Aalto
Tel. +358 50 316 0981
robin.gustafsson@aalto.fi
@robingustafs

References

1 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
2 Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations No 168/2013 and 2019/1020 and Directive 2020/1828, https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.
3 Regulation (EU) 2025/327 of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation 2024/2847, https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng.
4 Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
5 Regulation (EU) 2026/1744 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 (Digital Omnibus on AI), https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng.
6 European Commission, Proposal for a Regulation amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnbibus), COM/2025/837 final, 19 November 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0837.
7 European Commission, Commission proposes plan for simpler, clearer and better enforced EU rules, 28 April 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_901.
8 European Commission, Proposal for a Regulation on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU (Digital Networks Act), COM/2026/16 final, 21 January 2026, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0016.
9 European Commission, Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act), COM/2026/502 final, 3 June 2026, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0502.
10 European Commission, Proposal for a Regulation of EU Kids Act – 'EU Keeping Internet Digital Spaces Accountable and Trustworthy', COM/2026/681 final, 17 September 2026, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52026PC0681.
11 On large language models, see e.g. W. Zhao et al. (2026). A Survey of Large Language Models. Frontiers of Computer Science: 20. https://doi.org/10.1007/s11704-026-60308-3.
12 On mitigating hallucinations, see e.g. P. Pulkundwar et al. (2025) A Concise Review of Hallucinations in LLMs and their Mitigation, arXiv:2512.02527v1.
13 I. Barberá, AI Privacy Risks & Mitigations. Large Language Models (LLMs), 10 April, 2025, European Data Protection Board, https://www.edpb.europa.eu/system/files/documents/2025-04/ai-rivacy-risks-and-mitigations-in-llms.pdf.
14 European Data Protection Board, Guidelines 02/2026 on Anonymisation. Version 1.0., 7 July 2026, https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202602_anonymisation_v1_en_0.pdf.
15 On 15 September 2026, the International Association of Privacy Professionals (IAPP) published a PETs resource repository. See https://iapp.org/resources/article/privacy-enhancing-technology-resource-repository.