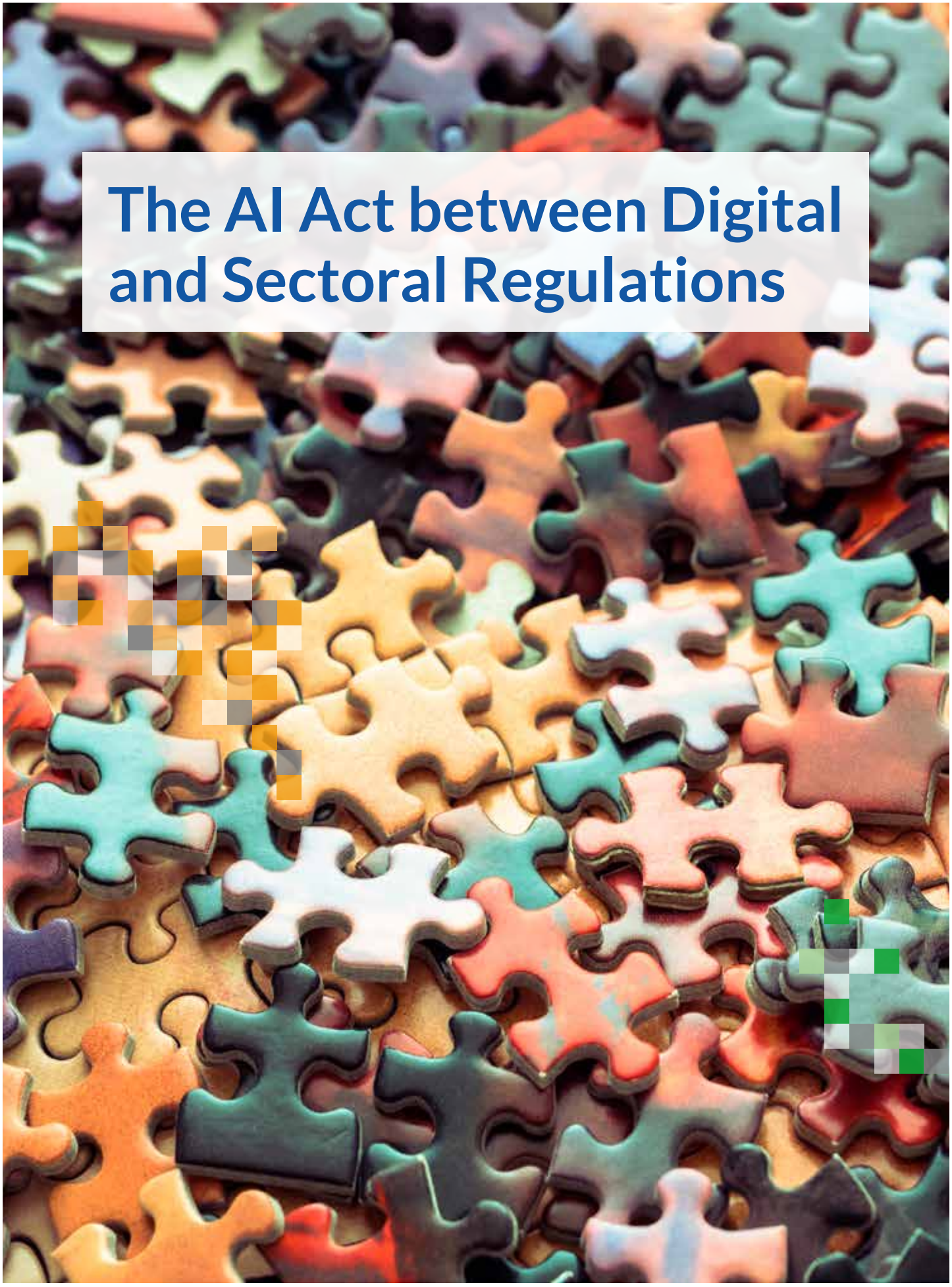
The AI Act between Digital and Sectoral Regulations



BertelsmannStiftung

Imprint

© Bertelsmann Stiftung, Gütersloh
December 2024

Publisher
Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Phone +49 5241 81-0
www.bertelsmann-stiftung.de

Author
Prof. Dr. Philipp Hacker

Responsible for Content
Asena Soydaş

Translation
Rudolf Jan Gajdacz, München

Grafic design
Nicole Meyerholz, Bielefeld

Image Rights
Cover photo: © utoi – stock.adobe.com
Page 7: © Ansichtssache_Britta Schröder

Recommended citation style
Hacker, Philipp (2024). The AI Act between Digital and Sectoral Regulations. Bertelsmann Stiftung. Gütersloh.

DOI 10.11586/2024188

The AI Act between Digital and Sectoral Regulations

Prof. Dr. Philipp Hacker

BertelsmannStiftung

Table of contents

Preface

Europe has taken a decisive step towards regulating AI systems by putting the Artificial Intelligence Act (AI Act) into effect in the summer of 2024. It is the first comprehensive, democratically legitimized set of rules, setting the course for a safer use of AI in compliance with European values. Adding further to completing the puzzle, the AI Act supplements European efforts of recent legislative periods towards making the European Union, and in particular the European single market, "fit for the digital age".

The AI Act will be implemented gradually in the best possible way until August 2026, defining specifically what its requirements mean for practical application. Just like with any complex project, it is already becoming apparent that not all of its parts interlink seamlessly. Inconsistencies, overlaps, and ambiguities may impair smooth implementation and lead to uncertainties that should be avoided.

One central issue is that many laws are considered in isolation upon creation, though they must fit into an overall picture together with other regulations. This is the case with the AI Act as well. Its horizontal approach places it in close connection with existing digital and sectoral regulations. It frequently refers to other legal acts for which practical significance has not yet been fully analyzed, tested, and implemented.

This is not just about legal precision. The effects of the AI Act affect key areas of the economy and society alike. Regulatory inconsistencies may slow down innovation and uncertainties can make the use of new technologies more difficult. Such ambiguities not only may reduce the efficiency of regulation but can even lead to fragmentation in interpretations and responsibilities. At the same time, regulatory arbitrage is possible, with companies exploiting inconsistent requirements to evade stricter requirements. There is much to learn here from the challenges of implementing the General Data Protection Regulation to make the enforcement of the AI Act even more effective.

We must discuss how European digital and sectoral legal acts can be better coordinated in their implementation soon. This issue demands further scientific insight and political debate to ensure both the coherence of regulation and its long-term effectiveness.

We want to address precisely this issue and provide an impetus for the creation of a sound scientific basis with our study in the reframe[Tech] – Algorithms project for the common. We have recruited Prof. Dr. Philipp Hacker from the European University Viadrina Frankfurt (Oder) for a legal analysis. The study provides an initial overview of how the AI Act interacts with available digital regulations such as the General Data Protection Regulation and the Digital Services Act, as well as with sectoral regulations. The current challenges in relation to the AI Act will be highlighted based on the example of selected sectors – the financial, medical, and automotive industries.

Each of these areas exhibits that the need for adaptation and readjustment varies depending on the digital and sectoral legislation.

Nevertheless, common structural actions can be identified across all sectors: In the short term, existing regulations must be better dovetailed in order to avoid duplication and increase efficiency. In the long term, both national and European approaches will be necessary to harmonize AI regulation with other legal acts and to eliminate regulatory inconsistencies in the long term. The regulatory framework should also be subject to regular review to ensure that technological and social developments are adequately considered.

The current time forms a crucial period in which joint effort is required: To be successful, implementation and enforcement of the AI Act requires that all relevant stakeholders in Europe and the Member States – from legislators and supervisory authorities to companies and civil society – work together. Together, we can ensure that this set of rules is more clearly coordinated and takes full effect – for a legally compliant, innovative, and responsible AI landscape.

We would like to thank Prof. Dr. Philipp Hacker for his important contribution to the analysis of the AI Act in the context of digital and sectoral legislation and the participants of the dialog meeting for the in-depth and insightful discussion. We are looking forward to your feedback and, of course, to any form of constructive criticism.

Asena Soydaş
Project Manager
reframe[Tech]
Bertelsmann Stiftung

Martin Hullin
Director Digitalisation and the Common Good
Bertelsmann Stiftung

Executive Summary

This study analyzes the AI Act in the context of existing EU digital regulations and sectoral regulations and identifies the relevant interfaces and potential conflicts. The AI Act, which entered into effect in August 2024, is part of a comprehensive EU regulation of digital technologies, which also includes the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA). The horizontal, risk-based approach of the AI Act is targeted at categorization of AI applications in accordance with their risk potential and creation of strict requirements for particularly high-risk systems. It is not limited to companies in the EU, but also affects companies based outside the EU whose AI systems are offered in the EU or whose output is used there.

Frictions and synergies

The study identifies frictions and synergies between the AI Act and other legal acts:

- **Conflicts with digital regulation:** Several EU legal acts from the digital sector interact with the AI Act in complex manners.

  _ **Frictions with the DSA:** There are some overlaps in the requirements to risk analyses for large platforms (e.g., VLOPs) and generative AI systems subject to both the DSA and the AI Act. Systemic risks are at the focus in both cases, though specific emphasis differs. These analyses should be combined in a smart manner, in particular when hybrid platforms increasingly integrate generative AI.

  _ **Interactions with the GDPR:** There is a systematic tension between the AI Act and the GDPR since the providers of AI systems are primarily liable under the AI Act, while the GDPR holds the operator responsible for data processing. In addition, the AI Act allows the processing of sensitive data in high-risk AI systems to prevent discrimination, which is otherwise prohibited under the GDPR. However, in spite of its great relevance, this exception does not apply to generative AI. Regulation of AI training with personal and sensitive data is, therefore, necessary.

- **Sectoral conflicts:** The AI Act is also in tension with several sectoral regulations, in particular due to its horizontal nature (i.e., cross-sectoral) that transcend existing, specialized regulatory frameworks.

  _ **Financial products (Annex III AI Act):** Credit scoring systems and other AI-based financial applications are heavily regulated already. The AI Act adds additional regulations. While compliance systems are to be explicitly integrated, the relationship between many other regulations that address the same risks is unclear, for example in the area of data governance and model performance.

  _ **Medical devices (Annex I Section A AI Act):** Dual obligations arise under the AI Act and the Medical Device Regulation (MDR), in particular in the case of high-risk AI systems such as cancer diagnosis. These systems are subject to both the

MDR and the strict requirements of the AI Act for risk management and documentation. This may lead to capacity issues for conformity assessment bodies in particular.

_ **Automotive sector (Annex I Section B AI Act):** The traditional assessment method (type approval) remains the central approval procedure for vehicles. It ensures that technical and safety standards are complied with. The AI Act introduces additional requirements only for AI systems that are not classified as high-risk. Such as safety-critical autonomous driving systems, sectoral regulation remains decisive for high-risk systems. Although such systems are exempt from the specific requirements of the AI Act, the sectoral regulations must be adapted in future to take account of the high-risk principles of the AI Act.

Recommendations for action

The AI Act is a horizontal legal framework to supplement sectoral regulations and other digital laws but is insufficiently coordinated with them. This results in recommendations for action for various stakeholders in the short, medium, and long term. These mostly are actions to simplify implementation of the AI Act, clarify tensions, strengthen cooperation, and enable evidence-based evaluations. In this manner, they make it possible to sustainably improve the regulatory environment for AI without lowering the protection of fundamental rights.

1. Short-term actions

- **Designation of a "Lead Act" (European legislator):** A "Lead Act" may be established as the primary legal framework to minimize conflicts between the AI Act and sector-specific regulations. Depending on the sector, this lead act could be the AI Act itself or central sectoral regulations. It is assumed that the requirements of the other regulations are also met, which reduces legal uncertainties if the requirements of the Lead Act are met.
- **Stronger interlinking of regulations (European Commission, in particular AI Office):** The present sector-specific legislation should be linked more closely with the AI Act in order to avoid double regulation. Particularly in the areas of financial services and medical devices, clear boundaries should be defined that specify the requirements of the AI Act in relation to the sector-specific regulations. This interlinking can largely be achieved through implementing regulations without having to amend the AI Act itself. Structurally, Art. 17 (4) AI Act serves as a model here: The paragraph is an example of successful interlinking since it particularly and very specifically regulates the parts of the AI Act that are automatically covered by existing regulatory law and which actions still need to be taken in addition. Unfortunately, this provision is also the only one in the AI Act that offers such clarity and precision with regard to sectoral entanglement. The same applies here: Legislating in this manner may considerably simplify the development and use of AI in the EU without having to make any compromises in terms of the protection of fundamental rights.
- **Definition of practical guidelines and content moderation (European Commission, in particular AI Office):** Guidelines are to be drawn up to show how content moderation can be designed at model level in order to minimize systemic risks, which are also exacerbated by the integration of platforms with generative AI. Such guidelines also are to ensure that moderation does not disproportionately interfere with freedom of opinion and that the diversity of AI results is preserved.
- **Conducting integrated risk analyses (AI Office and Commission supervision of VLOPs/VLOSEs):** Comprehensive risk analyses should be performed to assess both platform-specific and AI-specific risks for large platforms that use generative AI. This requires increased cooperation between the supervisory authorities in accordance with the Digital Services Act and the AI Act.

- **Development of specific guidelines (European Data Protection Board):** Specific guidelines on handling of personal data in AI training are to be developed in order to reduce legal uncertainties in harmonization with the GDPR. These guidelines should contain clear specifications for reuse of such data and be closely coordinated with the AI Office.

- **Institutional integration of supervision (national legislator):** Cooperation between the national AI supervisory authority and sector-specific regulatory authorities should be strengthened, e.g., by seconding experts from sector-specific authorities. They may perform a hinge function and help to provide sector-specific and project-related expertise. Exchange with the AI Office is important at the same time to create a permanent AI Enforcement Hub with corresponding expertise, feedback, and structured learning processes.

