Challenges of the European legal framework for AI models and AI systems

Professor Dr. Georg Borges, Saarland University

Expert opinion commissioned by the National Institute of Informatics, Tokyo

I. Introduction

The National Institute of Informatics (NII) commissioned the author to prepare an expert opinion on the challenges arising from the European Union's legal framework for Japanese providers of AI models and AI systems.

The expert opinion analyses the challenges from the perspective of Japanese manufacturers and users of AI systems that are exported to the EU, integrated into products for the European market, or used in the provision of services for European customers. The report considers key aspects of the European legal framework for AI that pose particular challenges for Japanese providers and users. The assessment includes the European AI Regulation (below II), aspects of data protection law (below III.) and copyright law (below IV), as well as liability for AI systems and products containing AI components (below V).

II. Challenges of the European AI Act for providers and deployers of AI systems and models from third countries

The European AI Act (AI Act)[1] came into force on 1 August 2024. Some parts of it are already applicable, while others will gradually become applicable by 2027 (see section 2(d) below). It is also of considerable importance for providers and deployers of AI systems, as well as for providers of general-purpose AI models outside the European Union.

The significance of the AI Act for providers and deployers of AI systems and general-purpose AI models from third countries is discussed below. After an overview of the provisions of the AI Act (see section 1 below), its scope of application (see

---

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), OJ L, 2024/1689, 12.7.2024.

section 2 below) is discussed, and the main regulatory standards (see sections 3 to 6 below), as well as public oversight (see section 7 below), are presented. On this basis, the significance of the AI Act for providers from third countries is then elaborated (see section 8 below).

1. An overview of the AI Act

The AI Act is an impressive piece of work, if only because of its enormous scope.[2] It comprises 13 chapters, totalling 113 articles, and the legislature's intention is explained in 180 recitals.

a. Regulatory concepts of the AI Act

The AI Act is based on four key substantive regulatory concepts.[3] These are: firstly, the prohibitions on certain uses of AI systems; secondly, the regulation of risk management for so-called high-risk AI systems and general-purpose AI models; thirdly, transparency requirements for generative AI systems; and lastly, promotion of the development and marketing of AI systems, accompanied by the waiver of specific obligations for what is estimated to be over 99% of all AI systems.

The pyramid shape often used in the media and the accompanying division into "minimal", "limited", "high" and "unacceptable" risks,[4] which suggests a ranking of risk classes with alternative classifications, is misleading, as the regulatory concepts coexist and are independent of each other.[5] The prohibitions and transparency obligations (cf. Art. 50(6) AI Act) are therefore independent of the classification as a high-risk AI system.[6] For example, a chatbot may be subject to both transparency obligations and the obligations for high-risk AI systems, but regardless of this, a specific use of the chatbot may still be prohibited under Article 5 AI Act.

These substantive regulatory concepts are supplemented by concepts of public oversight and cooperation between Member States in the enforcement of the rules.

---

2 *Borges*, CR 2024, 497, 498 (para. 10).

3 *Borges*, CR 2024, 497 (para. 3); *Roth-Isigkeit*, KIR 2024, 15, 17.

4 See the relevant description on the Commission's website at https://digital-strategy.ec.europa.eu/de/policies/regulatory-fr a mework-ai (last accessed on 9 October 2025).

5 *Borges*, CR 2024, 497 (para. 4).

6 *Guckelberger*, DÖV 2025, 45, 52; *Kirschke-Biller/Füllsack*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 83 (each with regard to transparency obligations).

The AI Act deliberately does not contain any rules on liability for AI systems.[7] With regard to data protection, the GDPR expressly takes precedence (Art. 2(7) AI Act). The AI Act is also silent in other areas where special rules for AI appear necessary, such as intellectual property law. In this respect, the general rules remain in place (for now).[8]

b. Overview of the subjects regulated by the AI Act

The AI Act contains quite different areas of regulation in its 13 chapters. Chapter I ("general provisions") with Articles 1 to 4 essentially contains the usual introductory rules. Article 2 of the AI Act regulates the material, personal and territorial scope of the Regulation (see section # below).

Chapter II ("prohibited AI practices") is extremely short, containing only Article 5 AI Act. This provision, which is largely independent of other regulatory areas, contains a short list of eight prohibited practices (see section # below).

The central and, by far, the most comprehensive part of the AI Act is Chapter III ("High-risk AI systems"), comprising Articles 6 to 49 (see section # below), which essentially contains provisions on risk management for such AI systems. Chapter V ("general-purpose AI models") with Articles 51 to 56, the most controversial area of the AI Act during the legislative process, also contains provisions on risk management.

Chapter IV ("transparency obligations for providers and deployers of certain AI systems") consists solely of Article 50 AI Act, which regulates transparency obligations in relation to generative AI systems (see section # below).

Chapter VI ("measures in support of innovation") contains a number of different provisions in Articles 57 to 63 AI Act, which is essentially a comprehensive regulation on so-called *regulatory sandboxes*.

Chapter VII ("governance") with Articles 64 to 70 AI Act, exclusively regulates the establishment and tasks of new institutions to be set up. The chapter is divided into two sections. Section 1 on "governance at Union level", which comprises Articles 64 to 69 AI Act, and Section 2 on "national competent authorities", comprising Article 70 AI Act. A total of four new institutions are to be created at Union level,

---

7 *European Commission*, Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SWD(2021) 84 final, p. 1.

8 *Borges*, CR 2024, 497, 498 (para. 6).

i.e., an AI Office (Art. 64 AI Act), an AI Board (Art. 65 AI Act), an Advisory Forum (Art. 67 AI Act) and a Scientific Panel of Independent Experts (Art. 68 AI Act).

Article 70 AI Act governs the establishment and tasks of national authorities.[9] According to Article 70(1) AI Act, each Member State must establish or designate a notifying authority within the meaning of Article 28 AI Act and a market surveillance authority. The market surveillance authority acts as the single point of contact for the AI Act (Article 70(2) sentence 3 AI Act). Member States may concentrate the tasks of the two authorities into a single authority or assign them to different authorities.

The brief Chapter VIII, consisting of Article 71 AI Act, regulates the establishment of an EU database for high-risk AI systems within the meaning of Annex III.[10] The database contains certain information listed in Annex VIII on high-risk AI systems and on systems operating in high-risk areas which, due to their "low-risk" classification pursuant to Article 6(3) AI Act, are registered under Article 49 or Article 60 AI Act (Article 71(1), first sentence). The information to be included in the database is specified in Article 71(2) and (3) AI Act by reference to Annex VIII. The database is maintained by the Commission (Article 71(6) AI Act), and, in principle, the information contained therein is publicly accessible (Article 71(4) AI Act).

The comprehensive Chapter IX ("post-market monitoring, information sharing and market surveillance"), comprising Articles 72 to 94 AI Act, sets out the essential supervision mechanism in five sections. Section 1 of Chapter IX governs the obligations of providers of high-risk AI systems regarding the monitoring of such systems after they have been placed on the market. According to Article 72(1) AI Act, providers must establish and document a risk-appropriate system for monitoring high-risk AI systems after they have been placed on the market. According to Article 72(3) AI Act, the system must be based on a post-market monitoring plan that is part of the technical documentation within the meaning of Annex IV. The core of the chapter consists of Section 3 ("Enforcement") with Articles 74 to 84 AI Act, which regulates market surveillance, i.e. regulatory oversight, with regard to AI systems, and Section 5 comprising Articles 88 to 94 AI Act on oversight with regard to general-purpose AI models (see section # below).

Chapter XII ("Penalties"), containing Articles 99 to 101 AI Act, sets out the rules on penalties for infringements of the AI Act (see section # below).

---

9 See, for example, *Martini/Botta*, MMR 2024, 630 ff.

10 For the concept of the database, see, for example: *Botta*, Die Verwaltung 58 (2025), 19, 31 ff.

Section 4 of Chapter IX, inserted at the initiative of the Parliament,[11] containing Articles 85 to 87 AI Act, introduces new rights under the heading "Remedies" that go beyond traditional product safety law. Article 85 AI Act grants the right to lodge a complaint with a market surveillance authority. According to this provision, any natural or legal person who has reasons to believe that the provisions of the AI Act have been breached may lodge a complaint with the relevant market surveillance authority. However, the complaint has no legal consequences.[12] In this respect, Article 85 AI Act states that such a complaint shall only be taken into account for the purpose of conducting market surveillance activities in accordance with the Market Surveillance Regulation.

The right to explanation is another fascinating inclusion under Article 86 AI Act. According to this provision, persons affected by a decision taken on the basis of the output of high-risk AI systems within the meaning of Annex III (with the exception of systems listed under No. 2 of Annex III) which has legal effects or similarly significantly affects them, may request from the deployer a clear and meaningful explanation of the role of the AI system in the decision-making process and of the main elements of the decision taken.

Chapter X ("Codes of Conduct and Guidelines"), comprising Articles 95 and 96 AI Act, regulates organisational aspects for voluntary codes of conduct and Commission guidelines on implementation. According to Article 95(3) AI Act, codes of conduct may be drawn up by individual providers or deployers of AI systems, or by both. Article 96 AI Act mandates the Commission to draw up guidelines for the practical implementation of the Regulation, covering *inter alia*, the prohibited practices, transparency obligations and rules for high-risk AI systems. The legal signif-

---

11 *European Parliament*, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), Document P9_TA(2023)0236, 628 ff.