- **Setting up a central data access portal (national legislator):** A central portal for accessing AI data is to be created to enable researchers and regulators to more easily monitor generative and high-risk AI systems.

- **Introduction of state scholarship programs (national legislation):** Companies in regulated sectors, in particular small and medium-sized enterprises (SMEs), should be supported by government scholarship programs to better understand and implement the requirements of the AI Act and sector-specific regulations. These programs may, for example, encourage participation in specialized training programs to strengthen operational compliance.

- **Development of detailed guidelines (national supervisory authorities):** National supervisory authorities should develop guidelines on application of the AI Act in specific sectoral contexts. Such guidelines may address the specifics of individual sectors and enable precise handling of the AI Act in interaction with sectoral regulations.

- **Establishment of enhanced cooperation mechanisms (national supervisory authorities):** National AI supervision should cooperate more closely with data protection authorities to ensure coherent implementation of the AI Act and GDPR. Consultations on a regular basis and agreements may reduce friction between the regulations.

- **Establishment of sector-specific expert committees (national supervisory authorities):** Sector-specific expert committees should be established within the national AI supervisory authority. They are to comprise representatives from science, civil society, and industry. These bodies may take sector-specific risks and special features into account when implementing the AI Act.

- **Establishment of overarching technical standards (standardization organizations):** Standardization organizations should develop technical standards that serve as safe harbor mechanisms and meet the requirements of the AI Act and sector-specific regulation. Furthermore, such standards should be developed jointly for the AI Act and the GDPR as well. This may help companies in effectively implementing regulatory requirements in a comprehensive manner.

- **Development of practical guidelines (companies):** Companies should develop codes of practice in accordance with Art. 56 AI Act to promote implementation of the AI Act at sector-specific level and strengthen cooperation between companies and regulators.

- **Clarification of the system (jurisprudence):** Legal scholars should also take a closer look at the systematics of and the relationship between instruments of digital legislation. The principle of special regulation to clarify priority issues (lex specialis) can be used as a starting point here. Such systematization may form a basis for official guidelines or court rulings further down the line.

2. Medium-term actions

- **Greater use of specific references in the legal text (European legislator):** The AI Act should be clarified by way of explicit references to other relevant regulations in order to avoid overlaps and facilitate the coherent application of the legal acts concerned.

- **Harmonization with the GDPR (European legislator):** The regulations in the AI Act and the GDPR should be better coordinated in order to enable the use of personal data in AI models and systems. This is made possible by specific exceptions and links in the AI Act, for which Art. 10 (5) AI Act, which deals with the use of sensitive data for fairness analyses, can be used as a template.

- **Legal framework for AI training (European legislator):** The AI Act should be supplemented by an explicit exception for the use of data for training purposes with corresponding safeguards, similar to the existing text and data mining exception in copyright law, in the medium term.

- **Content moderation at model level (European legislator):** The Digital Services Act should be expanded to intend for trusted whistleblowers to report malicious prompts and illegal AI outputs to comprehensively cover platform and AI-specific risks.

- **Linking of implementing laws (national legislator):** The national implementing laws for the AI Act, the Digital Services Act (DSA) and the GDPR should be better linked in order to create synergies, particularly in the area of data access and risk management.

3. Long-term actions

- **Evaluation of AI Act regulation (European legislator):** The AI Act should be fundamentally evaluated externally and revised after an appropriate period of application. This version may, for example, combine liability rules, rules for base models and transparency requirements, possibly without considering the specific procedural and substantive rules for high-risk AI (e.g., Art. 8 to 27 AI Act), and thus ensure more flexible compliance in high-risk areas.

- **Supervisory architecture (national legislator):** Cooperation between the sectoral and AI-specific supervisory authorities should be institutionalized in the long term and embedded in a clear legal framework. This framework must define responsibilities, communication channels, and decision-making processes in order to ensure coherent and efficient monitoring.

- **Development of a framework for cooperation and evaluation (supervisory authorities):** The supervisory authorities should introduce evidence-based mechanisms to evaluate their cooperation. This framework is to permit regular evaluations of the collaboration based on defined criteria such as speed, consistency, and completeness of the exchange of information. Evaluations results are to be applied to continuously adapt and optimize the cooperation structures and processes in order to increase the efficiency and impact of supervision in the long term.

It is to be hoped that the AI Act will be implemented more efficiently, regulatory conflicts will be avoided, and innovation in the EU will be strengthened at the same time thanks to these actions.

List of abbreviations

OJ	Official Journal
Para.	Paragraph
ADS	Automated Driving System
AI	Artificial Intelligence
Art.	Article
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority)
BDSG	Bundesdatenschutzgesetz (German Federal Data Protection Act)
BNetzA	Bundesnetzagentur (Federal Network Agency)
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CENELEC	Comité Européen de Normalisation Électrotechnique (European Committee for Electrotechnical Standardization)
CRA	Cyber Resilience Act
CRD	Capital Requirements Directive
CRR	Capital Requirements Regulation
CTR	Clinical Trials Regulation
DMA	Digital Markets Act
DORA	Digital Operational Resilience Act
DSA	Digital Services Act
GDPR	General Data Protection Regulation
ENISA	European Network and Information Security Agency (European Union Agency for Cybersecurity)
EU	European Union
ECJ	European Court of Justice
FDA	Food and Drug Administration
GDNG	Gesundheitsdatennutzungsgesetz (German Health Data Utilization Act)
GPAI	General-Purpose AI Models (generative AI technologies)
IVDR	In Vitro Diagnostic Medical Devices Regulation
SMEs	Small and Medium-sized Enterprises
KWG	Kreditwesengesetz (German Banking Act)
MaRisk	Mindestanforderungen an das Risikomanagementsystem (Minimum requirements for the risk management system)
MDR	Medical Device Regulation
StVZO	Straßenverkehrs-Zulassungs-Ordnung (Road Traffic Licensing Regulations)
VLOPs	Very Large Online Platforms
VLOSEs	Very Large Online Search Engines

I. Introduction

The AI Act, which entered into effect on 08/02/2024,[1] is at the heart of the debate on the legal framework for artificial intelligence (AI). However, this at times neglects to consider the fact that it has not entered a legal vacuum. In fact, products that use AI have been subject to regulation for a long time – through sector-specific instruments, technology-neutral legislation, and, most recently, additional digital laws. The EU has adopted a number of important legal acts to promote the supervision of digital technologies and to address key risks by law in the last few years. The main instruments include the General Data Protection Regulation (GDPR),[2] the Digital Services Act (DSA)[3] and liability law for AI.[4] Furthermore, banking, medical devices, and automotive law are particularly relevant in the sectoral area. Each of them responds differently to digital developments. All of these regulations are aimed at developing a balance between technological innovation and the protection of fundamental rights and competition.

The AI Act now pushes into this regulatory structure by pursuing a horizontal, risk-based approach. It classifies applications of AI systems and certain general-purpose AI models (e.g., GPT-4) in accordance with their risk potential for society, with particularly high-risk systems subject to strict regulations (e.g., in medicine, lending or personnel selection). Its range should not be underestimated: It applies not only to companies based in the EU, but also to those based outside the EU, provided that their AI models are offered in the EU or their results are used in the EU. The GDPR has a similar global effect.

A central matter in the regulation of artificial intelligence from a scientific and practical perspective, which has not yet been sufficiently highlighted in the debate to date, is the interface between the AI Act and existing sector-specific and digital regulations. These interfaces must be clearly named and addressed in order to avoid the exploitation of loopholes (regulatory arbitrage) and to ensure greater legal certainty for companies and users. This is the only manner in which it can be ensured that innovation is not hindered by unnecessary bureaucracy, while at the same time maintaining high standards for fundamental rights.

This study thus is aimed at examining legal overlaps, gaps, and synergies of the AI Act with existing regula-

1 Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13th, 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation), OJ L, 2024/1689, 07/12/2024, http://data.europa.eu/eli/reg/2024/1689/oj.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th, 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 (General Data Protection Regulation), OJ L 119, 05/04/2016, p. 1, http://data.europa.eu/eli/reg/2016/679/oj.

3 Regulation (EU) 2022/2065 of the European Parliament and of the Council of October 19th, 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 10/27/2022, p. 1, http://data.europa.eu/eli/reg/2022/2065/oj.

4 This applies in particular to the revised and now adopted Product Liability Directive and the proposal for an AI Liability Directive, see, for example Wagner 2022; Hacker 2023; De Bruyne, Dheu and Ducuing 2023; Novelli et al. 2024.

tions based on case studies (Section II.). Overarching findings (Section III.) and finally specific recommendations for action (Section IV.) are derived from this. They are to contribute to increasing regulatory coherence, proactively protecting fundamental rights, and promoting innovation.

II. AI Act and digital laws

The AI Act, like many other pieces of legislation, starts out by dutifully emphasizing that it does not affect certain related pieces of legislation, such as the General Data Protection Regulation (GDPR) and the parts of the Digital Services Act (DSA) on the liability of intermediary service providers. However, the fact that the AI Act so matter-of-factly takes a step back does not solve the factual issues at the intersection of the AI Act and other digital regulations in any way, form, or manner; rather, it merely highlights the tense relationship with the above and other legal acts. These overlapping areas and the resulting challenges, but also opportunities, will be explored below.

We will particularly discuss the DSA and the GDPR discussed. It largely omits liability law and the Digital Markets Act (DMA) in its entirety. First, this sets a significantly different focus with competition law regulations, as it is not aimed at the governance of AI. It also primarily affects gatekeepers in the e-commerce and search engine sectors. However, these areas are not designated as high-risk applications by the AI Act, which limits overlaps.

The AI Act also is not complete yet. In contrast to the other digital laws, the provisions of the AI Act are to be further specified through so-called technical standards. These are standards that are drawn up by expert committees, for example by the European standardization organization CEN/CENELEC. These standards are currently under development and meant to be published at the latest by early/mid-2026. They offer further definitions of key terms or describe procedures and, in some cases, specific quantitative thresholds that are intended to translate undefined legal terms for AI developers and providers and enable implementation, amongst other things.

It is assumed that the corresponding standard of the AI Act is also met (Art. 40 (1) AI Act) if these standards are met. Properly put, they thus may offer a kind of “safe harbor” for AI developers and users. We are going to return to this matter in the recommendations for action.

Safe Harbor mechanism

A Safe Harbor mechanism is a legal framework that offers companies or organizations legal certainty in various regulatory areas. It works as follows:

1. ***Definition:*** The legislator or a regulatory authority defines some specific criteria or behaviors.
2. ***Voluntary compliance:*** Companies may decide to fulfill these criteria on a voluntary basis.
3. ***Legal certainty:*** A company that can prove that it meets all the criteria of the Safe Harbor is automatically deemed to be legally compliant in the relevant area.
4. ***Flexibility:*** Use of a safe harbor is optional. Companies may also achieve legal compliance in other ways.
5. ***Examples:*** Safe Harbor regulations can be found in various areas of law, e.g., in data protection and capital market law.

The advantage of a safe harbor lies in the creation of clear guidelines and the reduction of legal uncertainties. It offers a "safe harbor" for companies that comply with the specified rules but does not rule out alternative ways of complying with the law.

1. Digital Services Act

The Digital Services Act (DSA) and the AI Act overlap in a number of areas. However, there are also some clear demarcations and gaps between the two sets of regulations. This begins with the technologies and systems covered.

While the DSA primarily regulates the obligations of online platforms and online search engines (in particular Very Large Online Platforms, VLOPs, and Very Large Online Search Engines, VLOSEs), the AI Act focuses on regulation of specific risk and development categories of artificial intelligence (e.g., high-risk AI and general-purpose AI models, GPAI). The AI Act uses the term of "general-purpose AI" to mean broadly applicable models, such as generative AI models like ChatGPT, Claude, Gemini, and the like.

The direction of travel also appears to differ considerably at first: The AI Act addresses specific AI risks such as lack of transparency, discrimination, unpredictability, and autonomy. It establishes guidelines for sufficient performance, robustness, and IT security and tries to reduce information asymmetries along the AI value chain and between providers and authorities. This is in line with the product safety law approach of protecting the market and those affected by potentially dangerous, low-quality products by means of specific requirements.

The DSA, in contrast, is not concerned with the quality of the platforms as such; instead, it uses these intermediaries as a gateway to gain better access to illegal or otherwise risky content shared on these platforms and to prevent its distribution in the interests of society as a whole. The actual requirements for this content (in particular in cases of illegality) are not found in the DSA itself, but in various special laws, some of them European, some of them national (e.g., criminal code, youth protection law).

However, both legal acts have a strong procedural component in common: Both encourage the respective regulatory addressees – platforms and AI provid-

ers/operators – to set up compliance systems in order to reduce certain risks for individuals and the general public. This indicates an important intersection. In accordance with both legal acts, the regulatory addressees not only need to conduct risk analyses after the damage has occurred (ex post), but even beforehand (ex ante) in order to take appropriate actions to minimize these risks – if possible before they have materialized.

a | Access areas: VLOPs/VLOSEs vs High-Risk/GPAI

The areas of application and objectives of the two laws thus are not congruent. Nevertheless, there are some overlaps, in particular with hybrid platforms that act both as VLOPs/VLOSEs in the sense of DSA and integrate generative AI into their platform. This is an extremely relevant phenomenon both economically and legally – and in both cases, systemic risk analyses are mandatory.

VLOPs and VLOSEs such as Google, Meta, Microsoft, LinkedIn, or X/Twitter[5] have been using classic AI in their services for some time to answer user queries and create rankings. These AI applications, however, are outside of the high-risk area of the AI Act, as this generally excludes e-commerce and search engines. More recently, however, it has been observed that large providers are integrating generative AI into their traditional search function, in particular in the area of online search (search). This can be observed with Bing, Google, or X (formerly Twitter).