12 Art. 85(2) AI Act does not oblige market surveillance authorities to take action in every case, see *Djeffal*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 85, para. 18; Individuals cannot force the authority to deal with their complaints, see *Hartmann,* in: Martini/Wendehorst, AI Act [KI-VO], 2024, Art. 85 para. 10.

icance of the guidelines, intended to support the implementation of the AI Act, remains unsettled.[13] However, they are likely to be of considerable importance for interpreting the requirements of the AI Act.[14]

The rather extensive Chapter XIII ("Final Provisions"), containing Articles 102 to 113 AI Act, implements amendments to various other legal Acts as well as the entry into force and temporal scope of the AI Act (see section #.#).

c. Legal policy discussion and possible amendments to the AI Act

The AI Act has been the subject of intense legal policy discussion since the Commission's draft was published in April 2021. According to a press release issued upon its entry into force, the Commission sees the AI Act as a basis for the responsible development and use of AI and wants to "take a global leadership role" in this regard.[15]

Some countries have initiated legislative initiatives clearly inspired by the AI Act. Brazil, for example, introduced a related bill into the parliamentary process in 2023.[16] In South Korea, an AI law was enacted in January 2025, clearly drawing from the AI Act.[17]

So far, most countries have taken a wait-and-see approach or even explicitly rejected the regulation of AI systems. The current situation is primarily shaped by the stance of the new U.S. administration. In February 2025, just a few days after Donald Trump took office, his administration explicitly opposed the AI Act and the

---

13 *Borges*, CR 2024, 497, 502 (para. 52).

14 *Borges*, CR 2024, 497, 502 (para. 52); *Brandt,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 96 para. 2; *Weiß,* in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 96 para. 2 f., 18.

15 European Commission, Directorate-General for Communication, AI Act enters into force, 1 August 2024, available at https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_de (last accessed on 9 October 2025).

16 *Federal Senate,* Bill No. 2338/2023 – Provides for the use of Artificial Intelligence [*Senado Federal*, Projeto de Lei nº 2338/2023 – Dispõe sobre o uso da Inteligência Artificial], available at: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347593 (last accessed on 9 October 2025); see *Shimoda Uechi/Guimarães Moraes,* 'Brazil's path to responsible AI', 27 July 2023, available at: https://oecd.ai/en/wonk/brazils-path-to-responsi b le-ai (last accessed on 9 October 2025).

17 See, *South Korean Ministry of Government Legislation*, Act on the Development of Artificial Intelligence and Establishment of Trust, English translation by the *Etcetera Language Group, Inc.*, available at: https://cset.georgetown.edu/wp-content/uploads/t0625_south_korea_ai_law_EN.pdf (last accessed on 9 October 2025).

regulation of AI in general.[18] This gave considerable impetus to the global debate on the appropriate form of the AI Act. The European business community vehemently called for a simplification or postponement of the AI Act's effective date.[19]

This discussion prompted the Commission to consider postponing the date of application of parts of the AI Act or even modifying it.[20] The Commission has announced the publication of a so-called omnibus regulation on digitalisation for 19 November 2025. According to a leaked draft, a specific omnibus regulation, the "Digital Omnibus on AI", is planned, which would introduce a number of changes.[21] The draft regulation mentions changes to the following elements of the AI Act:

• Adjustment of the implementation deadlines (Art. 111, 113 AI Act). According to the leaked draft, this point is still under consideration;

• Introduction of a transitional grace period for the "watermark" obligation for AI systems (Art. 50(2) AI Act) that were placed on the market before the watermark obligations came into force;

• Extension of regulatory privileges for small and medium-sized enterprises (SMEs) to small mid-cap companies, including simplified technical documentation requirements and special consideration when imposing penalties;

• Obligation on the Commission and Member States to promote AI literacy rather than enforcing unspecified obligations on operators (Art. 4 AI Act);

• Greater flexibility in post-market monitoring by abolishing the requirement for a harmonised post-market monitoring plan;

---

18 *The White House*, Removing Barriers to American Leadership in Artificial Intelligence, 23 January 2025, available at: https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/ (last accessed on 9 October 2025).

19 See, for example, the "Stop the Clock – Open Letter" initiative, available at: https://aichampions.eu/#stoptheclock (last accessed on 9 October 2025); see also *Krempl*, "Almost 50 European CEOs call for a pause in the implementation of the AI Act", in: heise online dated 3 July 2025, available at https://www.heise.de/news/Fast-50-europaeische-Firmenchefs-fordern-Pause-bei-der-AI-Act-Umsetzung-10474192.html (last accessed on 9 October 2025).

20 See *Tobey/Stokes/Carr/Dauzier/Sterneberg/Darling/Buckley*, The European Commission considers pause on AI Act's entry into application, DLA Piper, 4 June 2025, available at: https://www.dlapiper.com/en/insights/publications/ai-outlook/2025/the-european-commission-considers-pause-on-ai-act-entry-into-application (last accessed on 9 October 2025).

21 Proposal for a Regulation of the European Parliament and of the Council on the simplification of the implementation of artificial intelligence rules, amending Regulation (EU) 2024/1689 (Digital Omnibus on AI), available at https://cdn.netzpolitik.org/wp-upload/2025/11/EU-Kommission-Digital-Omnibus-B-KI.pdf (last accessed on 9 November 2025).

• Reducing the registration burden for AI systems used in high-risk areas where the provider has concluded that they do not pose a high risk because they are only used for narrowly defined or procedural tasks (Art. 6(4), Art. 71 AI Act);

• Facilitating compliance with data protection laws by allowing providers and deployers of all AI systems and models to process special categories of personal data to ensure the detection and correction of bias, subject to appropriate safeguards (Art. 10(5) AI Act).

• Enabling broader use of AI regulatory sandboxes and real-world testing (Art. 57 ff. AI Act);

• Clarification of the interplay between the AI Act and other EU legislation;

• Centralising the oversight of AI integrated into very large online platforms and search engines within the AI Office (Art. 88 AI Act).

The overview shows that the Commission does not plan any significant changes to the AI Act. Instead, the Omnibus Regulation is primarily intended to eliminate some errors and ambiguities that have already been identified. It is also expected to postpone the temporal applicability of numerous provisions, in particular the rules on high-risk AI systems, which is necessary due to delays in implementation to date.

d. The implementation of the AI Act in the Member States

The AI Act applies directly (within its scope) in all Member States of the European Union and does not require implementation. It also only provides for selective implementing acts by the Member States and thus relies heavily on uniform application at the European level.

The Member States must, above all, designate the authorities provided for in the AI Act and equip them with the necessary resources to perform their tasks. These are primarily: the market surveillance authorities within the meaning of Article 70 AI Act, responsible for supervising high-risk AI systems in the Member State concerned; the notifying authorities within the meaning of Article 28 AI Act, which designate and supervise the notified bodies within the meaning of Article 31 AI Act; and the authorities responsible for the protection of fundamental rights within the meaning of Article 77(1) AI Act, in relation to the high-risk AI systems referred to in Annex III AI Act.

In this regard, Member States are taking very different approaches.[22] In many cases, the implementing measures are adopted through formal legislation, but in some cases also through other forms of regulation. Denmark was the first Member State to enact an implementing law for the AI Act,[23] followed by Italy.[24] In Germany[25], Finland[26], Luxembourg[27], Poland[28], and Spain[29], legislative projects are currently underway or in preparation.

2. The scope of the AI Act

a. AI systems and general-purpose AI models as the subject matter of the AI Act

The AI Act does not apply comprehensively to artificial intelligence as such but, according to Article 2(1), to AI systems and general-purpose AI models (see section

---

22 See an overview of national implementation plans, available at https://artificialintelligenceact.eu/national-implementation-plans/ (last accessed on 31 October 2025).

23 Act No. 467 14/05/2025 – Act on Supplementary Provisions to the Regulation on Artificial Intelligence [LOV nr 467 af 14/05/2025, Lov om supplerende bestemmelser til forordningen om kunstig intelligens], available at https://www.retsinformation.dk/eli/lta/2025/467 (last accessed on 10 November 2025).

24 Law No. 132 of 23 September 2025 – Provisions and Delegations to the Government on Artificial Intelligence, Official Gazette of the Italian Republic, No. 223 of 25 September 2025. [LEGGE 23 settembre 2025, n. 132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale, Gazzetta Ufficiale della Repubblica Italiana, n. 223 del 25 settembre 2025].

25 Draft bill by the Federal Ministry of Digital and Public Administration, Draft law on the implementation of the AI Act (status: 11 September 2025, 15:44), available at https://bmds.bund.de/fileadmin/BMDS/Dokumente/Gesetzesvorhaben/CDR_Anlage1-250911_RefE_KIVO-Durchf%C3%BChrungsgesetz_Entwurf_barrierefrei.pdf (last accessed on 10 November 2025).

26 *Finnish Government*, Government proposal to Parliament for a law supplementing the EU AI Act [Hallituksen esitys eduskunnalle EU:n tekoälyasetusta täydentäväksi lainsäädännöksi], HE 46/2025 vp, 2 August 2025, available at https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_46+2025.pdf (last accessed on 10 November 2025).

27 *Chamber of Deputies of the Grand Duchy of Luxembourg*, Draft Law No. 8476 implementing certain provisions of Regulation (EU) 2024/1689 of the European Parliament and of the Council and amending various laws, submitted on 23 December 2024, Parliamentary file 8476 (Submission document), available at https://wdocs-pub.chd.lu/docs/Dossiers_parlementaires/8476/20250515_Depôt.pdf (last accessed on 10 November 2025).