5 https://digital-strategy.ec.europa.eu/de/policies/list-designated-vlops-and-vloses.

VLOPs and VLOSEs in the Digital Services Act (DSA)

The Digital Services Act introduces special categories for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) that are subject to particularly strict regulations:

1. ***Definition:***
   - VLOPs: Online platforms with an average of more than 45 million active users per month in the EU
   - VLOSEs: Online search engines with an average of more than 45 million active users per month in the EU

2. ***Classification:*** The EU Commission designates platforms and search engines as VLOPs/VLOSEs based on the reported user numbers. Providers must update the figures every six months.

3. ***Additional obligations:*** VLOPs/VLOSEs must adhere to the strictest rules of DSA, including:
   - Regular assessment of systemic risks (Art. 34 DSA)
   - Taking risk mitigation actions (Art. 35 DSA)
   - Conducting independent compliance audits (Art. 37 DSA)
   - Establishment of an independent compliance department (Art. 41 DSA)

4. ***Supervision:*** The EU Commission supervises compliance with the DSA obligations by VLOPs/VLOSEs.

5. ***Named VLOPs and VLOSEs:*** For example, the EU Commission has officially classified the following services as VLOPs or VLOSEs:
   - VLOPs: Amazon Marketplace, Apple AppStore, Booking.com, Facebook, and Instagram, Google Play, Google Maps, LinkedIn, X/Twitter
   - VLOSEs: Bing, Google Search

The DSA creates a risk-based regulatory framework that considers the special challenges and effects of very large platforms and search engines with the special rules for VLOPs/VLOSEs.

Generative functions are also increasingly being used in other VLOPs, for example to generate, rewrite or illustrate posts (Facebook, LinkedIn). However, such new AI models regularly qualify as generative AI technologies (GPAI) within the meaning of the AI Act, and therefore are subject to specific obligations. Art. 53 of the AI Act contains provisions on transparency and copyright for GPAI models, for example, and Art. 55 of the AI Act requires the review and reduction of systemic risks for particularly powerful GPAI models.

The obligations of the Digital Services Act (DSA) thus are combined with the requirements of the AI Act for hybrid platforms that use both traditional and generative AI, which poses new challenges for the classification and regulation of such platforms.

b | Systemic risk analysis

A central interface between the Digital Services Act (DSA) and the AI Act is the obligation to perform systemic risk analyses. Both sets of regulations stipulate that specific risks arising from digital platforms or AI systems must be identified, assessed, and mitigated on a regular basis. These requirements are particularly relevant for hybrid platforms that function both as large online platforms in the sense of DSA (VLOPs/VLOSEs) and integrate AI systems.

(1) Systemic risks under the AI Act and DSA

Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) must analyze systemic risks arising from the use of their platforms under the DSA. Such risks include dissemination of illegal content, undermining of democratic processes through misinformation, impairment of freedom of expression, health, public safety, and protection of users' privacy (Art. 34 (1) DSA). Platform operators are obligated to take actions to minimize these risks and to regularly review the effectiveness of these actions (Art. 35 DSA).

The AI Act also requires providers of large generative AI models (GPAI with systemic risks) to identify, assess and mitigate systemic risks arising from the use of such AI (Art. 55 (1) AI Act).[6] This includes risks to health, safety, fundamental rights, and environmental protection. In particular, if these systems are used on a large scale or in sensitive contexts and the risks can be passed on along the AI value chain, the threshold for systemic risks is quickly reached (Art. 3 (65) AI Act).

Although both cases refer to systemic risks, the emphasis on the legal acts differs slightly. The DSA places greater emphasis on freedom of information, while the AI Act focuses on public health and safety. All specific risks to any fundamental rights arising from the use of the respective technology (large platform; AI) generally must be analyzed in both cases, however.

(2) Consolidated and cross-technology risk analysis

The obligations under the DSA and the AI Act overlap at least in part in the cases of hybrid platforms that use generative AI technologies (e.g., Bing with embedded generative AI, LinkedIn with AI-enhanced posts, or X with AI-generated content). Based on the view expressed here – which has hardly been investigated so far – the fact that one technology is linked to the other should be considered in the risk assessment of one technology.

Generative AI should not only be examined for typical systemic risks such as bias or discrimination in the information generated under the AI Act. It must also be considered that such distorted content or other risks can be spread even more widely by connecting AI with large platforms. For example, the fact that the results provided by the AI model that Bing is based on are integrated into a classic Internet search must be considered when examining its systemic risks.

Vice versa, the DSA should examine the scope at which use of such AI technologies influences the systemic risks of the platform as a whole, e.g., with regard to the dissemination of false information or the protection of freedom of expression. This ap-

6 Art. 9 (1) AI Act, which provides for similar obligations, applies to high-risk providers.

plies, amongst other things, to use of conventional, but in particular to generative AI on platforms such as Facebook, X/Twitter, but also LinkedIn.

These interconnections make an integrative, comprehensive risk analysis appear sensible (reciprocal risk analysis). This kind of analysis should include three things: 1) the platform-specific risks that the DSA focuses on, 2) the AI-specific risks that the AI Act addresses, and 3) additionally the effects resulting from technological entanglement. This permits bundling of all key items into a consolidated process.

Reiterating the focus point: It is particularly important in the context of this reciprocal, cross-technology risk analysis that the use of generative AI is considered in the risk assessment in accordance with the DSA. After all, this may create new systemic risks for the platform. Vice versa, the AI Act risk analysis must also consider the fact that AI is used on a large platform, which increases the spread of AI spending and its potential risks.

Providers must reduce these risks. The actions taken for this must then reflect this interlocking and its reinforcement potential. For example, it may be insufficient to simply enrich the training database with various data points and implement filters to reduce discriminatory results; efforts must also be made to reduce the range of such AI results on the platform. The reasonable effort required to manage the risk of AI and platform is therefore generally higher than if the technologies were used in isolation (identical AI without a platform or the identical platform without generative AI).

Such a consolidated analysis would ensure that both the systemic risks of the platform and the risks caused by the use of AI are assessed holistically and mitigated effectively.

c | Access for scientists: Art. 40 (8) DSA

Another key difference between the Digital Services Act (DSA) and the AI Act concerns access to data and models by researchers. Art. 40 (8) of the DSA grants researchers who receive a verified status (vetted researchers) a right of access to data from Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs).[7] This access is used to monitor compliance with the provisions of the DSA and to analyze systemic risks, such as spreading of illegal content, false information, or detrimental effects on fundamental rights. This regulation at least theoretically represents an important action to increase transparency and enable independent research in the field of digital platforms.

However, there is no comparable mechanism in the AI Act, which does not contain any explicit provisions regulating access to data for the review of AI systems by researchers. This gap makes it difficult to gain independent, science-driven, or civil society-driven insights into the functioning of AI systems. This significantly restricts transparency and the ability to review risks externally. In particular, this may be an issue since many hybrid platforms act as both VLOPs/VLOSEs and Generative AI (GPAI) providers, which requires a detailed risk assessment for both aspects, independent of the respective provider.

Researchers potentially using the provisions of Art. 40 DSA to gain access to data on AI systems integrated into these platforms is an important consideration, in particular for hybrid platforms. Since these AI systems are closely linked to the systemic risks of the platforms as mentioned above, a comprehensive risk analysis could include AI data (training, validation, output) as a necessary element. A research team may thus combine the risk assessment of the platform (in accordance with DSA) with the assessment of the risks of the AI used (in accordance with the AI Act) and acquire relevant insights. At the same time, however, this requires considerable resources and skills on the part of (civil society) researchers, which must first be built up slowly and while maintaining their independence.

7 See also Harrington and Vermeulen 2024, https://blog.mozilla.org/wp-content/blogs.dir/278/files/2024/10/External-researcher-access-to-closed-foundation-models.pdf.

All in all, it would also be useful to interlink the access options to platform and AI data more closely in order to perform a uniform, comprehensive risk analysis. This would enable researchers and civil society not only to assess platform-specific risks, but also to investigate the impact of AI technologies on these risks. This would also permit further research into the general mode of action of particularly powerful models – up to the limit of legitimate business secrets, also to prevent industrial espionage – which would not only be important for AI security, but also for the development of further systems and architectures.

d | Content moderation and Art. 55 AI Act

There is no explicit obligation to moderate AI outputs under the AI Act. However, the DSA imposes a significant responsibility on hosting service providers to moderate content. Hosting services are characterized by the fact that they store information provided by users. This includes practically all platforms on which content can be stored and distributed, including the Very Large Online Platforms (VLOPs). Art. 16 DSA obligates hosting service providers to provide procedures for reporting illegal content. These procedures must be easily accessible, electronic, and user-friendly. In addition, reported content is expected to be checked quickly and objectively.

Finally, Art. 22 DSA introduces the status of "trusted whistleblowers" who may submit priority reports. This function aims to efficiently mitigate the risk of systematic abuses (e.g., frequent illegal content, false health information) on platforms and ensure that specialists in their field have a targeted impact on content moderation. This enforces decentralized monitoring.

In contrast, the AI Act does not provide for any specific obligations to moderate AI-generated content. Providers and operators of AI systems, in particular of Generative AI (GPAI), are not explicitly obligated to moderate the content generated by their systems. Nevertheless, AI is able to generate illegal content in areas that may be relevant under criminal law, such as copyright or the right to make statements. At the very least, this also affects fundamental rights that must be considered under Art. 55 AI Act. Based on the view expressed here, providers of GPAI models with systemic risks must, therefore, take reasonable technical and organizational actions to prevent the generation of illegal content (e.g., racist insults) at the technical level. However, the technical details and the specific legal aspects still need to be clarified and examined in detail.

This proactive action would aim to block illegal or systemic risk content before it can be distributed on platforms. This may tackle the issue at its technical root in a manner of speaking: Technical and organizational risk mitigation does not only take place when an AI-generated, illegal post appears on a platform, but already when it is to be generated. The strategies and techniques required for this must be regularly reviewed and revised. It must be ensured that excessive moderation impairs neither freedom of speech nor diversity of perspectives. The fact that illegal posts and false reports can of course also be written without AI in no way cancels out the possible obligations at model level.

Apart from this, any AI models used by platforms to moderate content may also fall under Art. 53 and 55 AI Act. This would mean that comprehensive information about these systems would have to be provided and risks to freedom of speech and other fundamental rights would have to be included in the risk analysis of these specific AI systems.

e | Interim result for AI Act and DSA

There is an increasing overlap between the obligations under the Digital Services Act (DSA) and the AI Act, particularly in the case of hybrid platforms that operate both as Very Large Online Platforms (VLOPs/VLOSEs) and integrate generative AI technologies (GPAI). Such platforms must analyze and mitigate both the systemic risks that result from their size and scope (in accordance with the DSA) and the specific risks posed by AI systems (in accordance with the AI Act).

A central problem is the combination of these two technologies and the new risks that arise from this. A consolidated risk analysis across technologies is required here. This includes both platform-specific and AI-specific risks and their mutual reinforcement.

In addition, there is a discrepancy between the regulations of the DSA and the AI Act regarding access to data for researchers. There is no provision in the AI Act to grant scientists explicit access to platform data, like the DSA included, which makes it more difficult to review AI systems. Consistent access to data from platforms and AI systems for scientists and civil society would be necessary to enable independent, decentralized, and comprehensive risk analyses.

Finally, there is an explicit obligation to moderate content under the DSA only for hosting platforms. However, the AI Act can be interpreted to mean that AI expenditure must also be moderated in individual cases as a result of the systematic risk analysis if this is necessary to reduce significant risks to individuals or democratic processes.

2. General Data Protection Regulation

The General Data Protection Regulation (GDPR) provides a comprehensive legal framework for the processing of personal data by private and public bodies with a connection to the EU. In accordance with Art. 2 (7) AI Act, it remains independent of the AI Act. However, there are several areas in which the AI Act may affect the GDPR.[8] One key aspect here is the matter of how the two sets of regulations interact with each other in practice, particularly with regard to balancing interests, risk assessments and liability issues. The general effects of the AI Act on the GDPR are considered here before specific frictions will be discussed and solutions outlined.

8 See also Hüger 2024: 263; Engeler and Rolfes 2024: 423; Radtke 2024: 353; Hense 2024: 449; Braegelmann 2024: 39, 41.

a | Impact of the AI Act on the GDPR

An important interface concerns the balancing of interests in accordance with point (f) of Art. 6 (1) GDPR.[9] Personal data accordingly can also be processed if the controller – usually the data processing body – has a legitimate interest in doing so and the fundamental rights and interests of the data subjects do not outweigh this. Commercial interests such as use for advertising can also constitute a legitimate interest.

In any case, a comprehensive weighing of interests is required. Some literature rightly argues as follows: Compliance with the AI Act should influence the balancing of interests in favor of, and a violation of the AI Act to the detriment of, the controller.[10] The AI Act indicates a legitimate interest or lack thereof in this context. In accordance with the view expressed here, this link goes even further: Violation of the AI Act generally means that there is no legitimate interest in the processing of data by the unlawful AI system,[11] unless it is a violation of purely formal requirements, such as documentation obligations. Providers and operators then must rely on the effective consent of the data subjects. However, apart from exceptional cases, the violation of the AI Act itself should not affect the validity of any consent.[12]

Another central interface refers to data protection impact assessments in accordance with Art. 35 GDPR. This becomes mandatory for the data controller(s) if processing is associated with a high risk to the rights of the data subjects. The important aspect here is that: High-risk applications under the AI Act are not congruent with high-risk applications under the GDPR. One example of this is personal profiling using AI, which is almost always classified as a high-risk ap-

9 See, for example, Reichert, Radtke, and Eske 2024: 483, 485; Hacker 2021: 257, 291 et seq.

10 See, for example, Hüger 2024: 263, 283 et seq.

11 See GA Bobek, Opinion of 12/19/2018, item C-40/17, Fashion ID, lit. 122; Hacker 2020: 273.

12 For detailed information on this complex of problems, e.g., the violation of the GDPR, see Hacker 2020: 397 et seq.

plication under the GDPR, whereas it does not necessarily fall into this category under the AI Act. For example, AI-based profiling for advertising or recommendation purposes is generally considered a high-risk activity under the GDPR, but not so under the AI Act.