28 *Ministry of Digital Affairs*, Draft Act on Artificial Intelligence Systems of 15 October 2024, available at https://legislacja.rcl.gov.pl/docs//2/12390551/13087907/13087908/dokument687327.docx (last accessed on 10 November 2025).

29 *Ministry for Digital Transformation and Public Administration*, Draft Bill on the Proper Use and Governance of Artificial Intelligence, text version dated 6 March 2025, available at https://avance.digital.gob.es/_layouts/15/HttpHandlerParticipacionPublicaAnexos.ashx?k=19128 (last accessed on 10 November 2025)

below).[30] It primarily lays out the obligations of so-called providers of AI systems and general-purpose AI models, as well as of deployers of AI systems (see Section # below).

aa. AI system and general-purpose AI model

The term "AI system"[31], as defined in Article 3 No. 1 AI Act, is of fundamental importance.[32] The definition was rightly very controversial during the legislative process,[33] and is also extremely complex and ambiguous in the version that has now become law.[34] The definition, which is intended to distinguish AI systems primarily from traditionally programmed software, describes the characteristics of an AI system by means of four features: An AI system is (1) a machine based system that (2) generates outputs based on inputs it receives, which (3) contain relevant information for the potential recipient that can influence physical or virtual environments, and (4) acts with a certain degree of autonomy, i.e. generates the output through a derivation process that is difficult to trace due to its complexity.[35] In its guidelines on the definition of an AI system in accordance with the wording of Article 3 No. 1 AI Act, the Commission refers to seven characteristics to be taken into account.[36] This definition is essentially intended to cover software based on an AI model that has not been programmed in the traditional way, but has been generated using artificial intelligence methods, namely machine learning (see recital 12 AI Act). [37]

The term "general-purpose AI model" is defined in Article 3 No. 63 AI Act. Essentially, these are AI models that (1) display significant generality, (2) are capable of

---

30 *Borges*, CR 2024, 497, 503 (para. 64); *Voigt*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 2 para. 16.

31 Art. 3 No. 1 AI Act states that: "AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".

32 *Borges*, CR 2023, 706, 707 (para. 6, 8).

33 *See Glauner/Pieper*, in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 3 para. 16 ff.

34 *Borges*, CR 2024, 497, 503 (para. 65).

35 *Borges*, CR 2024, 497, 503 (para. 66).

36 *European Commission*, Commission Guidelines on the definition of an artificial intelligence system under Regulation (EU) 2024/1689 (AI Act), C(2025) 5053 final, para. 9.

37 *Blasek*, KIR 2025, 100, 102; *Borges*, CR 2024, 497, 503 (para. 66); "Simplistic comparisons", in particular of machine learning and rule-based software development, rejected by *Kirschke-Biller/Füllsack,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 21.

performing a wide range of distinct tasks, and (3) can be integrated into a variety of downstream systems or applications.[38] However, the definition contains an important exception. It does not cover (4) AI models that are used for research and development activities and have not (yet) been placed on the market. In summary, the term is primarily intended to cover large models,[39] such as "large language models (LLMs)".[40]

The underlying term "AI model" is not defined in the AI Act.[41] Recital 97 AI Act describes AI models as the result of training using various methods, thereby referring to neural networks and machine learning techniques.[42] An essential characteristic of an AI model is, therefore, that it independently derives the rules by which it transforms inputs into outputs on the basis of data.[43]

In computer science, the term "model" is used to emphasise the information stored within the model.[44] Unlike an AI system, an AI model does not have to be operational.[45] Notably, recital 97 AI Act points out that AI models can also exist (and be placed on the market), for example, as "physical copy". However, the distinction between an AI system and an AI model should be made based on the presence of a user interface.[46] While being an essential component of AI systems, they do not constitute an AI system on their own. AI models must be combined with other components, such as a user interface, to become an AI system. This fits with the definition of an AI system as one that can interact with its environment.[47] While the AI

---

38 *Borges*, CR 2024, 497, 503 (para. 68).

39 See, for example, EC 97 p. 3 AI Act; *Blasek*, KIR 2025, 100, 102; *Borges*, CR 2024, 497, 503 f. (para. 68).

40 *Borges*, CR 2024, 497, 504 (para. 68); see also *Biallaß,* MMR 2024, 646, 648; *Schneider/Schneider,* in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 3 para. 460 ("Probably in response to the release of ChatGPT and other well-known LLMs [...]").

41 *Bender*, KIR 2025, 3. 4; *Borges*, CR 2024, 497, 504 (para. 69); *Engel,* KIR 2024, 21, 22; *Schneider/Schneider,* in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 3 para. 462.

42 *Borges*, CR 2024, 497, 504 (para. 69).

43 See, for example, *Stiemerling*, CR 2024, 554, 556 (para. 12); see also *Steen*, KIR 2024, 7, 8 ("Principles of inference").

44 *Borges*, CR 2024, 497, 504 (para. 70).

45 *Borges*, CR 2024, 497, 504 (para. 70); according to *Blum/Rappenglück*, CR 2024, 626, 628 (para. 16), "AI models [...] cannot be used independently"; According to *Sassenberg,* CR 2025, 209, 214 (para. 31), AI models are characterised by the fact that "they are not capable of running independently".

46 *Borges*, CR 2024, 497, 504 (para. 71); see also *Kirschke-Biller/Füllsack*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 23.

47 *Borges*, CR 2024, 497, 504 (para. 71).

model is an essential component on which the performance and risks of AI systems are based,[48] it is only subject to the rules of the AI Act if it is a general-purpose AI model (see section # below).

bb. AI system and physical product

A key feature of the AI system is its nature as software (cf. recital 12 AI Act).[49] This characteristic, which was an even more explicit part of the definition in the Commission's 2021 draft[50], is not explicitly mentioned in the final text of the Act but is implied by the definition.[51]

The reference to software goes hand in hand with a fundamental conceptual decision in the AI Act: it does not apply (directly) to hardware, i.e. to physical products.[52] Insofar as physical products often contain AI systems, the product itself does not become an AI system, but rather a product that contains one or more AI systems (see also Art. 6(1) AI Act).[53] For example, a highly automated vehicle is not an AI system, but contains numerous AI systems.[54] The same applies if an AI system is integrated as a component into other software.[55] As a result, the manufacturer of the product into which an AI system is integrated is not the provider of the AI system in question (save for the circumstances foreseen under Art. 25(3) AI Act) and

---

48 *Borges*, CR 2024, 497, 504 (para. 73); on the significance of a (machine learning) model in the development of an AI application, see also *Wendehorst/Nessler/Aufreiter/Aichinger*, MMR 2024, 605, 607 f.

49 *Bauer/Merkle/Sedlmaier,* KIR 2025, 300, 301; *Borges*, CR 2024, 497, 504 (para. 74); *Chibanguza/Steege,* NJW 2024, 1769, 1770 (para. 7); *Glauner/Pieper,* in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 3 para. 30 ("AI is software"); *Klos/Taylan,* CCZ 2024, 205, 207; *Schultzky,* in: Zöller, Code of Civil Procedure [Zivilprozessordnung], 36th edition (as of 10.2025), Use of AI in civil proceedings para. 1; implicitly also *European Commission,* Commission Guidelines on the definition of an artificial intelligence system under Regulation (EU) 2024/1689 (AI Act), C(2025) 5053 final, para. 61.

50 See, Art. 3 No. 1, *European Commission,* Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union acts, 21 April 2021, COM(2021) 206 final.

51 *Borges*, CR 2024, 497, 504 (para. 74).

52 *Borges*, CR 2023, 706, 711 (para. 42). A.A., at least with regard to Art. 15(4) and arguing with the characteristic "machine-supported" in Art. 3 No. 1, *Moritz,* in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 15 para. 53.

53 *Borges*, CR 2023, 706, 711 (para. 49).

54 See *Bauer/Merkle/Sedlmaier*, KIR 2025, 300, on the use of AI in vehicles.

55 *Wendehorst/Nessler/Aufreiter/Aichinger*, MMR 2024, 605, 607 ("in the case of functionally clearly defined modules" if "the inputs and outputs of the AI system are transparently identifiable").

is therefore not addressed by the AI Act.[56] This is particularly relevant in relation to risk management for high-risk AI systems.

This truly counterintuitive result is not an oversight, but rather a correct consequence of the classification of the AI Act under product safety law.[57] The manufacturer of a product in which an AI system is integrated can only fulfil the specific risk management obligations to a limited extent. It is therefore appropriate to address exclusively the provider as the manufacturer of the respective AI system within the framework of the AI Act.[58] The manufacturer of the product in which one or more AI systems are integrated remains responsible for the overall safety of the product in accordance with the rules of product safety law and product liability, so that no gaps in protection arise.[59] This result is also ensured under the new product liability law.[60]

Focusing on the respective software rather than on the composite product necessitates precise demarcation from various perspectives. In particular, providers and deployers of composite products must determine whether, and which, AI systems are included and whether these are subject to specific rules under the AI Act.[61]

This distinction should not pose any insurmountable difficulties for product manufacturers, as both the differentiation between software and hardware and the distinction between different computer programs are familiar tasks.[62] In contrast, deployers of computer programmes, and especially composite products, will not easily be able to determine whether, which, and how many AI systems the product they are using contains.[63]

---

56 *Borges*, CR 2024, 497, 504 (para. 76); cf. *Rohrßen*, ZfPC 2025, 6, 10.

57 *Borges*, CR 2024, 497, 504 (para. 77).