Vice versa, however, high-risk applications under the AI Act often also pose a high risk within the meaning of Art. 35 GDPR.[13] Accordingly, a data protection impact assessment is mandatory if the data processing is associated with a high risk for data subjects. The AI Act has a similar requirement: In a number of high-risk cases – in particular where public authorities, credit institutions or insurance companies are concerned – operators must also perform a fundamental rights impact assessment in accordance with the AI Act. However, a fundamental rights impact assessment under the AI Act can certainly be integrated into a data protection impact assessment under the GDPR in order to meet the requirements of both sets of regulations.[14]

A third area of overlap refers to IT security. Art. 32 of the GDPR and Art. 15 of the AI Act go hand in hand since both require controllers to take appropriate security actions. In accordance with Art. 32 GDPR, controllers must take appropriate technical and organizational actions to ensure IT security, depending on the respective risks and the state of the art. Similarly, Art. 15 (5) AI Act states that technical solutions to ensure the cybersecurity of high-risk AI systems must be appropriate to the respective circumstances and risks. The criteria thus can be considered in sync here.

13 On the details of the criteria, see 2020: 304; see also guidance from the Conference of Independent Federal and State Data Protection Supervisory Authorities of May 6th, 2024, Artificial Intelligence and Data Protection, Version 1.0 lit. 38-40, https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf.

14 Schemmel 2024: 321.

However, the provisions of the NIS-2 Directive,[15] the planned Cyber Resilience Act (CRA)[16] and the Digital Operational Resilience Act (DORA)[17] in the financial sector, which place additional requirements on the IT security of some AI systems, must also be considered. This shows once again that the AI Act and the GDPR depend on interaction with other digital laws.

b | Different responsibilities

Thus, there are a number of overlaps between the AI Act and the GDPR. The first real point of friction between the two acts arises from the different responsibilities of the actors involved. The operator of the AI application is generally the controller for the processing of personal data under the GDPR while the provider of an AI system bears the main obligations under the AI Act. This leads to the obligations being addressed differently, which can lead to uncertainties in the question of liability. If an error occurs in a high-risk AI system, the provider could be held liable under the AI Act, while the GDPR sees the operator as the controller. In addition, the controller is responsible for performing a data protection impact assessment, for example, and must then ensure that the provider provides the necessary information.[18] In certain cases, however, there may also be joint responsibility under data protection law, meaning that both the provider

15 Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14th, 2022 concerning actions for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS-2 Directive), OJ L 333, 12/27/2022, p. 80, http://data.europa.eu/eli/dir/2022/2555/oj.

16 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.

17 Regulation (EU) 2022/2554 of the European Parliament and of the Council of December 14th, 2022 on digital operational resilience in the financial sector, OJ L 333, 12/27/2022, p. 1, http://data.europa.eu/eli/reg/2022/2554/oj.

18 Guidance from the Conference of Independent Federal and State Data Protection Supervisory Authorities of May 6th, 2024, Artificial Intelligence and Data Protection, Version 1.0 lit. 40, https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf; cf. Art. 25 (2) AI Act.

and the operator are liable under the GDPR.[19] All in all, however, the spheres of responsibility of the players involved are not coordinated.

c | Data collection and reduction of bias

There are further tensions between the thrust of the AI Act to reduce discrimination in the use of AI systems and Art. 9 of the GDPR. In accordance with this, data subject to particular protection, such as age, religious affiliation, or ethnic origin, may not be processed at all unless there is an explicit legal exception. This rule is not without issues: This is because in order to discover and eliminate inequalities between protected groups in the output, you first need to know which individuals belong to which group (e.g., religion, age, ethnic origin). However, many of these protected characteristics are also sensitive data within the meaning of Art. 9 (1) GDPR, the processing of which is generally prohibited. This is the case, for example, with the attributes "religion", "age", and "ethnic origin". Although Art. 9 (2) GDPR contains an exception for data processing in the public interest, it is unclear whether this applies across the board and may be doubted.[20] AI developers who collect this data therefore expose themselves to a considerable liability risk under data protection law.[21]

The European legislator has recognized this. The AI Act now provides for an exception for the processing of sensitive data in Art. 10 (5) for the detection and reduction of bias in high-risk AI systems. At the same time, actions are required to safeguard the data protection interests of the data subjects and processing for the purposes of reducing discrimination must be limited to what is necessary. However, this useful exception will only apply to high-risk AI and not to generative AI or non-high-risk systems – even though there is also considerable potential for discrimination here.

19 Gierschmann 2020, for example, deals with this in greater detail: 69; Hacker 2020: 130 et seq.

20 See also Hacker 2021: 257, 294.

21 See also van Bekkum and Borgesius 2023: 263, 280.

Health Data Utilization Act (GDNG)

Entering into effect: March 26th, 2024

Goal: Facilitating the use of health data for research and improving care

Important items: The German Health Data Utilization Act (GDNG) aims to facilitate the use of health data for research and care improvement by creating a new health data infrastructure with a central data access and coordination point.[1] The law supplements the GDPR by establishing new provisions for data use, data protection and research processes. It enables more efficient linking of health data and simplifies transnational research projects.[2]

Challenges: At the same time, a number of challenges remain in the area of data protection law due to its fragmentation between different countries and hospital laws.[3] Furthermore, the facilitated use of health data by health insurance companies, even without the consent of those affected, is often viewed critically – and not without any reason.[4]

1 See, for example, Rauch, Richters, and Naucke 2024: 218.

2 Schneider and Katzenstein 2024: 196.

3 Rauch, Richters, and Naucke 2024: 218, 220.

4 See, for example, Weichert 2023; Theisen 2024: 54.

d | Data collection and performance

Finally, there is another potential conflict between the performance requirements of the AI Act (Art. 15) and the provisions of the GDPR (Art. 9). Art. 15 (1) AI Act requires an "adequate level of accuracy" for high-risk systems, whereby accuracy should correctly be read as performance or efficiency in the sense of technical quality actions. Art. 9 GDPR, on the other hand, forbids use of certain categories of sensitive data, as we have just seen.

However, development of powerful AI models, particularly in the medical field, sometimes requires the processing of sensitive data (e.g., health data). The use of such data could be required under the AI Act to ensure sufficient performance and also coverage of diverse population groups by the AI model. However, Art. 9 GDPR generally forbids this. New approaches are needed in this context. In Germany, the Health Data Utilization Act (Gesundheitsdatennutzungsgesetz; GDNG) points in this direction. A regulation at European level may provide considerable progress and clarification here. The European Health Data Space is a first step in this direction.[22]

e | AI training in accordance with the GDPR

Taking a step back will make the fundamental issue apparent. At the moment, a legal gap exists regarding the reuse of personal data for AI training purposes, which should be closed by new legal instruments or a revision of existing laws. In particular, the question of how personal data may be reused in accordance with data protection law must be clarified in this context.[23]

Under the GDPR, there is no clear boundary between legal and illegal reuse of data for AI training purposes. Many things depend on the specific circumstances of the individual case.[24] However, point (f) of Art. 6 (1), Art. 6 (4), and Art. 9 GDPR are particularly decisive for a legal analysis. See on this in detail:

In accordance with point (f) of Art. 6 (1) GDPR, processing of personal data for the training of AI models is permitted if the legitimate interests of the controller or third parties are not overridden by the rights and interests of the data subjects. Factors such as the degree of anonymization, the social benefits of the model, the duration of data storage and the proximity of the data to sensitive categories must be considered. Art. 6 (1) (f) GDPR will often be the central legal basis for AI training with personal data since obtaining individual consent retrospectively would often involve disproportionately high transaction costs.[25]

Art. 6 (4) GDPR imposes additional requirements on the secondary use of data and includes a compatibility test that considers several. These include the connection between the original and secondary use, the context of collection, the proximity to sensitive data categories, the impact on the data subjects and the existence of protective actions such as encryption and pseudonymization.

It becomes even more complex when it comes to sensitive data. For example, there is no general balancing criterion under Art. 9 GDPR as there is under point (f) of Art. 6 (1) GDPR. Rather, processing of sensitive data (e.g., health data) is, as seen, prohibited unless an exception under Art. 9 (2) GDPR applies. However, developers may be able to make use of the public interest exception under point (g) of Article 9 (2) GDPR in cases where the training itself poses relatively low risks, for example if the model is specifically aimed at promoting legal equality and non-discrimination.[26] However, this only applies to the training process,

22 See, for example, Werry and Ntanas 2024: 641.

23 See, for example, the current debates about the use of user data for training purposes by platforms such as X/Twitter or Meta: Gkritsi 2024; Weatherbed 2024.

24 Hüger 2024: 263, 284.

25 This is partly different in the case of platforms that want to use the data of their users, with whom they already have a contractual relationship, for AI training. Consent certainly may be used as an instrument here. However, it does not offer a one-size-fits-all solution, see only the numerous articles criticizing the consent mechanism, overview for example in Hermstrüwer 2016: Chapter 5; Hacker 2020: 577 et seq.

26 Hacker 2021: 257, 294.

not to the application of the model in the field, and is also not always guaranteed for the training.

If the AI model is only developed for research purposes, Art. 9(2)(j) and Art. 89 GDPR offer the Member States leeway to adopt specific rules for the processing of sensitive data in research. For example, the German legislator has introduced a specific balancing test for the use of sensitive data in research contexts in § 27 BDSG, which is, however, stricter than point (f) of Art. 6 (1) GDPR.

All in all, there thus is a clear need for a new provision on the processing of sensitive and non-sensitive personal data for the training of AI, in particular with regard to Art. 6 and 9 GDPR.

f | Interim result on the GDPR and AI Act

The AI Act and the GDPR interact with each other in a complex way, particularly with regard to balancing interests, risk assessments and liability issues. While the GDPR remains independent, the requirements of the AI Act can still have a significant impact on the data protection framework. The data protection impact assessments in accordance with Art. 35 GDPR are particularly relevant here, as they often overlap with the high-risk applications of the AI Act but are not congruent. Integration of the risk assessments of both sets of regulations is proposed for such cases.

There are also tensions between the two sets of regulations, particularly with regard to the responsibility of the players (providers vs. operators) and the processing of sensitive data to reduce discrimination in the context of AI applications. There is a need for reform here, such as the extension of exemptions for the processing of sensitive data to non-high-risk AI systems, e.g., generative AI (see in detail below, section IV.).

There generally is an urgent need for a clear legal framework on the reuse of personal data for AI training purposes, as there are no clear rules on this yet.

AI Act and liability law

Digital product liability law in the context of artificial intelligence is a complex and topical issue that is regulated by various EU legal acts, such as the new Product Liability Directive, the planned AI Liability Directive, and the AI Act.[1]

Relationship between the AI Act and product-liability law:

- If a company violates the AI Act, it is typically also liable under product liability law or tort law.
- However, companies could also be liable in individual cases despite complying with the AI Act.
- This would result in double, potentially divergent requirements for companies.
- Solution approach: Harmonization of technical standards as safe harbor regulations for AI Act and product liability law

1 See, for example, Hacker 2024; Novelli et al. 2024; Wachter 2024: 671; Wagner 2021; Hacker 2023.

III. AI Act and sectoral regulation

The AI Act interacts not only with new EU digital laws, but also in particular with existing sectoral regulation. Specific sectors have been explicitly listed in annexes to the AI Act, for this. Most of them are already subject to specific product safety legislation. The various sectoral regulations are mentioned in three different sections: sectoral regulation of products under Annex I Section A AI Act, under Annex I Section B and under Annex III.

Three representative sectors will be examined below: Medical devices (Annex I Section A), automotive (Annex I Section B), and financial products (Annex III). An entire class of high-risk applications relates directly to existing product safety law (as listed in Annex I Section A AI Act). These include, amongst other things, the area of machines, medical devices, and toys (under c). However, the links between the AI Act and these specific areas of law are only incompletely developed in spite of improvements in the final version of the AI Act as compared to the original Commission draft. This applies in particular to high-risk systems from Annex III AI Act, which are also subject to complex, existing regulatory law, for example in the area of lending and insurance (under b). Products that fall under the old product safety law and are listed in Annex I Section B AI Act, such as those from the automotive sector (under d), are much more clearly defined. The specific product safety law applies primarily here, not the AI Act. General forms of interlinking of the AI Act and sectoral regulation should be addressed (under a)) before looking at these specific delimitations, however.

1. General interlinking

The fact that the AI Act is applied at all in addition to sectoral regulatory instruments is comprehensible as far as these existing sector-specific acts regularly address the classic risks of the respective products, in particular for health and safety, but not further-reaching AI risks such as discrimination or lack of transparency.

Recital 64 of the AI Act thus emphasizes that sectoral regulation and the AI Act apply in parallel and that the provisions of all acts must be complied with. At the same time, it is acknowledged that suppliers of products with high-risk AI systems subject to both the AI Act and other sectoral legislation may be flexible in implementing the compliance requirements. Sector-specific regulations on the need for a new conformity assessment following a change to the AI model also have priority (EC 84 AI Act). The Medical Device Regulation (MDR) does not require the product itself to be reassessed if, for example, only the packaging of a medical device is changed. The AI Act adopts this result. This is intended to avoid unnecessary administrative work and costs.

Flexibility relates in particular to the integration of testing and reporting procedures into existing documentation and compliance and quality management systems, as long as all requirements of the various legal acts are met.[27] Recital 158 explains this further for regulated credit institutions and certain insurance

27 See also EC 81 and Art. 9 (10), Art. 11 (2), and Art. 17 (3) AI Act.

companies. The Commission may also „take initiatives, including sectoral initiatives, to facilitate the removal of technical barriers that hinder the cross-border exchange of data in the context of AI development“ (Recital 165 AI Act). The technical standards that are so important and that are central to implementation must also be compatible with the existing, sector-specific standards (Art. 40 (2) AI Act). This interconnection is also reflected in supervisory law in that the sectoral market surveillance authority is also responsible for compliance with the AI Act (Art. 74 (3) (1) AI Act). In Germany, for example, the Federal Financial Supervisory Authority (BaFin) will probably also be responsible for the supervision of financial products under the AI Act. Member States may deviate from this rule in favor of sectoral authorities, but then close coordination between the central market surveillance authority and the sectoral authorities must be ensured (Art. 74 (3) (2) AI Act). This also applies to the respective rules of procedure, i.e., the way in which the authorities perform their duties and how data subjects can assert their rights (Art. 74 (4) AI Act).

However, a closer look at the sectors concerned shows that significant demarcation problems persist. This is discussed below using examples from the financial sector (Annex III), medical devices (Annex I Section A) and automotive (Annex I Section B).

2. Financial products

Financial products are not generally assigned to the high-risk category of the AI Act. Rather this only concerns systems that

- are to be used to assess the creditworthiness and credit rating of natural persons or that
- are intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance in accordance with Annex III No. 5 AI Act.

Credit assessment systems based on statistical models, heuristics and AI-based decision-making processes are therefore explicitly classified as high-risk applications in the AI Act (point (b) of Annex III No. 5 AI Act). Deployments of AI systems that only involve preparatory actions are excluded from the high-risk categories of Annex III (Art. 6 (3) AI Act). However, credit scores typically play a decisive role in the credit decision, which the ECJ correctly clarified in the SCHUFA decision.[28] Such AI systems accordingly do not fall under the exception mentioned.[29] Such systems are therefore subject to the high-risk requirements of the AI Act in terms of data quality, transparency, and monitoring. This affects both traditional banks and fintech companies, which are increasingly making AI-supported lending decisions. It is essential that the AI Act's definition of AI is very broad: In addition to advanced models, this also includes classic machine learning methods, some of which have been used in the financial sector for decades, such as statistical modeling, linear or logistic regression.[30] The same applies to credit rating systems.

Use of AI systems for fraud detection forms one exception here. AI systems used solely to detect financial fraud are exempt from the high-risk provisions of the AI Act even though credit scoring systems are subject to strict regulation. In accordance with the wording of Annex III, however, this only concerns recognition systems in the area of credit and creditworthiness assessment. However, this exception will also have to be applied analogously to the fight against fraud in the area of life and health insurance since no objective reason for differentiation is apparent.

28 EuGH, item C-634/21, SCHUFA, lit. 75.

29 Radtke 2024: 353, 359 et seq.

30 See, for example, Hacker 2024: 10; Woesch and Vogt 2024: 689, 691.

However, the regulation of these activities by the AI Act gives rise to various conflicts and inconsistencies with existing banking and insurance regulations.[31] The focus below is on coordination with banking law; however, similar considerations also apply to insurance law.[32]

a | Partial integration

Some of the provisions of the AI Act are compatible with the requirements of the existing financial supervisory regime and are certainly interlinked, as the general considerations above have already shown. Art. 9 of the AI Act, for example, deals with risk management, an area that has also been regulated by banking law for some time. Financial institutions are already required to implement internal control and risk management systems to ensure the safe use of AI systems. Art. 17 AI Act requires a quality management system for high-risk AI systems as well. This is already regulated in the financial sector.

Therefore, Art. 9 (10) AI Act correctly refers to the fact that regulated credit institutions, as well as other sectorally regulated entities, may combine the existing risk management systems with the system required under the AI Act. The requirements for the bank's risk management system are defined in more detail by two central mechanisms in Germany: the DORA (Digital Operational Resilience Act)[33] in the area of IT security and a BaFin circular (Minimum Requirements for the Risk Management System, MaRisk), which has been amended several times.[34] The latter is based on legal requirements[35] and corresponding guidelines of the European Banking Authority. It explicitly continues to apply when using AI.[36] In particular, the AI extension of model validation, which has been included since the last amendment, offers major overlaps with the conformity assessment required under the AI Act, i.e., the testing of AI with regard to compliance with the requirements of the AI Act. The next update of MaRisk should, therefore, explain how banking supervisory requirements and the requirements of the AI Act are interlinked as clearly as possible.

Art. 17 (4) AI Act goes even further than that: It stipulates that the obligation to set up a quality management system for regulated financial service providers is, with a few exceptions, deemed to be fulfilled by a legally compliant quality management system within the meaning of financial services law. Only the components of the correspondingly restructured risk management system, the market monitoring system, and the system for reporting serious breaches, each of which is required under the AI Act, still need to be integrated.

Art. 17 (4) AI Act thus serves as a model: The paragraph is an example of successful interlinking since it particularly and very specifically regulates the parts of the AI Act that are automatically covered by existing regulatory law and which actions still need to be taken in addition. Unfortunately, this provision is also the only one in the AI Act that offers such clarity and precision with regard to sectoral entanglement.

b | Gaps and potential duplication of regulations

The AI Act clearly introduces some new requirements that go beyond the previous banking regulations and in some cases duplicate them. Data governance is a key example of this. Art. 10 AI Act lays down strict standards for the quality of the data used. Companies must ensure that the training data of their AI systems is complete, error-free, representative, and non-discriminatory.

31 See, for example, Eber and Hacker (in prep.); Feldkamp et al. 2024: 60; Woesch and Vogt 2024: 689.

32 See, for example, Marano and Li 2023: 12.

33 Regulation (EU) 2022/2554 of the European Parliament and of the Council of December 14th, 2022 on digital operational resilience in the financial sector, OJ L 333, 12/27/2022, p. 1, http://data.europa.eu/eli/reg/2022/2554/oj.

34 BaFin, Circular 06/2024 (BA) dated 05/29/2024, Minimum Requirements for Risk Management – MaRisk, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_06_2024_MaRisk_pdf_BA.html.

35 Art. 97 (1) CRD IV, § 25a (1) KWG.

36 MaRisk, AT 4.3.5, lit. 1.

Art. 17 (4) AI Act – Harmonization with sectoral regulation

Art. 17 (4) AI Act is a prime example of harmonization between the AI Act and existing sectoral regulations:

1. ***Basic principle:*** Financial institutions that are already subject to internal governance, arrangement or process requirements under EU financial services law are considered compliant with most of the quality management requirements of the AI Act.

2. ***Areas covered:*** Most aspects of the quality management system in accordance with Art. 17 (1) are met by existing financial law.

3. ***Additional requirements of the AI Act:*** Financial institutions must also implement three specific areas:
   - Risk management system (item (g) of Art. 17 (1))
   - Post-market surveillance system (item (h) of Art. 17 (1))
   - Incident reporting system (item (i) of Art. 17 (1))

4. ***Clear demarcation:*** The article creates legal certainty by precisely defining which requirements are fulfilled by existing regulations and which must be implemented additionally.

5. ***Restriction:*** This clear harmonization has so far been limited to the quality management system in the financial area. There are no similarly detailed regulations for other requirements of the AI Act or other sectors.

This regulation thus represents how cross-sector and sector-specific regulations can be effectively harmonized in order to avoid double regulation and at the same time cover specific AI risks.

These requirements supplement existing provisions under banking supervisory law. In Art. 76 CRD IV, the Capital Requirements Directive IV 2013/36/EU (CRD IV) stipulates that financial institutions require robust risk management systems based on high-quality and regularly reviewed data. Another key instrument of banking law, the Capital Requirements Regulation (EU) No. 575/2013 (CRR), requires financial institutions to use high-quality, complete, and up-to-date data to calculate and model risks. Art. 185 CRR obligates banks to review the quality of the scoring models ("accuracy and consistency") for internal ratings and risk assessments on an ongoing basis. This is achieved, amongst other things, by continually monitoring the function of such models. Art. 174 CRR also stipulates that statistical models and "other mechanical methods" for risk assessment must have a high predictive power (letter a). The input data must in turn be checked for accuracy, completeness, appropriateness, and representativeness (points (b), (c)). In addition, the models must be periodically validated (lit. d) and operated under human supervision (point (e)).

This shows that the requirements of Art. 174 CRR and Art. 10 AI Act are mostly identical and even use the same terms in some cases (completeness, representativeness). However, there is no standard that, like Art. 17 (4) AI Act, would precisely regulate which elements of Art. 10 AI Act are to be considered to be covered by Art. 174 CRR and which are not. However, a comparative analysis will make clear that the obligation to minimize distortions in training data (lit (g) of Art. 10 (2) AI Act)

in particular is not explicitly reflected in Art. 174 CRR, even if this can be read into the general quality requirements.[37] Ann in all, it can thus be said that compliance with Art. 174 CRR generally should lead to the central data quality characteristics set out in the AI Act, such as representativeness, relevance, accuracy, completeness, statistical suitability and, where applicable, the minimization of distortions, also being met.

However, the AI Act also contains some new obligations, e.g., in relation to transparency and documentation. Financial companies that use high-risk AI systems such as credit scoring systems must maintain extensive documentation and ensure that appropriate human oversight of these systems is in place. These requirements may lead to an additional burden, as financial institutions are already subject to existing documentation and transparency requirements. The only thing that helps here is the mentioned 64th recital of the AI Act, in accordance with which, in particular, documentation obligations from several legal acts may be combined and handled flexibly as long as all obligations are met overall. MaRisk already notes that it is necessary to be able to explain models to a sufficient degree, in particular if they operate with AI.[38]

The AI Act also establishes some additional requirements with regard to quality actions and cybersecurity (Art. 15 AI Act). As mentioned above, an appropriate level of performance in the sense of technical quality actions must be maintained in accordance with Art. 15 (1) AI Act; as also mentioned, cybersecurity must be risk-adequate. Banks not only need to comply with the security actions already in place, but also meet the requirements for robustness and IT security stipulated by the AI Act. However, these are also likely to be mostly in line with the existing requirements of banking law.[39] For example, lit (a) of Art. 174 CRR already requires good forecasting capability of the models used, and the DORA contains very specific rules on the required IT security.

The lack of explicit coordination between the sectoral regulations of the banking sector and the new regulations of the AI Act leads to regulatory duplication that has not been resolved in terms of legislation. Financial institutions thus need to make an educated guess in many areas as to the extent to which the requirements of the AI Act may go beyond individual requirements of banking law. This situation clearly is not satisfactory.

c | Interim result on financial products

Introduction of the AI Act leads to a complex area of tension between the new requirements for high-risk AI systems and the existing banking regulations. There are significant gaps and duplicate regulations in others that pose challenges for financial institutions even though integration has been achieved in some areas. It would have been possible to avoid these relatively easily without any loss of protection of fundamental rights by using clearer references and delimitations. Credit rating systems and insurance products in the life and health sector are areas that are particularly affected. These need to comply with additional and possibly stricter regulations in future. The AI Act will significantly change the regulatory environment for many financial products in spite of some exceptions, such as fraud detection systems.

3. Medical devices

The financial sector is not the only one to be confronted with a further, horizontal layer of regulation as a result of the enactment of the AI Act. The same applies to use of artificial intelligence (AI) in the medical field. The integration of AI into medical devices leads to delimitation difficulties between the Medical Device Regulation (EU) 2017/745 (MDR) and the

37 The model must not contain any material systematic errors, which can certainly include discriminatory distortions in accordance with point (a) of Art. 174 CRR.

38 MaRisk, AT 4.3.5, lit. 6.

39 See, for example, MaRisk, AT 4.3.5, lit. 5 (stability) and AT 7.2 (IT security) as well as the DORA.

AI Act.[40] This is particularly relevant as the two regulations pursue different risk assessments. The AI Act with its international scope is going to affect virtually all of the 690 medical device suppliers approved by the Food and Drug Administration (FDA) in the USA – and thus virtually all those operating in the EU.[41] For a better understanding of the conflicts arising from this, take a look at some specific examples such as cancer diagnosis, the creation of doctor's letters and the management of a doctor's appointment calendar.

a | General conflicts between MDR and AI Act

The Medical Device Regulation (MDR) and the AI Act pursue complementary but not congruent objectives: While the MDR focuses primarily on the safety and effectiveness of medical devices, the AI Act is aimed at further minimizing the risks of AI systems, particularly with regard to discrimination, lack of transparency and IT security. The benefit-risk assessment (Art. 61 (1), 2 (24) MDR) is a central component of the MDR. In the end, both the risks and possible advantages of use as a medical device will be considered and brought into proportion. The medical device is only approved if the benefit outweighs the risk. The AI Act does not explicitly provide for such a consideration of not only the risks but also the opportunities. There is a considerable difference in the methodology of the assessment even though it may be possible to read this into some undefined legal terms (e.g., "reasonable degree of accuracy", Art. 15 (1) AI Act; "appropriate actions", Art. 10 (2) AI Act).

The general restrictions and relaxations named above also apply here, particularly with regard to the risk management system. However, many other regulations are not linked to sectoral regulation in the medical sector as well as in the financial sector. This also leads to potential overlaps and double regulation for products that fall under both the MDR and the AI Act. A central problem is the question of which requirements take precedence when an AI system is simultaneously classified as a medical device and as high-risk AI.

b | Example 1: Cancer diagnosis

An AI system used for cancer diagnosis clearly shows the difficulties in differentiating between the two prescriptions. The MDR recognizes three central risk classes: Class III (potential impact: patient death); Class II (direct impact on diagnostic or therapeutic decisions, with subclasses IIb – potentially severe deterioration of health status – and IIa – diagnostics/therapy only) – and Class I (miscellaneous). Under the MDR, such a cancer diagnostic system typically falls into risk class IIa or even IIb and higher when linked to effectors, as it then has a direct impact on diagnostic and therapeutic decisions and can potentially cause a serious deterioration in a person's state of health (Annex VIII chapter 3 rule 11 MDR).[42]

The AI Act also treats such systems as high-risk AI systems under Art. 6 (1) AI Act.[43] This brings about a double regulation to some degree since both the MDR and the AI Act place strict requirements on quality management, risk management and technical documentation.