58 *Borges*, CR 2024, 497, 504 (para. 77).

59 *Borges*, CR 2024, 497, 504 (para. 77); *European Commission,* Guide to the implementation of EU product rules 2022 ("Blue Guide"), OJ (EU) 2022 C 247, 1, 17; *Lejeune,* ITRB 2024, 131.

60 See, Art. 8(1), Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (Text with EEA relevance), OJ L, 2024/2853, 18.11.2024, p. 15.

61 *Borges*, CR 2024, 497, 504 (para. 78).

62 *Borges*, CR 2024, 497, 504 (para. 79).

63 The fact that users generally have difficulty understanding the exact functioning of a complex product is also assumed by recital 48 of the Product Liability Directive (Directive (EU) 2024/2853).

cc. Exceptions to the scope of application

The scope of application of the AI Act is significantly restricted by a list of exceptions.[64]The most important exception is set out in Article 2(10) of the AI Act. According to this, the AI Act does not apply to the obligations of deployers who are natural persons and use AI systems exclusively for personal and non-professional activities. The same restriction also arises from the definition of deployer in Article 3(4) of the AI Act: according to this, the use of AI systems in the context of a personal and non-professional activity is excluded from the "operation" of an AI system.

Thus, as is typical for product safety law, the regulation is characterized as a regulation for commercial use, and consumers are excluded from its scope of application.[65] Whether the term "professional" activity includes dependent professional activity can be left open, since according to Art. 3 No. 4 AI Act, an operator is only someone who uses the AI system "under its authority."[66] This does not apply to use in the context of dependent activity, except in cases of excess.[67]

Further exceptions relate, for example, to the manufacture and operation of AI systems and AI models for the sole purpose of research and development (Article 2(6) of the AI Act), as well as research, testing, and development activities on AI systems and AI models prior to their placing on the market or putting into service (Article 2(8) of the AI Act), and AI systems that are placed on the market or put into service exclusively for military purposes, defense, or national security purposes (Art. 2(3) subpara. 2 AI Act).

An exception also applies to open source AI systems, which are excluded from the scope of application in accordance with Art. 2(12) AI Act. However, this does not apply if they are placed on the market or put into service as high-risk AI systems or

---

[64] *Borges*, CR 2024, 497, 504 (para. 89).

[65] *Blasek*, KIR 2025, 100, 103.

[66] *Borges*, CR 2024, 497, 504 (para. 92).

[67] *Borges*, CR 2024, 497, 505 (para. 92); *Grimm*, GmbHR 2025, 800, 802 (footnoe 27 zu para. 12); *Heine/Köhler*, NZA 2025, 521, 523.

if they fall under Art. 5 AI Regulation (prohibition) or Art. 50 AI Act (transparency).[68] The practical significance of the exception is therefore unlikely to be particularly high.[69]

b. The group of addressees

A key characteristic of the AI Act stems from the scope of its addressees. The law focuses on the so-called "provider". According to the definition in Article 3 No. 3 AI Act, this means, among others, a natural or legal person who develops or has developed an AI system or a general-purpose AI model, and places it on the market or puts it into service in their own name.

This definition is rooted in European product safety law.[70] As a corresponding definition to that used in product safety law,[71] it covers the manufacturer of the AI system; however, it includes important modifications compared to the concept of a manufacturer in other areas of law, which was presumably the reason for the unusual choice of terminology.[72]

---

[68] *Borges*, CR 2024, 497, 504 (para. 97).

[69] *Bomhard/Siglmüller*, RDi 2024, 45, 54 (para. 43); *Borges*, CR 2024, 497, 506 (para. 97); *Feuerstack/Becker/Hertz*, ZfDR 2023, 421, 424; *Voigt*, in: Schefzig/Kilian, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 2 para. 45.

[70] Art. 3 No. 8, Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA relevance), OJ L 135, 23.5.2023, p. 20; Art. 2 No. 3, Regulation (EC) 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance), OJ L 218, 13.8.2028, p. 35; Art. 3 No. 8, Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance), OJ L 169, 25.6.2019, p. 12; Art. 2(1) No. 12, Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Text with EEA relevance), OJ L 153, 22.5.2014, p. 71; Art. 3 No. 3, Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (Text with EEA relevance), OJ L 170, 30.6.2009, p. 6.

[71] *Borges*, CR 2024, 497, 505 (para. 83); see also *European Commission*, Guide to the implementation of EU product rules 2022 ("Blue Guide"), OJ (EU) 2022 C 247 of 29 June 2022, p. 1, 34 ff.; *Hilgendorf/Härtlein,* AI Act [KI-VO], 2025, Art. 2 para. 3 and Art. 3 para. 5; *Kirschke-Biller/Füllsack,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 76 ff.; *Wiebe,* BB 2022, 899.

[72] *Borges*, CR 2024, 497, 505 (para. 83); see *Kirschke-Biller/Füllsack*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 76.2, for the differences between the definitions.

It is important to note that development for own use is also covered,[73] meaning that in-house developments are fully subject to the requirements applicable to high-risk AI systems, including transparency obligations.[74] It is also essential that it is not only the actual development that matters, but that the client is held accountable.[75]

The second key addressee of the AI Act is the deployer of the AI system. This is defined in Article 3 No. 4 AI Act as the person who uses an AI system under their own authority, unless it is used in the context of a personal non-professional activity. The deployer is not the individual natural person who operates or uses an AI system.[76] The actions of natural persons are attributed to the respective organisation.[77] The conditions under which such attribution occurs, particularly where employees use an AI system without the employer's consent, are not regulated, giving rise to difficult distinctions in practice.[78]

As in other areas of law, attribution must be based on the employee's task.[79] As long as the employee uses the AI system within the scope of a task assigned to them, attribution is made to the employer.[80] The limit of attribution is exceeded only if the employee uses the system contrary to the employer's instructions, and the employer has taken reasonable measures to ensure compliance with those instructions.[81]

---

73 *Borges*, CR 2024, 497, 505 (para. 84); *Fleischmann/Sassenberg,* CR 2025, 561, 563 (para. 11); *Hilgendorf/Härtlein,* AI Act [KI-VO], 2025, Art. 3 para. 5; *Kirschke-Biller/Füllsack,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 76.2.

74 *Borges*, CR 2024, 497, 505 (para. 84).

75 *Borges*, CR 2024, 497, 505 (para. 84).

76 *Borges*, CR 2024, 497, 505 (para. 87); *Eulenpesch/Malczyk*, GRUR 2025, 40, 45; *Hilgendorf/Härtlein*, AI Act [KI-VO], 2025, Art. 2 para. 4 and Art. 3 para. 6; *Schuh/Witt,* EuDIR 2025, 142; see also the example case in *Kirschke-Biller/Füllsack,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 127.

77 *Borges*, CR 2024, 497, 505 (para. 87); *Kirschke-Biller/Füllsack,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 120, 122 f; *Schuh/Witt,* EuDIR 2025, 142, 147 (para. 20).

78 *Heine/Köhler*, NZA 2025, 521, 523; *Schuh/Witt*, EuDIR 2025, 142, 147 (para. 20).

79 *Borges*, CR 2024, 497, 505 (para. 87).

80 *Borges*, CR 2024, 497, 505 (para. 87).

81 *Borges*, CR 2024, 497, 505 (para. 87); for an analogous application of the exculpation rules developed in accordance with the case law of the ECJ on Art. 82(3) GDPR with regard to the attribution of employee conduct in a similar context*, see Schwartmann/Zenner,* EuDIR 2025, 3, 9 (para. 29).

Other parties addressed in the law are the provider's authorised representative (Art. 3 No. 5 AI Act), the importer (Art. 3 No. 6 AI Act) and the distributor (Art. 3 No. 7). The term "operator" (Art. 3 No. 8 AI Act) refers to all addressees collectively.

The AI Act thus exclusively regulates the obligations of so-called operators of AI systems (and, subsidiarily, of other parties involved). Other parties involved are not addressed, particularly users of an AI system who are also not its operators.[82] In fact, the use of an AI system is not regulated, especially the use of the outputs produced by such a system.[83] This is significant, not least for generative AI systems, which are currently in the spotlight. The entity that requests a specific result by means of an input (prompt) is not addressed, nor is the entity that uses the output, for example, as the basis for a decision or as the content of a communication.

c. The international scope of the AI Act

The international scope of application of the AI Act is governed by a complex provision in Article 2(1) AI Act, which is linked to the regulation of its material and personal scope of application. Article 2(1) AI Act distinguishes between different addressees: for providers, lit. a) and c) are relevant; for deployers, lit. b) and c) apply. The application of the AI Act to importers and distributors is set out in lit. d), to product manufacturers in lit. e), to authorised representatives in lit. f), and to affected persons in lit. g).

Of particular interest are the rules governing providers and deployers, who are the primary addressees of the obligations under the AI Act. In this regard, the relevant connecting factors are the place where the AI system is placed on the market or put into service (lit. a)), the location of the deployer's place of establishment (lit. b)), and the place where the output produced by the AI system is used (lit. c)). The regulation raises complex questions in all three respects.

aa. The link to the placing on the market or putting into service – Article 2(1) lit. a) AI Act

According to Article 2(1) lit. a) AI Act, the regulation applies to providers who place AI systems or general-purpose AI models on the market in the Union or put AI systems into service in the Union. As lit. a) expressly clarifies, the location of the provider's registered office or place of establishment is irrelevant.

---

82 *Schuh/Witt*, EuDIR 2025, 142 (para. 2).

83 For further information on the example of the employee, see *Heine/Köhler*, NZA 2025, 521, 523.

The term “placing on the market” is defined in Article 3 No. 9 AI Act as the first making available of an AI system or a general-purpose AI model on the Union market. The key term “making available on the market” is defined in Article 3 No. 10 AI Act as “the supply of an AI system or a general-purpose AI model for distribution or use on the Union market in the course of a commercial activity”. This definition of making available is surprisingly narrow, as it does not cover the offering of an AI system. However, this approach is appropriate, as it prevents overregulation and avoids protection deficits by applying the AI Act only once a supply has actually occurred following a successful offer.

The link to placing on the market is consistent with the classic principles of product safety law, but is not without challenges in practice. This raises the question of how to determine the place of “supply” of an AI system. In this regard, the location of the recipient’s establishment should be taken into account, not the location of the server from which the AI system is transmitted. If an AI system or a general-purpose AI model is transmitted to an establishment in the EU, Article 2(1) lit. a) AI Act applies. As is typical for software, such transmission will often take place via the internet, for instance, through downloading from a website by the recipient. In this case, it is therefore necessary for the download to be carried out by an establishment located in the EU.

Furthermore, the supply must be based on an offer that is directed at recipients in the Union,[84] in order to avoid an unlimited scope of application of the AI Act.[85] However, such targeting of recipients in the Union does not exist simply because the economic operator concerned directs its activities in some way to at least one Member State of the Union, or because the AI system is in fact made available to end users in the Union,[86] as this would again defeat the purpose of the restriction. Rather, the principles known from consumer conflict law should be applied, according to which it depends on whether the content of the offer is intended for recipients in the EU.

Determining the place of deployment is problematic in the case of software. This raises the question of whether the location of the server or servers on which the software runs should be taken into account, or the establishment from which the

---

84 *Wendehorst*, in: Martini/Wendehorst, AI Act [KI-VO], 2024, Art. 2 para. 16.

85 *Pieper*, in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 2 para. 49; *Ruschemeier*, AI as a challenge for legal regulation, p. 371; *Schopper/Raschner,* KIR 2025, 91, 94; *Voigt,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 2 para. 25.

86 However, see *Wendehorst*, in: Martini/Wendehorst, AI Act [KI-VO], 2024, Art. 2 para. 16.

software is controlled. This question is highly controversial in data protection law. As in data protection law, it is also appropriate in the context of the AI Act to refer to the location of the establishment from which the AI system is controlled. An AI system is therefore considered to be put into service in the Union if it is operated from an establishment in the Union.[87]

bb. The link to the place of establishment – Article 2(1) lit. b) AI Act

According to Article 2(1) lit. b) AI Act, the regulation applies to an AI system if the deployer is established within the Union. The connection to the place of establishment refers to the registered office.

Furthermore, the AI Act applies if the deployer is "located" in the Union. The use of this term is highly unfortunate, as it refers to the place of residence, which is widely used in conflict of laws in relation to natural persons or property, but is not appropriate for organisations. What is meant is the existence of an establishment located in the EU or, in the case of natural persons, their habitual residence as a functional equivalent of the establishment.

The general principles apply to the determination of the place of establishment and location. The main criterion to determine the place of establishment is the place of management, while other establishments exist, in any event, at facilities where persons with external contact regularly work (not in a home office).

The AI Act does not regulate which establishment is relevant if the deployer has several places of establishment. Consistent with other legal systems and in accordance with general principles, it should be sufficient that there is an establishment in the EU with a connection to the AI system's operation. According to the case law of the ECJ, an office that, for example, distributes services provided by means of an AI system or acts as a contact point for those services would be sufficient. If OpenAI maintains an office in the EU that serves as a contact point for questions relating to ChatGPT, the connecting factor under Article 2(1) lit. b) AI Act applies.

cc. The place of use of the AI system's output – Article 2(1) lit. c) AI Act

For providers and deployers alike, the connecting factor under Article 2(1) lit. c) AI Act is decisive. According to this, they are subject to the AI Act if they are established or located in a third country (only have branches there), if the output generated by the AI system is used in the Union.

---

87 *Wendehorst*, in: Martini/Wendehorst, AI Act [KI-VO], 2024, Art. 2 para. 18.

This connecting factor is extremely unusual and highly unclear. The place of use of the output is not a common connecting factor in international economic or general conflict-of-law rules. Very different places can be considered as the place of use. The receipt of the output or the processing of the output by persons, which in turn can involve various processing steps, may be decisive. It is also questionable whether only the first processing step is decisive or whether, if the output passes through different hands, each processing step triggers the AI Act. If, for example, a citizen in the EU uses prompting to generate a result from an AI system located in the US and then disseminates it as a social media post, where the result is accessed by other citizens, the multitude of possible connecting factors becomes clear. The difficulties persist, as the link to the place of activity in the processing of electronic data is itself highly problematic. Particularly, the question arises as to whether it should depend on the (simple) location of the person acting or, preferably, on the location of the recipient.

Regardless of these numerous interpretative difficulties, the connecting factor under Article 2(1) lit. c) AI Act results in an extremely broad extraterritorial scope of application of the AI Act.[88] This is problematic, as neither providers nor deployers can control where the output of an AI system is used. [89]

The connection under lit. c) is also problematic under international law. While the extraterritorial application of legal norms is not per se inadmissible under international law, a *sufficient connection* between the regulating state and the subject matter of the regulation is required.[90] In practice, various standards have been developed to determine such a sufficient connection.[91] The extraterritorial application of EU law is based, among other things, on the criteria of *nationality, presence , conduct, and effects.*[92] The extraterritorial application of law based on effects is recognised in principle almost worldwide. Its classic field of application is antitrust law. Its applicability to antitrust cases is assumed if these cases are expected to have *substantial effects* within the territory of the Union. [93]

---

88 *Borges*, CR 2024, 497, 498 (para. 13).

89 *Borges*, CR 2024, 497, 498 (para. 13).

90 *Kamminga*, 'Extraterritoriality', in: Peters (ed.), Max Planck Encyclopedia of Public International Law (as of September 2020), para. 9.

91 *Kamminga*, loc. cit. para. 10 ff.

92 *Hornkohl*, The Extraterritorial Application of Statutes and Regulations in EU Law, MPILux Research Paper Series 2022 (1), p. 13 ff.

93 *Hornkohl*, The Extraterritorial Application of Statutes and Regulations in EU Law, MPILux Research Paper Series 2022 (1), p. 20.

Notably, the connection between European economic law and the doctrine of effect extends beyond antitrust law.[94] Extraterritorial application under Article 2(1) lit. c) AI Act can therefore, in principle, be justified on the basis of the effects doctrine. However, even under the effect doctrine, not every effect on the territory of a state constitutes a sufficient basis for the application of its own law. According to the case law of the ECJ, extraterritorial application of European antitrust law can only be considered if it is foreseeable that the conduct will have a foreseeable, direct and significant impact on the EU market.[95]

The requirement of foreseeability is also recognised internationally in antitrust law. For example, the 1982 U.S. Foreign Trade Antitrust Improvements Act (FTAIA)[96] requires that the extraterritorial application of the *Sherman Antitrust Act*[97], the US antitrust law, have *a reasonably foreseeable effect* within the territory of the United States.

The principle of foreseeability of connection also underlies European product safety law. Its legal basis generally provides that the rules of product safety law apply where products are made available or placed on the market within the EU.[98] Both formulations aim to determine whether the end use of the product is intended to take place on the EU market.[99] A product is therefore subject to European product safety law only if it is intended for the European market. These principles, therefore, also apply to the extraterritorial application of the AI Act. A restrictive interpretation of Article 2(1) lit. c) AI Act is thus necessary, resulting in a scope of application that is predictable for providers and deployers.

---

94 *Hornkohl,* The Extraterritorial Application of Statutes and Regulations in EU Law, MPILux Research Paper Series 2022 (1), p. 21.

95 ECJ, 6 September 2017, C-314/ – Intel, para. 49; see also Hornkohl, The Extraterritorial Application of Statutes and Regulations in EU Law, MPILux Research Paper Series 2022 (1), p. 20 et seq.

96 Foreign Trade Antitrust Improvements Act (FTAIA) of 1982, Pub. Law. No. 97-290, 96 Stat. 1246 (1982).

97 Sherman Antitrust Act, Chapter 647, 26 Stat. 209 (1890).

98 See, for example, Art. 2(1) Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA relevance), OJ L 135, 23.5.2023, p. 19.

99 See, for the German Product Safety Act, *Heuser*, in Ehring/Taeger, Product liability and product safety law [Produkthaftungs- und Produktsicherheitsrecht], 2022, Section 2 Product Safety Act [ProdSG], para. 34.

Predictability is ensured for the provider if the AI system is intended for use in Europe or is at least approved for use there. The same standard should apply as in the context of Article 6(2) AI Act with regard to the intended use. Providers must therefore specify the intended use of AI systems not only with respect to their purpose but also with respect to their geographical scope of use. The change of role under Article 25 AI Act therefore also occurs where a deployer operates an AI system domestically, even though such domestic operation was not authorised by the provider. This ensures a restriction of the international scope of application that is consistent with both legitimate interests and principles of international law.