Priority regulations have been introduced very selectively, in accordance with which MDR has priority. This includes, amongst other things, the question of whether changes to an AI system require a new conformity test. In this case, the 84th recital of the AI Act states that the Medical Devices Regulation decides how this is to be assessed. If no new review is required thereafter (e.g., Art. 16 (2) MDR), the AI Act does not require this either. Apart from this, quality manage-

40 The EU In Vitro Diagnostic Medical Devices Regulation (EU) 2017/746 (IVDR) and the Clinical Trials Regulation (EU) No 536/2014 (CTR) also apply, but are not included here; see also Onitiu, Wachter, and Mittelstadt 2024.

41 Aboy, Minssen, and Vayena 2024: 2.

42 See also Onitiu, Wachter and Mittelstadt 2024: 5 fn. 17 and 6 fn. 19, where an "advanced imaging tool for prediction and diagnosis" is classified as a product in risk class IIa. However, these subtleties (IIa or IIb) do not play a role in the distinction from the AI Act.

43 In connection with Annex I Section A No. 11.

ment systems under the AI Act and MDR can be integrated with each other (Art. 17 (3) AI Act). In contrast to financial market regulation, however, there are no specific, detailed restrictions here as in Art. 17 (4) AI Act, which only benefit financial institutions, but not manufacturers of medical devices.

This double regulation can lead to considerable bureaucratic hurdles, in particular for small and medium-sized enterprises (SMEs), which are confronted with the requirements of both regulations. Not only do they have to provide MDR-compliant technical documentation, test, and maintain MDR-compliant safety mechanisms, they also must meet the additional requirements of the AI Act, such as the extended documentation obligation,[44] automatic logging of events, specific data governance and traceability. A better division and coordination of requirements would have avoided unnecessary duplication of work.

Although the technical documentation under the MDR and the AI Act can be combined (Art. 11 (2) AI Act), significantly more information is required under the AI Act than under the MDR. After all, simplified documentation is planned for SMEs, in accordance with a Commission form (Art. 11 (1) (2) AI Act). However, operationalization of the additional AI Act requirements – useful as they may be in particular cases – will pose a considerable challenge for many companies due to the lack of delimitation standards since providers of medical devices, and in particular SMEs, are already experiencing significant issues with implementation of the MDR,[45] not least due to a shortage of conformity assessment bodies.[46] The same applies here: A clear demarcation reduces this without affecting the protection of fundamental rights for those affected..

c | Example 2: Doctor's letters

An AI system that is used to create doctor's letters illustrates the problem of differentiating between administrative and medical functions. Under the MDR, such a system likely would not be classified as a high-risk system, as it has no direct impact on diagnosis or therapy (Annex VIII Chapter 3 Rule 11 MDR). It thus falls into Class I, which requires only minimal regulatory control. In this case, self-certification is possible.[47]

The AI Act initially follows this assessment: If certification by external bodies is not required under sectoral regulation – e.g., since the AI only performs support functions without intervening in diagnostic decisions – it is not generally considered a high-risk AI system under the AI Act.[48] Further requirements connected to this thus only arise from the transparency obligations of Art. 50 AI Act and the requirement to ensure AI competence of all parties involved in accordance with Art. 4 AI Act. This appears entirely appropriate.

However, the challenge here is to ensure that the use of doctor's letter AI does not indirectly interfere with medical decisions. This creates a gray zone where manufacturers must prove that their AI will not influence any significant medical decision-making processes. In the end, this produces uncertainties of classification in accordance with the MDR and AI Act, which, however, may also be justified in the case of possible diagnostically or therapeutically relevant processes.

d | Example 3: Appointment schedule and triage

An AI-supported appointment schedule is a minimally invasive model. Such systems are neither covered by the MDR as high-risk medical devices nor by the AI

44 Aboy, Minssen, and Vayena 2024: 2.

45 Carl and Hochmann 2023.

46 Aboy, Minssen, and Vayena 2024: 4.

47 Aboy, Minssen, and Vayena 2024: 4.

48 See point (b) of Art. 6 (1) AI Act; but differently in Aboy, Minssen, and Vayenaa 2024: 4.

Act as high-risk AI systems, as they have no influence on medical decisions. Thus, they are considered systems subject to limited risk that only need to meet minor regulatory requirements (transparency and AI competence).

However, further requirements may arise if, for example, the appointment calendar is equipped with an algorithm that automatically prioritizes based on medical data. In such a case, it is conceivable that both the MDR and, subsequently, the AI Act could provide for additional requirements. The AI Act even classifies the AI independently as high-risk AI (point (d) of Annex III No. 5 AI Act) for triage performed during emergency care (but not during regular operation) – though it will generally also constitute a Class II device in accordance with the MDR. This emphasizes the fact that the distinction between risk classes and prescriptions can be complex even for systems that are not diagnostic/therapeutic at first glance.

e | Interim result for medical devices

The examples of the cancer diagnosis, the doctor's letters, and the appointment schedule illustrate the difficulties in differentiating between the MDR and the AI Act. While systems with direct medical relevance, such as cancer diagnosis, are squarely placed in the high-risk category in accordance with both regulations, administrative systems such as doctor's letters or appointment calendars require differentiated considerations. Though potential overlaps and additional requirements under the AI Act increase the workload for manufacturers that need to ensure that their products meet both medical law and AI-specific requirements, they are generally sensible in view of the prevailing risks in the medical sector. Even so, a specification of precisely which additional criteria must effectively be met under the AI Act would be useful.

However, in light of the already-present bottlenecks in the approval of medical devices, the capacities of conformity assessment bodies in particular must be increased urgently and quickly in order to cope with the expected volume of new systems and to release responsible medical AI for use in Germany and Europe after a reasonable period of testing.

4. Automotive

Finally, the AI Act affects the automotive sector, in particular in the area of systems for autonomous driving. The high-risk provisions of the AI Act do not apply directly to the automotive sector, as this is explicitly excluded in essential parts (Art. 2 (2) in conjunction with Art. 6 (1) and Annex I Section B AI Act). The exception has not been established to exempt autonomous driving systems from regulation in the first place, but to ensure revision of the existing, specific approval regulation for vehicles should be revised by the Commission (recital 49 AI Act). In the new version, the provisions of the AI Act for high-risk systems must then be specifically incorporated into this sectoral regulation (Art. 104 and 107 AI Act).[49]

The regime clearly differs from the sectoral regulations considered until now, remain unchanged as the AI Act takes its place alongside them, in this respect. The sectoral rules apply exclusively in the automotive sector as well as in all other sectors listed in Annex I Section B AI Act (e.g., civil aviation, railroad interoperability, marine equipment). However, they are subject to revision. The requirements of the AI Act for high-risk AI systems must be considered as well. On the other hand, it is not clear exactly which provisions of automotive regulation are covered and how.

a | Approval procedure in the automotive sector

In order to comprehend more precisely which areas are affected by the AI Act and how, it is first necessary to gain an overview of the various regulatory systems and approval procedures in the automotive sector.

Type approval, also referred to as homologation, is the key here. This is a process that ensures that a vehicle or vehicle component complies with EU-wide

49 See, for example, Kilian 2024a: 130, 132; Kilian 2024b: 5 et seq.

safety and environmental standards. This process involves inspection by the authorities and includes the issuing of a certificate confirming the vehicle's conformity. Type approval covers various aspects, including emissions, safety, energy efficiency, and general roadworthiness. The Commission published an implementing regulation that covers the essential aspects for the testing of automated driving systems for fully automated vehicles for type approval in August 2022 already.[50] Further implementing regulations are expected in the future, which will also regulate type approval for other AI systems in more detail.[51] National legislators are also going to need to adapt the relevant licensing legislation (e.g., the Road Traffic Licensing Regulations (StVZO)) and to specifically consider the requirements for high-risk systems in the AI Act (Art. 107 AI Act).

b | Possible conflicts between the AI Act and existing automotive regulations

On the industry side, there have been concerns during the legislative process that the AI Act could lead to double regulation.[52] In particular, it was thought that certain systems that would not pose any high risks may be regulated needlessly strictly. This might – as the industry stated – hinder innovation in the automotive sector.[53] On the other hand, it must be considered that even systems that are not inherently high-risk (e.g., infotainment, voice control) must ensure that they do not lead to an unnecessary reduction in driver attention.

However, the risk of double regulation appears to be largely averted in the area of products covered by Annex I Section B AI Act (e.g., motor vehicles). After all, Art. 2 (2) AI Act contains a far-reaching exemption. The high-risk provisions of the AI Act explicitly exclude any systems subject to Annex I Section B of the AI Act; in the automotive sector, this includes in particular:

- the Type Approval Regulation: Regulation (EU) 2018/858 of the European Parliament and of the Council of May 30th, 2018, on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles
- Regulation (EU) No 168/2013 of the European Parliament and of the Council of January 15th, 2013, on the approval and market surveillance of two- or three-wheel vehicles and quadricycles
- Regulation (EU) 2019/2144 of the European Parliament and of the Council of November 27th, 2019, on type-approval requirements for motor vehicles and their trailers, and for systems, components and separate technical units intended for such vehicles, with regard to their general safety and the protection of occupants and vulnerable road users
- Regulation (EU) No. 167/2013 of the European Parliament and of the Council of February 5th, 2013, on the approval and market surveillance of agricultural and forestry vehicles

This exemption is comprehensive in accordance with Art. 2 (2) AI Act: It is sufficient that they are high-risk systems in accordance with Art. 6 (1) AI Act that are "in connection with products" subject to Annex I Section B. Thus, it also includes systems that are not directly installed in the product itself but are essential for its operation.

50 Implementation regulation (EU) 2022/1426 of the Commission from August 5th, 2022, with detailed provisions on implementation of Regulation (EU) 2019/2144 of the European Parliament and the Council with regard to uniform procedures and technical specifications for type approval of the Automated Driving System (ADS) of fully automated vehicles, also see https://ai-regulation.com/the-eu-commission-regulatory-stance-on-autonomous-vehicles/.

51 Köllner 2024.

52 VDA 2023: 13.

53 See loc. cit: 6.

However, an at first glance paradoxical consequence of the exemption is also that such systems that are not classified as high-risk systems under Art. 6 (1) AI Act are fully subject to the requirements of the AI Act – such as the requirements for the AI competence of the employees involved in the system under Art. 4 AI Act and the transparency provisions under Art. 50.

This may become relevant for elements that are not directly assigned to the safety systems, such as infotainment or control systems such as a voice assistant: If these are classified as high-risk systems in accordance with Art. 6 (1) AI Act due to their integration into other relevant hardware, they are exempt from the AI Act and are only subject to the respective sectoral regulation. However, the exception under Art. 2 (2) AI Act only applies to systems qualified as high-risk systems. Otherwise, for example, the transparency requirements under Art. 50 AI Act must be met based on interaction with humans, as well as the requirements regarding the AI competence of the developing and operating companies under Art. 4 AI Act.

Even if the classification is ultimately a question of the individual case, the safety relevance of these systems (infotainment; voice assistant) cannot be completely denied. Such systems may also lead to an accident if they malfunction, as drivers may be distracted by the difficulty in operating them.[54] While not an AI-specific risk since it may also occur when interacting with the radio or other occupants, distraction by infotainment products should be technically prevented as far as possible by developing them in a manner that does not permit long-term operation or interaction while the driver is driving.

c | Interim result for the automotive sector

Type approval is the central procedure for the approval of vehicles, in which compliance with technical and safety-related standards will be reviewed. The AI Act introduces additional requirements specifically for AI systems in vehicles that are not high-risk in accordance with its terminology. High-risk systems in the narrower sense, on the other hand, are exempt from the requirements of the AI Act. They are instead subject to the EU Type Approval Regulation and other European and national regulations, although these will have to be revised in future to take account of the high-risk principles of the AI Act.

54 See VDA 2023: 6.

IV. Recommendations

This study examines the frictions and synergies between the AI Act and existing EU regulations. It was shown above that the AI Act, as a horizontal legal framework, complements the sectoral regulations, for example in the financial, medical, and automotive sectors, but is insufficiently coordinated with them. A number of recommendations for action can be derived from this. They will be broken down into short-term, medium-term, and long-term actions below. The respective proposals within these are divided in accordance with addressees, ranging from the European legislator and various regulatory authorities to national legislators, standardization organizations, companies and, last but not least, the legal community itself. Table 1 provides an overview of the proposals.

1. Short-term actions

A number of actions can be taken to reduce friction and strengthen synergies in the short term.

a | European legislator

Designation of a "Lead Act": One proposal for minimizing any conflicts involves the introduction of a "Lead Act", which serves as the primary legal framework for AI applications. Such a specification of relationships would have to be done at a statutory level. Depending on the sector, the lead act could be the AI Act, but also one or more particularly important acts of sectoral regulation. The idea would then be: If the "Lead Act" is met, there is a presumption that the requirements of the other regulations are also fulfilled, unless specific standards from other regulations or directives must be explicitly complied with independently of the Lead Act. For example, it would be conceivable to designate the Medical Device Regulation (MDR) as the lead act and then only explicitly define individual provisions of the AI Act that go significantly beyond the MDR as additional requirements to be met.

b | European Commission (esp. AI Office)

Stronger interlinking of regulations: It is generally recommended that existing sector-specific regulations be linked more closely with the AI Act in order to avoid double regulation. For example, there is considerable overlap in the areas of financial services, medical devices, and the automotive industry. This should be minimized by stipulating clearer delimitations and precise information on which provisions of the AI Act have been implemented through compliance with sector-specific requirements and which have not. This may be achieved primarily, as far as possible, by means of implementing regulations, for which no amendment to the AI Act itself is necessary.