Similar restrictions apply to deployers of AI systems. In this case, Article 2(1) lit. c) AI Act does not apply merely because a result is retrieved from within the EU or otherwise enters the Union, but only where the deployer specifically targets the European market. The mere technical accessibility of an AI system via the internet is not sufficient for this purpose. However, services that are globally accessible and clearly address a global market are, in principle, also directed at the EU. For such services accessible via the internet, such as chatbots or other generative AI systems, specific restrictions are therefore necessary to exclude targeting of the European market. In this regard, the principles developed for determining market targeting by websites can be applied: deployers of AI systems whose services are demonstrably intended to address the European market are subject to the AI Act.

d. The temporal scope of the AI Act

The temporal scope of the AI Act is governed by Article 113 AI Act. Pursuant to sentence 1, the Regulation entered into force, as usual, twenty days after its publication in the Official Journal of the European Union, i.e. on 1 August 2024. According to sentence 2, it will generally apply two years after its entry into force, i.e., from 2 August 2026, subject to certain special provisions outlined in sentence 3. In particular, Chapters I and II, i.e., the general provisions and prohibitions, have been applicable since 2 February 2025. The rules in Chapter III, Section 4 (notifying authorities and notified bodies), Chapter V (general-purpose AI models), Chapter VII (governance), Chapter XII (penalties), and Article 78 AI Act (confidentiality), with the exception of Article 101 AI Act, apply from 2 August 2025. Article 6(1) AI Act and the corresponding obligations will take effect two years later, on 2 August 2027.

The staggered application of the AI Act takes into account the dependence of various actors on infrastructures and underlying components, not least on general-pur-

pose AI models.[100] For example, providers of AI systems depend on receiving information from providers of the underlying AI models to fulfil their obligations under the AI Act. The rules on conformity assessment for high-risk AI systems, in turn, require the establishment of notified bodies capable of carrying out conformity assessments in the cases referred to in Article 6(1) AI Act. This also makes it clear that the individual operators ultimately have very little time to adapt to the requirements of the AI Act,[101] insofar as they depend on the outcomes of activities carried out by other operators, not least on delegated legal acts or specifications through technical standards, etc. Delays in one stage of the implementation of the rules, therefore, have an impact on subsequent regulatory levels.

The transitional provisions in Article 111 AI Act concerning the application of the AI Act to general-purpose AI models and AI systems already placed on the market or put into service are of particular importance. The regulation distinguishes between AI systems that are components of certain large-scale IT systems listed in Annex X (Art. 111(1) AI Act), operators of high-risk AI systems (Art. 111(2) AI Act) and providers of general-purpose AI models (Art. 111(1) AI Act). Components of large-scale IT systems established under the legal Acts listed in Annex X that were placed on the market or put into service before 2 August 2027 are subject to a generous compliance period until 31 December 2030 (Art. 111(1) AI Act). For general-purpose AI models placed on the market before 2 August 2025, a corresponding compliance period applies until 2 August 2027 (Art. 111(3) AI Act).

According to Article 111(2) AI Act, the regulation applies (without prejudice to Article 5 AI Act) to operators of high-risk AI systems placed on the market or put into service before 2 August 2026 only if those systems have been significantly modified in their design thereafter. Providers and deployers of high-risk AI systems intended for use by public authorities must, in any case, comply with the requirements set out in Article 111(2) AI Act by 2 August 2030, even if the systems in question were put into service before 2 August 2026.[102]

3. The prohibitions of the AI Act

Article 5 AI Act prohibits certain practices related to the use of AI systems. The provision is mainly independent of the other areas of the regulation and sets its own

---

100 *Borges*, CR 2024, 497, 503.

101 *Borges*, CR 2024, 497, 503.

102 *Wendehorst*, in: Martini/Wendehorst, AI Act [KI-VO], 2024, Art. 111 para. 7.

terms, as it does not refer to providers and users, but to anyone who places an AI system on the market, offers it, or uses it for the purposes specified.

The prohibitions are very heterogeneous in terms of their subject matter and other characteristics. Prohibitions include, for example, the placing on the market, putting into service or use of an AI system that employs "subliminal techniques" on persons for specific purposes (Art. 5(1) lit. a) AI Act), as well as the placing on the market, putting into service or use of an AI system that "exploits the vulnerability of a natural person or a specific group of persons in need of protection" in order to influence their behaviour in a manner that is harmful to them (Art. 5(1) lit.b) AI Act). Also prohibited is the placing on the market, putting into service or use of an AI system for the evaluation of persons on the basis of their social behaviour, known as social scoring (Art. 5(1) lit. c) AI Act), as well as placing on the market, putting into service or use of an AI system "to carry out risk assessments of natural persons in order to assess or predict their propensity to commit a criminal offence" (Art. 5(1) lit. d) AI Act).

The prohibition also applies to AI systems that "create or expand facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage" (Art. 5(1) lit. e) AI Act), or "to infer emotions of a natural person in the workplace and in educational institutions," except this serves medical or safety purposes (Art. 5(1) lit. f) AI Act). Similarly prohibited are AI systems "for biometric categorisation to derive certain characteristics, such as race, religious beliefs or sexual orientation" (Art. 5(1) lit. g) AI Act).

Finally, Article 5(1) lit. h) AI Act impose specific conditions on the use of the so-called "real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes".

In the event of violations of the prohibitions, the competent supervisory authority may take measures in accordance with Regulation (EU) 2019/1020 (Art. 74(1) sentence 1 AI Act). In particular, it may require the cessation of the relevant activity. In addition, it shall impose a fine (Art. 99(3) AI Act).

4. Risk management for high-risk AI systems

Chapter III (Art. 6 - 49) AI Act, which is mainly based[103] on the rules of the Machinery Regulation,[104] sets out in five sections the requirements for risk management applicable to so-called high-risk AI systems. It includes, rules on the "classification of AI systems as high-risk AI systems" (Section 1, Art. 6 - 7 AI Act), on the "requirements for high-risk AI systems" (Section 2, Art. 8 - 15 AI Act), on the "obligations of providers and deployers of high-risk AI systems and other parties involved" (Section 3, Art. 16 - 27 AI Act), on the establishment of specific authorities and bodies for conformity assessment, known as "Notifying Authorities and Notified Bodies" (Section 4, Art. 28 - 39 AI Act), and finally the rules on "standards, conformity assessment, certificates, registration" (Section 5, Art. 40 - 49 AI Act).[105]

The rules on risk management are supplemented by regulatory oversight, a European register, and an infrastructure for the adoption of technical standards for testing AI systems. These rules apply only to a specific category of AI systems, referred to as high-risk AI systems. The scope of application of these rules is discussed below (see section 2 (a)), followed by an overview of the rules on risk management (see section 2 (b)).

a. The concept of high-risk AI systems

The risk management rules and other key components of the AI Act, such as supervision, apply only to so-called "high-risk AI systems" whose operations pose significant risks.[106]

This key term is used to describe two fundamentally different types of AI systems, regulatory approaches, and purposes of the AI Act:[107] The Regulation distinguishes between high-risk AI systems within the meaning of Article 6(1) in conjunction with Annex I AI Act, which primarily covers AI systems as product components

---

103 See *Mössner/Kittelmann*, ARP 2025, 217, 220.

104 Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (Text with EEA relevance), OJ L 165, 29.6.2023, p. 1.

105 *Borges*, CR 2024, 497, 499 (para. 20).

106 See recital 7, 26 AI Act; *Ossmann-Magiera/Dehmel*, KIR 2024, 134, 135 f.

107 *Braun Binder/Egli*, MMR 2024, 626; *Dubovitskaya*, AG 2024, 877, 881; *Gehrmann*, in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 6 para. 6 f. and 46, 56; *Linardatos,* ZIP 2024, 2497, 2498; *Marnau,* DuD 2025, 231, 232; *Schwartmann/Pottkämper,* in: Schwartmann/Keber/Zenner, AI Act – Practical Guide [KI-VO – Leitfaden für die Praxis], 2024, para. 155.

and aligns with existing European product safety law (see below), and high-risk AI systems within the meaning of Article 6(2) in conjunction with Annex III AI Act, which covers new categories of software that were not previously subject to European product safety law (see below).

aa. High-risk AI systems within the meaning of Article 6(1) in conjunction with Annex I AI Act

According to Article 6(1) AI Act, an AI system is a high-risk AI system if it is a product covered by the Union harmonisation legislation listed in Annex I or a safety component of such a product, and if it or the product is subject to third-party conformity assessment in accordance with the applicable harmonisation legislation.[108]

With these two cumulative conditions, the AI Act refers to the rules of European product safety law.[109] Annex I lists a total of 20 legal Acts, all of which belong to European product safety law.[110] This covers all types of transport and machinery, as well as lifts, toys, radio equipment and pressure equipment, and medical devices (see also recital 50, AI Act).

The term "product" within the meaning of Article 6(1) AI Act is not defined in the AI Act.[111] It is to be understood in a broad sense and ultimately encompasses any physical machine, as well as software.[112] The scope of application is thus defined by the legal Acts referred to in Annex I, each of which has its own rules governing

---

108 *Bronner*, KIR 2024, 55, 58; *Ebers/Streitbörger*, RDi 2024, 393, 395; *Gehrmann*, in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 6 para. 50; *Honer/Schöbel,* JuS 2024, 648, 651; *Marnau,* DuD 2025, 231, 232; *von Welser,* GRUR-Prax 2024, 485, 486; *Wiebe,* BB 2022, 899, 900.

109 *Braun Binder/Egli*, MMR 2024, 626; *Ebers/Streitbörger*, RDi 2024, 393, 395; *Gehrmann*, in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 6 para. 4 f.; *Kirschke-Biller/Füllsack,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 255; *Marnau,* DuD 2025, 231, 232.

110 See Annex I AI Act and *Bronner*, KIR 2024, 55, 58; *Dubovitskaya*, AG 2024, 877, 881; *Ebers/Streitbörger*, RDi 2024, 393, 395 f.; *Gehrmann,* in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 6 para. 55 f.; *Hilgendorf/Härtlein,* AI Act [KI-VO], 2025, Art. 6 ff. para. 3; *Kirschke-Biller/Füllsack,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 255 et seq.; *Marnau,* DuD 2025, 231, 232; *von Welser,* GRUR-Prax 2024, 485, 486.

111 *Kirschke-Biller/Füllsack*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 258; similarly *Gehrmann*, in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 6 para. 51.

112 See *Ruschemeier*, in Martini/Wendehorst, AI Act [KI-VO], 2024, Art. 6 para. 37, 40 f.

the scope of application. It therefore depends on whether the AI system or the product containing an AI system as software falls within the scope of one of the listed legal Acts. [113]

According to Article 6(1) lit. a) AI Act, AI systems themselves may be regarded as products within the meaning of (other) European product safety law. However, this will rarely be the case, as product safety law has so far mainly referred to physical products such as machinery and equipment. [114]

The machines covered by the product safety legislation listed in Annex I usually contain several, often numerous, software components and, in some cases, several AI systems, which may well have been developed by different providers.

According to Article 6(1) lit. a) AI Act, AI systems are only considered high-risk AI systems if they are safety components of a product covered by product safety law. The term "safety component" is defined in Article 3(14) AI Act as a component that performs a safety function or whose malfunction endangers the health and safety of persons or property.[115] The decisive factor is therefore whether the AI system in question is relevant to the product's safety.[116] The manufacturer of the product in question must ensure the overall safety of the product and, in this respect, must also comply with the risk management requirements for the product in question and the safety-related components. Consequently, safety components within the meaning of Article 6(1) AI Act are to be understood as all software components that are relevant for this purpose or, in other words, all AI systems that are relevant to the safety of the product according to the relevant harmonised standards and are subject to the product's risk management requirements.

Another prerequisite for classification as a high-risk AI system is that the product requires third-party conformity assessment in accordance with the relevant product safety legislation.[117] Conformity assessment is a central element of European product safety law. The conformity assessment, which must be carried out before a product is placed on the market, checks whether the product meets the requirements of

---

113 *Gehrmann*, in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 6 para. 51.

114 *Linardatos*, ZIP 2024, 2497, 2498; *Marnau*, DuD 2025, 231, 233; *Wiebe*, BB 2022, 899, 900.

115 Critical *Ebers/Streitbörger*, RDi 2024, 393, 395 (para. 15).

116 *Borges*, CR 2024, 565, 566 (para. 9); *Hilgendorf/Härtlein*, AI Act [KI-VO], 2025, Art. 3 para. 16; *Kirschke-Biller/Füllsack,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 3 para. 261; *Marnau,* DuD 2025, 231, 233.

117 *Borges*, CR 2024, 565, 566 (para. 12); *Hilgendorf/Härtlein*, AI Act [KI-VO], 2025, Art. 6 para. 8 f.; *Honer/Schöbel,* JuS 2024, 648, 651; *Klawonn,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 6 para. 13; *Marnau,* DuD 2025, 231, 233.

European product safety law. It can be carried out using various procedures and is usually performed by the manufacturer itself.[118] Only in rare, exceptional cases does European product safety law stipulate that the conformity assessment must be carried out by an independent third party.[119]

This requirement significantly reduces the scope of high-risk AI systems under Article 6(1) AI Act and covers only a small range of AI systems.[120]

bb. High-risk AI systems within the meaning of Article 6(2) in conjunction with Annex III AI Act

According to Article 6(2) AI Act, AI systems listed in Annex III are also to be classified as high-risk AI systems. Even though Articles 6(1) and (2) AI Act both refer to an annex to describe the scope of high-risk AI systems, they are completely different regulatory concepts.[121] While Annex I, as shown, refers to European product safety law, Annex III covers areas that were not typically subject to European product safety law until now.[122]

(1) The classification of AI systems according to Article 6(2) AI Act

With Annexe III, the European legislature aims to cover certain areas in which AI systems make assessments and decisions that pose particular risks to personal rights. These can be referred to as "high-risk areas".[123]

In the case of such assessments and decisions by AI systems, it must be taken into account that the risks associated with an incorrect assessment typically do not materialise directly in the result produced by the AI system, i.e. the assessment, but rather in the use of this result.[124] For example, if an AI system assesses the creditworthiness of a natural person or their suitability for a job, the result of the AI system is typically used by a third party, and it is only the behaviour of the third party,

---

118 *Borges*, CR 2024, 565, 566 (para. 12); *Marnau*, DuD 2025, 231, 233.

119 *Borges*, CR 2024, 565, 566 f. (para. 12); *Marnau,* DuD 2025, 231, 233; see, for example, on the Medical Devices Regulation*, Klawonn,* in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 6 para. 14.

120 *Borges*, CR 2024, 565, 567 (para. 12); *Marnau*, DuD 2025, 231, 233.

121 *Hilgendorf/Härtlein*, AI Act, 2025, Art. 6 para. 10; *Honer/Schöbel*, JuS 2024, 648, 651 ("two categories of high-risk AI systems"); *Spiegel/Höving*, KIR 2025, 231, 233.

122 *Gehrmann*, in: Bomhard/Pieper/Wende, AI Act, 2025, Art. 6 para. 7 f.; *Guckelberger,* DÖV 2025, 45 f. (fn. 11); similarly, *Saam/Hermann,* RDi 2024, 608, 609 (para. 7).

123 See, *Sesing/Tschech*, MMR 2022, 24, 28 f.; *Vasel/Müller*, MMR 2024, 291, 293.

124 *Kätscher/Pesch*, KIR 2024, 46, 48.

such as the refusal of a desired loan, that (potentially) leads to discrimination against the affected person.[125] The provision in Article 6(2) AI Act must therefore take into account that particular risks to personal rights do not depend directly on the characteristics of an AI system or its results, but rather on the intended use of those results.[126]

Therefore, classification as a high-risk AI system is not based on the AI system's characteristics, but solely on the use of its results.[127] Classification takes place in two main stages:[128] In the first step, the AI system in question must be covered by Annex III, and in the second step, the AI system must, in accordance with Article 6(3) AI Act, pose risks of harm to the health, safety or fundamental rights of natural persons based on a specific assessment. This means that only AI systems whose use may pose risks to natural persons are covered.[129]

Below, we first provide an overview of the high-risk areas listed in Annex III ((2)). We then describe the concept for determining whether an AI system belongs to a high-risk area ((3)) and finally the second stage, the specific risk assessment ((4)).

(2) The high-risk areas of Annex III

Annex III, which is relatively short compared to Annex I, essentially lists in eight points certain areas in which the European legislator sees risks to personal rights arising from the use of AI systems.

No. 1 covers the area of biometrics, specifically: remote biometric identification systems (lit. a)); AI systems for biometric categorisation (lit. b)); and AI systems for emotion recognition (lit. c)).

No. 2 covers AI systems to be used as safety components in the management and operation of critical infrastructure, specifically digital infrastructure, road traffic, or water, gas, heat, or electricity supply.

---

125 *Paal/Schulz*, ZfDR 2025, 89, 101; *Steenbergen*, KIR 2025, 326, 328.

126 See *Ebers/Streitbörger*, RDi 2024, 393, 394 f.; on the scope of Annex III No. 8 AI Act [KI-VO], see *Saam/Hermann*, RDi 2024, 608, 610.

127 *Borges*, CR 2024, 565, 570 (para. 21); cf. *Buchalik/Gehrmann,* CR 2024, 145, 150; *Gehrmann,* in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 6 para. 66; *Wachter,* Yale J.L. & Tech. 26 (2024), 671, 684 f.

128 *Borges*, CR 2024, 565, 570 (para. 21); *Saam/Hermann*, RDi 2024, 608, 610.

129 See *Biallaß*, MMR 2024, 646, 649; *Braun Binder/Egli*, MMR 2024, 626, 627; *Buchalik/Gehrmann*, CR 2024, 145, 149 f.; *Dilling/Musiol,* CCZ 2024, 257, 262; *Ebers/Streitbörger,* RDi 2024, 393, 396; *Linardatos,* ZIP 2024, 2497, 2498; *Saam/Hermann,* RDi 2024, 608, 610 f.; *Wachter/Leeb,* RDi 2024, 440, 445.

No. 3 covers AI systems in the field of education and vocational training: specifically AI systems intended to be used to determine access or admission to education and vocational training institutions at all levels (lit. a)); AI systems for evaluating learning outcomes (lit. b)); AI systems for the purpose of assessing the appropriate level of education (lit. c)); and AI systems for monitoring and detecting prohibited behaviour by students during examinations (lit. d)). No. 3, therefore, does not cover the use of AI systems for teaching purposes, but focuses on the assessment of individuals by AI systems.

No. 4 covers AI systems in the fields of employment, workers management and access to self-employment, i.e. AI systems in the field of human resources (HR): This includes AI systems used for the recruitment or selection of natural persons (lit. a)); as well as systems intended to be used for decisions on the conditions of employment, for promotions or termination, or for the monitoring and evaluation of persons in employment relationships (lit. b)).