The important factor is that this is going to reduce the regulatory burden and promote the development and use of AI without reducing the protection of fundamental rights one iota since the existing regulations are only organized more advantageously and brought into a clearly implementable relationship, but not reduced or restricted.

Practice guidelines and content moderation at model level: Moderation of AI outputs is not required explicitly under the AI Act. However, this may become necessary based on Art. 55 if systemic risks, e.g., for non-discrimination and democratic (electoral) processes, cannot be effectively reduced otherwise. This should also be set out in the practice guidelines under Art. 56 AI Act.

At the same time, care must be taken to ensure that excessive moderation does not have a negative impact on freedom of expression and the diversity of output. However, note that legal AI content that is erroneously blocked by the model may, of course, also be recorded and posted without the help of generative AI.

Reciprocal risk analyses (AI Office and Commission supervision of VLOPs/ VLOSEs): An integrated risk analysis that assesses both the platform-specific and AI-specific risks may be performed in particular in the case of large platforms (VLOPs/VLOSEs) that integrate generative AI. The supervisory authorities (under the DSA and AI Act) should actively encourage this. After all, closer interlinking of the risk analyses from the AI Act and the Digital Services Act is essential here.

c | European Data Protection Board

Harmonization with the GDPR: It is recommended that the European Data Protection Board (point (e) of Art. 70 (1) GDPR) develop specific guidelines speedily, if possible jointly or at least in coordination with the European AI Office, in order to reduce the legal uncertainty in the handling of training data for AI models. These guidelines should contain clear specifications on the reuse of personal data for training purposes, considering the GDPR.

d | National legislator

Interlinked supervision: Coordination between the national market supervisory authority (e.g., the Federal Network Agency (BNetzA) in Germany) and sector-specific regulatory authorities (e.g., in the healthcare or transport sector) could be improved through closer, institutionally secured interlinking of supervision. For example, individual civil servants may be seconded from the sectoral authority to the central authority; they could then take on a hinge function and be called upon in cases that require sector-specific expertise. Furthermore, regular exchange formats (jour fixe etc.) should be set up between the respective authorities involved. This may lead to more coherent and efficient regulatory processes and reduce duplication of checks.

Introduction of a central data access portal for AI: A central portal could be developed to facilitate access to AI data for researchers and regulators to meet the requirements of the Digital Services Act (DSA) and the challenges of the AI Act. This would create transparency and improve the monitoring of high-risk AI systems. Such a portal could also be set up in national implementation laws for the AI Act. In addition, a right of access for authorized researchers should be enshrined in the AI Act for GPAI and high-risk systems, as in Art. 40 (8) DSA, although this would be the responsibility of the European legislator.

Strengthening sectoral education and training: For companies in regulated sectors, government scholarship programs could be set up to (co-)finance participation in specific, standard market training programs. In the related area of cybersecurity, entire awareness campaigns and training programs are provided by the European authority (ENISA) (Art. 10 Cybersecurity Act). In particular small and medium-sized enterprises (SMEs), including start-ups, should thus be prepared for the requirements of the AI Act and sector-specific regulations at reduced costs. This could ensure that companies can better understand and implement not only the technical but also the legal requirements. This enables medium-sized companies to explore at an early stage which AI applications could be useful for them, and which are not. The aim would be to prevent SMEs from refraining from socially useful AI applications due to concerns about costs and compliance.

e | National supervisory authorities

Guidelines (national AI supervision, AI Office if applicable): National supervisory authorities, including, where appropriate, the AI Office that has now been established at the European Commission, should develop detailed guidelines to provide clarity on how the AI Act should be applied in specific cases where sectoral regulation also comes into play. These non-committal guidelines may also consider sector-specific differences and thus precisely control and facilitate the development and use of AI. However, the prerequisite is that the authorities are also provided with the appropriate resources to develop such guidelines – in addition to their day-to-day business.

Harmonization with the GDPR (national AI supervision and data protection supervision): In order to mitigate conflicts between the AI Act and the GDPR, enhanced cooperation mechanisms between the competent authorities should also be established (see also section IV.1.d) above). National AI regulators need to work closely with data protection authorities to ensure that both regulations are implemented coherently and that frictions are mitigated through guidance and advice. However, such cooperation obligations have not yet been sufficiently specified, which could lead to uncertainties in practice. For example, an internal guideline that provides for consultation of the data protection authorities by the market supervisory authority at least whenever the GDPR is relevant for the assessment of AI Act compliance would appear to make sense. This is regularly the case in the cases discussed in Section II.2 (e.g., AI training; bias reduction).

All in all, harmonization between the AI Act and the GDPR remains challenging and must be addressed both at legal and technical levels to protect the interests of data subjects and at the same time enable socially desirable innovations in the field of artificial intelligence, in particular in the EU and Germany.

Cooperation between the supervisory authorities: Regulatory authorities must also work closely together to facilitate the implementation of both sets of regulations. An agile structure should be introduced for this within the national AI Act market surveillance authority, bringing together permanent staff and those seconded from sectoral authorities. Teams may and must be formed from case to case to combine the AI competencies of the market surveillance authority with the technical expertise of the seconded persons in each specific situation at hand. Exchange with the AI Office is important as well, which means that a permanent, new, and comprehensive AI Enforcement Hub with the corresponding expertise, feedback, and structured learning processes may be established.[55]

Strengthening sectoral expert committees: Sector-specific expert committees should also be set up within the market surveillance authority to coordinate the implementation of the AI Act in conjunction with sector-specific regulations. Its members should be recruited primarily from science and civil society, but also from industry. These bodies may ensure that specific risks and particularities of individual sectors are adequately considered in the context of the AI Act and its enforcement.

f | Standardization organizations

Development of overarching technical standards: The AI Act is supplemented by standards that are currently being developed to support its practical implementation. Overarching technical standards may be established as safe-harbor mechanisms for the AI Act and sectoral regulations as well as under other digital laws such as the GDPR in order to reduce legal uncertainties. Such standards may help companies meet the requirements of several sets of regulations at the same time. If there is no lead act or delegated act that ensures a clear distinction (see recommendation IV.1.a and b), these standards can be used to establish concrete cross-links between the AI Act and

55 See also Novelli et al. 2024: 4.

sectoral regulation. If the standards are met, there is a presumption of conformity with the corresponding requirements of the AI Act (Art. 40 (1) AI Act).

g | Companies

Utilization and update of existing compliance systems: Companies that already operate established compliance systems for other regulations (e.g., GDPR, product safety law) can adapt these for the AI Act. However, the specific innovations brought about by the AI Act must be examined in detail and the differences from existing requirements and practices must be clarified. Such innovations must then be translated into corresponding compliance routines. Their integration may reduce the effort required for additional compliance procedures and facilitate the introduction of the AI Act into existing operational structures.

Codes of Practice: The development of Codes of Practice in accordance with Art. 56 AI Act constitutes a flexible method for regulated self-regulation and could promote harmonized implementation in various industries. Sectoral codes in particular could operationalize sector-specific requirements and ensure effective cooperation between regulators and companies.

h | Jurisprudence

Lex specialis: The general legal methodology must be applied in cases without a designated Lead Act, e.g., also the principle of the primacy of the special rule („lex specialis derogat legi generali"[56]). This means that more specific regulations, such as those contained in sector-specific regulations, generally take precedence over the general rules of the AI Act. Specifically, this may mean If the provisions on the necessary performance of a medical device under the Medical Device Regulation (MDR) are met, no further requirements on "accuracy" can be derived from the more general Art. 15 (1) AI Act. However, it must be clarified from case to case whether the sectoral regulation (material proximity) or the AI Act (technical proximity) is actually the more specific standard. This must be decided on a case-by-case basis. Jurisprudence can make a significant contribution to systematization here;[57] these rules should then be taken up in guidelines issued by the authorities or in specific court rulings.

2. Medium- and long-term actions

While short-term actions are primarily targeted at regulatory authorities, national legislators, standard-setting organizations, and companies themselves, fine-tuning of the AI Act as such and its related digital laws will be necessary in the medium and long term. This is primarily the responsibility of the European legislator, but national legislators are also required to implement the laws.

a | European legislator

Greater use of specific references in the legal text: The AI Act includes obligations for regular evaluations (Art. 112 AI Act). These also are to shed some light on the sectoral interfaces. In the event of revision, further explicit references to other relevant regulations would then have to be included in order to avoid overlaps and ambiguities. These references should clarify the legal framework and harmonize the application of the legal acts concerned. Art. 17 (4) AI Act serves as a model here.

Harmonization with the GDPR: As the AI Act requires the processing of sensitive data in some areas, exemptions from and links to the GDPR should be phrased more clearly and comprehensively. The requirements of the GDPR and the AI Act should be better coordinated, in particular for GPAI models and systems that process discrimination-sensitive data.

56 A special law (lex specialis) will take precedence over the general law (lex generalis) and therefore has priority of application.

57 See Hacker 2020: § 5 A.II. with further documentation.

Art. 10 (5) AI Act stipulates an exception from the prohibition of processing of sensitive personal data set out in Art. 9 GDPR. Such data may now be processed if processing serves to reduce discriminatory bias in high-risk AI systems and a number of precautions are taken to protect fundamental rights. This sensible exception should be extended by law to all AI systems in order to enable powerful and at the same time discrimination-sensitive models. Otherwise, the GDPR and the AI Act would needlessly obstruct each other, especially in the particularly important field of generative AI. It also appears to be much more efficient economically to reduce discrimination once at the source (the basic model) than separately in each individual (high-risk) application.

It should also be made clear that the exception for sensitive data also applies to non-sensitive personal data: Apart from this, sensitive data may be processed to reduce discrimination, while "regular" personal data must not be, which would be contradictory. At present, this rule on personal data will have to be read into the balancing test in accordance with point (f) of Art. 6 (1) GDPR.

Furthermore, new exemptions such as those stipulated by Art. 10 (5) of the AI Act are necessary to enable a balanced use of data that both ensures the protection of data subjects through special procedural safeguards and enables innovative solutions in key areas of social importance, such as medicine. Otherwise, Art. 9 GDPR may come into conflict with the performance criteria in Art. 15 AI Act. The Health Data Utilization Act takes the first steps in this direction (see section II.2.d) above).

Legal framework for AI training: In the medium term, a coherent legal framework is required that integrates both the AI Act and the GDPR with regard to training data in order to promote the development of responsible and data protection-compliant AI in Europe. It must be ensured that this framework enables and promotes innovation, in particular in areas where compliance is complex due to overlaps with sectoral regulation. At the same time, fundamental rights must be duly considered by way of procedural regulations as well as with hard limits on data use where necessary.

Revision of the AI Act thus should aim to create an explicit exception for the use of data for training purposes. However, only the European legislator is called upon to do this. While there is already an exception for text and data mining in copyright law, there is no such regulation in data protection law. This gap could be closed with a revision of the AI Act, as already provided for specific purposes (e.g., reducing discrimination in medical AI) in its Art. 10 (5).

Any new exemption from the protection of sensitive data under Art. 9 GDPR for AI training should be sector-specific, with strict procedural safeguards (cf. Art. 10 (5) AI Act and Art. 22 (3) GDPR) and an opt-out option (cf. Art. 21 GDPR) if necessary.[58] Art. 10 (5) AI Act could serve as a template to regulate specific areas of application such as medical AI. As in Art. 10 (5) AI Act, a limitation to specific purposes (e.g., training for medical AI or for specific robotics) with stringent, procedural safeguards for data subjects is then required. Protection of health-related data in Germany in particular has become a jungle that is difficult to penetrate due to fragmented regulations at state level, which no longer provides an adequate basis for sophisticated research (see also section II.2.d) above on the GDNG).

Content moderation at model level: It would also be a useful extension if trusted whistleblowers could also report harmful prompts and illegal output from generative AI systems, e.g., on hybrid platforms, but also in other generative AI systems, in accordance with Art. 22 DSA. This would enable a comprehensive integration of platform and AI risks and ensure that risks are covered at both platform and AI level.

58 Also see the text and data mining exception in copyright law, for example Raue 2021: 793.

b | National legislator

Connection of implementing laws: In the medium term, national legislators should ensure that the various implementing laws and supplementary regulations for the individual digital laws, such as the GDPR, the Digital Services Act (DSA) and the AI Act, are revised and linked in a coherent manner. This means that certain synergies, for example in the area of data access or risk management, can be supported even better at a legal level.

3. Long-term actions

Finally, European and national legislators and supervisory authorities also must take actions for ongoing improvement of the fine-tuning of AI, digital and sectoral regulation on a solid data basis in the longer term. This way, the short and medium-term actions can also be taken up and developed further.

a | European legislator

Basic Evaluation AI Act: The AI Act should be fundamentally reviewed externally, empirically, and theoretically, even beyond Art. 112 AI Act following an appropriate period of application, and it should be evaluated for its impact on the protection of fundamental rights and the development and application of AI. Another area that bears examination is whether or not liability rules in conjunction with prohibitions on socially undesirable practices, rules on GPAI and transparency requirements could be sufficient, possibly without retaining the specific procedural and substantive rules for high-risk AI (e.g., Art. 8 to 27 AI Act). This may enable leaner compliance while at the same time maintaining incentives to develop and use responsible AI, even in the previous high-risk areas – on the basis of the liability law that has been tightened and possibly readjusted by the recast of the Product Liability Directive and possibly the AI Liability Directive. Sectoral regulation that would also continue to apply in such areas may be adapted as well. Data subject rights that have proven their worth could then be retained in the AI Act; however, they come alongside the often sharper sword of data subject rights under the GDPR.

b | National legislator

Supervisory architecture: The cooperation established over time between the various sectoral and AI-specific supervisory authorities should be institutionalized. This requires a clear legal framework that defines responsibilities, communication channels and decision-making processes.

c | Supervisory authorities

Framework for cooperation and evaluation: Evidence-based mechanisms for evaluation are required to ensure and continuously improve the effectiveness of this cooperation. They should periodically assess the cooperation based on defined criteria such as speed, consistency, and completeness of the exchange of information as well as the ability to develop joint positions and actions. The results from these evaluations should be published as far as appropriate and used in any case to continuously adapt and optimize the cooperation structures and processes.

Table 1 **Overview of the recommendations for action**

Time frame	Actor	Action	Description
Short term	European legislator	Designation of a "Lead Act"	A "Lead Act" as the primary legal framework for minimizing conflicts in AI applications
Short term	European Commission (esp. AI Office)	Stronger interlinking of regulations	Clearer definitions and precise information in implementing regulations
Short term	European Commission	Implementation of integrated risk analyses	For VLOPs/VLOSes with generative AI by AI Office and VLOP/VLOSE supervision
Short term	European Commission (esp. AI Office)	Definition of practical guidelines for content moderation	In guidelines under Art. 56 AI Act, considering possible negative consequences for freedom of expression
Short term	European Data Protection Board	Development of specific guidelines	On handling of training data to reduce legal uncertainties in harmonization with the GDPR
Short term	National legislator	Institutional integration of supervision	Between the national AI supervisory authority and sector-specific regulatory authorities
Short term	National legislator	Establishment of a central data access portal	For access to AI data for researchers and regulators
Short term	National legislator	Support for training courses	Scholarships for SMEs in regulated sectors to prepare for AI Act and sector-specific regulations
Short term	National supervisory authorities	Development of detailed guidelines	On the application of the AI Act in the case of sectoral regulation by national AI supervisory authorities and, where applicable, the AI Office
Short term	National supervisory authorities	Establishment of enhanced cooperation mechanisms	Between national AI supervision and data protection supervision for harmonization with the GDPR
Short term	National supervisory authorities	Introduction of an agile structure	Within the national AI supervisory authority with delegations from sectoral authorities for case-specific teams
Short term	National supervisory authorities	Establishment of sector-specific expert committees	Within the national AI supervisory authority to coordinate the implementation of the AI Act
Short term	Standardization organizations	Introduction of overarching technical standards	As safe harbor mechanisms for AI Act, sectoral regulations, and other digital laws
Short term	Standardization organizations	Developing technical standards	As safe harbor mechanisms for the AI Act and GDPR to create legal certainty
Short term	Companies	Adaptation of established compliance systems	For the AI Act by examining specific innovations and translating them into corresponding compliance routines
Short term	Companies	Development of codes of practice	In accordance with Art. 56 AI Act for flexible regulated self-regulation and harmonized implementation in various industries
Short term	Jurisprudence	Systematization of the standards and their relationship	To clarify precedence of more specific sectoral regulations over general rules of the AI Act in individual cases

Time frame	Actor	Action	Description
Short term	European legislator	Greater use of specific references in the legal text	With explicit references to other relevant regulations in the AI Act to avoid overlaps and ambiguities
Medium-term	European legislator	Harmonization with the GDPR	Clearer and more comprehensive formulation of exemptions and links to the GDPR, in particular for GPAI models and systems
Medium-term	European legislator	Legal framework for AI training	Revision of the AI Act to create an explicit exception for the use of data for training purposes
Medium-term	European legislator	Content moderation at model level	Extension of the DSA to allow trusted whistleblowers to report harmful prompts and illegal outputs from generative AI systems
Medium-term	National legislator	Linking of implementing laws	Coherent revision and linking of the various implementing laws and supplementary regulations for digital laws
Long-term	European legislator	Evaluation AI Act and new architecture of AI regulation	Fundamental review of the AI Act and examination of a new architecture for AI regulation based on liability rules, rules for GPAI and transparency requirements
Long-term	National legislator	Supervisory architecture	Institutionalization of cooperation between sectoral and AI-specific supervisory authorities through a clear legal framework
Long-term	Supervisory authorities	Framework for cooperation and evaluation	Development of evidence-based mechanisms for the regular evaluation of cooperation and ongoing adaptation of cooperation structures and processes

Source: own presentation

List of sources

Aboy, Mateo, Timo Minssen, and Effy Vayena (2024). "Navigating the EU AI Act: implications for regulated digital medical products". *npj Digital Medicine* 7 art. no. 237. https://doi.org/10.1038/s41746-024-01232-3.

Braegelmann, Tom (2024). "KI-VO und Compliance – aktuelle Brennpunkte". *Künstliche Intelligenz und Recht (KIR)* 2. 39–42.

Carl, Ann-Kathrin, and David Hochmann (2023). "Impact of the new European medical device regulation: a two-year comparison". *Biomedical Engineering / Biomedizinische Technik* (69) 3. 317–326. https://doi.org/10.1515/bmt-2023-0325.

De Bruyne, Jan, Orian Dheu, and Charlotte Ducuing (2023). "The European Commission's approach to extra-contractual liability and AI – An evaluation of the AI liability directive and the revised product liability directive". *Computer Law & Security Review* (51) Article 105894. https://www.sciencedirect.com/science/article/abs/pii/S0267364923001048 (Download 11/19/2024)

Eber, Maximilian, and Philipp Hacker (i. E.). "Policy Brief on the Future of Credit Underwriting under the EU AI Act: Implications for Europe and beyond".

Engeler, Malte, and Louis Rolfes (2024). "Datenschutzrechtliche Korrekturansprüche bei Erzeugung von Falschinformationen durch LLMs". *Zeitschrift für Datenschutz (ZD)* 8. 423–428.

Feldkamp, Jakob, Quirin Kappler, Maximilian Poretschkin, Anna Schmitz, and Erik Weiss (2024). "Rechtliche Fairnessanforderungen an KI-Systeme und ihre technische Evaluation – Eine Analyse anhand ausgewählter Kreditscoring-Systeme unter besonderer Berücksichtigung der zukünftigen europäischen KI-Verordnung". *Zeitschrift für Digitalisierung und Recht (ZfDR)* 60.

Gierschmann, Sibylle (2020). "Gemeinsame Verantwortlichkeit in der Praxis". *Zeitschrift für Datenschutz (ZD)* 2. 69–72.

Gkritsi, Eliza (2024). "X suspends processing of some personal data for AI training". *EURACTIV* 9.8. https://www.euractiv.com/section/data-privacy/news/x-suspends-processing-of-some-personal-data-for-ai-training/ (Download 11/10/2024).

Hacker Philipp (2024). *Proposal for adapting non-contractual civil liability rules to artificial intelligence: Complementary impact assessment.* Study written at the request of the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament, requested in turn by the JURI Committee of the European Parliament, September 19. Strasbourg: European Parliamentary Research Service. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2024)762861 (Download 11/10/2024).

Hacker Philipp (2023). "The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future": *Computer Law &*

Security Review (51) Article 105871. https://www.sciencedirect.com/science/article/pii/S026736492300081X?via%3Dihub (Download 11/19/2024).

Hacker, Philipp (2021). "A legal framework for AI training data – from first principles to the Artificial Intelligence Act". *Law, Innovation and Technology* (13). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3556598 (Download 11/19/2024).

Hacker, Philipp (2020). *Datenprivatrecht: Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB*. Tübingen.

Harrington, Esme, and Mathias Vermeulen (2024). *External researcher access to closed foundation models. State of the field and options for improvement.* Report. https://blog.mozilla.org/wp-content/blogs.dir/278/files/2024/10/External-researcher-access-to-closed-foundation-models.pdf (Download 11/19/2024).

Hense, Peter (2024). "Overfitting". *Multimedia und Recht (MMR)* 6. 449–450.

Hermstrüwer, Yoan (2016). *Informationelle Selbstgefährdung*. Tübingen.

Hüger, Jakob (2024). "Die Rechtmäßigkeit von Datenverarbeitungen im Lebenszyklus von KI-Systemen". *Zeitschrift für Digitalisierung und Recht (ZfDR)* 3. 263–292.

Kilian Robert (2024a). "Nationale Spielräume bei der Umsetzung des Europäischen AI Act". *Zeitschrift für Rechtspolitik (ZRP)* 5. 129–160.

Kilian Robert (2024b). "Nationale Spielräume bei der Umsetzung des Europäischen Gesetzes über Künstliche Intelligenz". Written statement for the 63rd meeting of the Committee for Digital Affairs of the German Bundestag on May 15th, 2024. www.bundestag.de/resource/blob/1002540/2c7af0e644c2d1b19d20896994727736/Kilian.pdf (Download 11/19/2024).

Köllner, Christiane (2024). "Was bedeutet das KI-Gesetz für die Autoindustrie?". *Springer Professional* 1.8. https://www.springerprofessional.de/kuenstliche-intelligenz/automatisiertes-fahren/was-bedeutet-das-ki-gesetz-fuer-die-autoindustrie-/26700940 (Download 11/10/.2024).

Marano, Pierpaolo, and Shu Li (2023). "Regulating robo-advisors in insurance distribution: Lessons from the Insurance Distribution Directive and the AI Act". *Risks* (11) 12. https://www.mdpi.com/2227-9091/11/1/12 (Download 11/19/.2024).

Novelli, Claudio, Frederico Casolari, Philipp Hacker, Giorgio Spedicato, and Luciano Floridi (2024). "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity". *Computer Law & Security Review* (forthcoming), Article 106066. https://www.sciencedirect.com/science/article/pii/S0267364924001328?via%3Dihub (Download 11/19/2024).

Onitiu, Daria, Sandra Wachter and Brent Mittelstadt (2024). "How AI challenges the medical device regulation: patient safety, benefits, and intended uses". *Journal of Law and the Biosciences* lsae007. https://doi.org/10.1093/jlb/lsae007.

Radtke, Tristan (2024). "Das Verhältnis von KI-VO und Art. 22 DS-GVO unter besonderer Berücksichtigung der Schutzzwecke". *Recht Digital (RDi)*. 353–360.

Rauch, Pauline, Carina Richters, and Christoph Naucke (2024). "Gesundheitsdatennutzungsgesetz: Der Zielkonflikt zwischen Datenschutz und Datennutzung". *GesundheitsRecht* 218. https://www.degruyter.com/document/doi/10.9785/gesr-2024-230404/html (Download 11/19/2024).

Raue, Benjamin (2021). "Die Freistellung von Datenanalysen durch die neuen Text und Data Mining-Schranken (§§ 44b, 60d UrhG)". *Zeitschrift für Urheber- und Medienrecht (ZUM)* 2021. 793–802. https://irdt.uni-trier.de/wp-content/uploads/2022/02/formatiert_Raue_ZUM-2021-793.pdf (Download 11/19/2024).

Reichert, Florian, Kristina Radtke, and Hermann Eske (2024). "KI-Verordnung, Rechtsgrundlagen für die Bereitstellung und Nutzung von KI". *Zeitschrift für Datenschutz (ZD)* 9. 483–489.

Schemmel, Frank (2024). "Grundrechte- und Datenschutz-Folgenabschätzung – zwei Seiten einer Medaille des Daten-Risikomanagements". *Compliance Berater (CB)* 9. 321–325.

Schneider, Uwe K., and Till Katzenstein (2024). "Weiterverarbeitung von Versorgungsdaten nach § 6 GDNG". *Gesundheit und Pflege (GuP)* Issue 5. 196–202).

Theisen, Susanne (2024). "Eine neue Form der Übergriffigkeit". *Zahnärztliche Mitteilungen (ZM)* 3. 54–55.

van Bekkum, Marvin and Frederik Zuiderveen Borgesius (2023). "Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?". *Computer Law & Security Review* 48 Article 105770. https://www.sciencedirect.com/science/article/pii/S0267364922001133?via%3Dihub (Download 11/19/2024).

VDA – Verband der deutschen Automobilindustrie (2023). "Position Artificial Intelligence Act". Berkin. https://www.vda.de/de/aktuelles/publikationen/publication/ki-verordnung---artificial-intelligence-act-- (Download 11/21/2024).

Wachter Sandra (2024). "Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond". *Yale Journal of Law & Technology* (26) 3.

Wagner, Gerhard (2022). "Liability Rules for the Digital Age – Aiming for the Brussels Effect". *European Journal of Tort Law* 191. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4320285 (Download 11/19/2024).

Weatherbed, Jess (2024). "Meta fed its AI on almost everything you've posted publicly since 2007". *The Verge* 12.9. https://www.theverge.com/2024/9/12/24242789/meta-training-ai-models-facebook-instagram-photo-post-data (Download 11/10/2024.mm.yyyy).

Weichert, Thilo (2023). "Gesundheitsdatennutzung contra heilberufliche Vertraulichkeit. Eine Kritik am Referentenentwurf für ein Gesundheitsdatennutzungsgesetz". Network data protection expertise (as of 08/09/2023). https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2023_08_gdng.pdf (download 11/10/2024).

Werry, Susanne and Elena Ntanas (2024). "Sekundärnutzung von Gesundheitsdaten – Quid deinde?". *Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR)* 641.

Woesch, Philippe and Melanie Vogt (2024). "Die KI-Verordnung – Die digitale Zukunft im Finanzsektor". *Bank- und Kapitalmarktrecht (BKR)* 16. 689–736.

Adresse | Kontakt

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Phone +49 5241 81-0
bertelsmann-stiftung.de

Asena Soydaş
Project Manager
Digitalization and the Common Good
Phone +49 5241 81-81247
asena.soydas@bertelsmann-stiftung.de