No. 5 covers AI systems in the context of so-called "essential [...] services and benefits" and explicitly includes both private and public services. This umbrella term covers a catalogue of four quite heterogeneous areas. It covers AI systems intended to be used to assess eligibility for: essential public assistance benefits and services (lit. a)); systems for assessing the creditworthiness of natural persons (lit. b)); systems for risk assessment and pricing in relation to life and health insurance (lit. c)); and systems to be used for prioritisation in emergency and rescue services and in the context of emergency medical aid (lit. d)).

No. 6 covers AI systems in certain areas of law enforcement, essentially predictive policing, as well as AI systems for evaluating evidence, in particular lie detectors.

No. 7 covers the area of migration, asylum and border control. It covers AI systems intended for use as: lie detectors (lit. a)); systems for assessing the risks posed by an incoming person, such as security risks (lit. b)); systems for examining asylum and visa applications (lit. c)); and systems for detecting, recognising or identifying natural persons, except for the verification of travel documents (lit. d)).

No. 8 addresses two very different areas. Lit. a) covers AI systems designed to support judicial activity, defined as AI systems intended to assist judicial authorities "in researching and interpreting facts and the law and in applying the law to a concrete set of facts". Lit. b) covers AI systems that are intended to influence the outcome of an election or the voting behaviour of natural persons under the heading of "democratic processes". According to sentence 2, this does not include systems whose outputs are not intended to be communicated directly to natural persons, such as systems for organising or optimising political campaigns.

The overview shows that Annex III comprises a heterogeneous catalogue of different areas, but with a clear focus on the evaluation, monitoring and influencing of individuals by AI systems.

This makes it clear that the AI Act aims to use the instruments of product safety law to protect personal rights. This is a highly innovative approach, as product safety law has traditionally focused on protection against risks to health and property. At the same time, it is clear that the AI Act emphasises regulating AI systems for decisions and assessments concerning natural persons.

With the approach of enumerating high-risk areas, the European legislature is making an important fundamental decision: neither AI systems for automated decision-making nor AI systems for analysing individuals are covered across the board, but only those systems to be used for the purposes of Annex III. This is obviously intended – and rightly so – to prevent overregulation and ensure that the rules for high-risk AI systems apply only to those that pose risks, particularly to personal rights.

This has the interesting consequence that one and the same AI system, depending on its intended use, may or may not constitute a high-risk AI system and thus be subject to the demanding rules on risk management – or, conversely, may be exempt from all such requirements.[130]

(3) Determining high-risk character based on the use of the result

The determination of the high-risk nature of an AI system pursuant to Article 6(2) in conjunction with Annex III AI Act depends on the area in which the system is to be used as intended.[131] If, for example, an AI system is used to evaluate students, it falls within the high-risk area under No. 3(b) of Annex III; if it is used for assessment in the context of self-study, it is not a high-risk AI system from the outset.[132] The situation is similar in other areas: if an AI system is intended for use by a judge, it may be a high-risk AI system under No. 8(a) of Annex III, but not if it is intended for use by lawyers.[133] If an AI system is to be used by a waterworks that is part of

---

130 *Borges*, CR 2024, 565, 568 (para. 32); *Buchalik/Gehrmann*, CR 2024, 145, 150.

131 See *Braun Binder/Egli*, MMR 2024, 626, 627; *Roth-Isigkeit*, KIR 2024, 15, 17; *Saam/Hermann*, RDi 2024, 608, 609.

132 Annex III No. 3 lit. b) AI Act [KI-VO] is intended to prevent discrimination based on the AI system's inability to adequately exercise the discretion and judgement required in examination performance, see *Gehrmann*, in: Bomhard/Pieper/Wende, AI Act [KI-VO], 2025, Art. 6 para. 98.

133 See *Wöbbeking*, AnwBl 2025, 17, 18.

critical infrastructure, it is a high-risk system under No. 2 of Annex III, but not if its intended use is for the operation of small non-critical waterworks.[134]

For this classification, it is irrelevant whether the decision is made or prepared by the AI system or by an actor who merely uses the AI system's result, possibly as one of several pieces of information, for their own decision. For example, if an AI system generates a credit rating[135] for a natural person and a bank employee takes it into account in their credit decision, this is a case of Annexe III No. 5 lit. b), as is an automatic credit decision by the AI system itself.

This concept, which differs significantly from traditional product safety law, poses several new challenges. Obvious questions are who makes the determination, to which numerous numbers in Annex III expressly refer, and what the consequences are when an AI system is used in a manner that deviates from its original intended purpose.

This classification within the framework of Article 6(2) AI Act, which cannot be described in detail here,[136] is based on a double standard under the AI Act: In principle, the intention of the provider who manufactures an AI system for specific purposes is decisive. The provider must specify the intended use and can thus control whether or not the AI system it manufactures constitutes a high-risk AI system when placed on the market.

However, the actual use of the result generated by the AI system in question is then decisive: if this deviates from the use specified by the provider, the actual use prevails.

(4) The specific risk assessment, Article 6(3) AI Act

The second stage of assessing an AI system as a high-risk AI system within the meaning of Article 6(2) in conjunction with Annex III AI Act is regulated by Article 6(3) AI Act. This standard, introduced only during the trilogue negotiations,[137] makes the high-risk nature of an AI system dependent on a specific risk assessment.

---

134 For the concept of critical infrastructure within the meaning AI Act, see *Buchholz*, EnWZ 2025, 309, 311 ff.

135 For general information on the use of AI for payment forecasts, see *Khosravi*, MMR 2025, 596.

136 For details, see *Borges*, CR 2024, 565, 567 ff.

137 *Bronner*, KIR 2024, 55, 58; *Klawonn*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 6 para. 22.

According to subparagraph 1 of Article 6(3) AI Act, an AI system listed in Annex III is not high-risk "where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons by, including by not materially influencing the outcome of decision-making". The addition of Article 6(3) AI Act with its specific risk assessment was a necessary correction, as otherwise the scope of high-risk AI systems under Article 6(2) AI Act would have been far too broad – it is alarming that this essential element of the AI Act was only introduced at the last minute.

The absence of a significant risk is described in more detail in subparagraphs 2 and 3 of Article 6(3) AI Act. According to subparagraph 2, subparagraph 1 "applies" if one of the conditions specified in points (a) to (d) is met, for example if the AI system is intended to perform a "narrowly defined procedural task" (point (a)), improve the result of a "previously completed human activity" (point (b)), it is intended to "recognise decision-making patterns or deviations from prior decision-making patterns [...]" and not meant to "replace or influence the previously completed human assessment without proper human review [...]" (lit. c)), or it is intended to perform "a preparatory task to an assessment" (lit. d)). According to subparagraph 3, an AI system listed in Annex III is always considered high-risk if it "profiles natural persons".

It is questionable whether the specific wording of Article 6(3) AI Act is flawless. The lack of discussion of the provision in the legislative process could have a negative impact here. In particular, the relationship between subparagraphs 1 and 2 of Article 6(3) AI Act is problematic. Subparagraph 2 is sometimes understood as a definitive definition of significant risk,[138] but is predominantly interpreted as a list of standard examples,[139] or, with the same result, as a presumption.[140]

The phrasing of the first half of the sentence in subparagraph 2 of Article 6(3) AI Act suggests a definitive definition. Also, from a systemic point of view, the fact that the Commission can amend the list in subparagraph 2 pursuant to Article 6(7) AI Act supports the definition's definitive nature. However, this interpretation would not be appropriate in view of the very narrow wording of the case groups

---

138 See, for example, *Bronner*, KIR 2024, 55, 59; *Ebers/Streitbörger*, RDi 2024, 393, 396; *Ebers/Quarch/Rode,* LTZ 2025, 21, 26; *Hilgendorf/Härtlein,* AI Act [KI-VO], 2025, Art. 6 para. 14.

139 *Borges*, CR 2024, 565, 571; *Saam/Hermann*, RDi 2024, 608, 611.

140 *Klawonn*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 6 para. 26.

referred to in points (a) to (d) of subparagraph 2. The power to amend under Article 6(7) Act is equally plausible if understood as an exemplary rule or a presumption.

It therefore makes sense to understand subparagraph 2 of Article 6(3) AI Act as a formulation of standard examples and to regard the criterion of "materially influencing the outcome of decision-making" referred to in subparagraph 1 as decisive. Ultimately, the determining factor is whether the output of the AI system is capable of materially influencing a decision in a high-risk area. Such suitability does not exist beyond the examples mentioned in lit. a–d), for example, where the decision, according to the applicable decision-making procedure, is not intended to depend on the AI system's output.

This also makes it clear that information generated by an AI system that may be causal for a decision within the meaning of Annex III is, in principle, covered. Such causality also exists when the information influences individual elements of a decision, such as the interest rate on a loan, or the ranking of candidates for a job or promotion, etc.

Additionally, as an exception to subparagraph 1 of Article 6(3) AI Act, subparagraph 3 stipulates that an AI system must always be classified as a high-risk AI system if it performs profiling.[141] This is presumably intended to ensure that AI systems that generate assessments of individuals in the areas listed in Annex III, such as their performance, creditworthiness, etc., are always classified as high-risk AI systems.

Accordingly, assessing whether a significant risk within the meaning of Article 6(3) AI Act exists is extremely complex and can involve considerable effort and uncertainty. Pursuant to paragraph 5, the Commission shall, by 2 February 2026 at the latest, i.e. before Article 6 AI Act becomes applicable, provide guidelines on practical implementation, including a comprehensive list of practical examples of use cases of high and non-high risk AI systems. It would have been better if the legislature had explicitly formulated the list as a *safe harbour*, listing only those applications that do not pose a significant risk within the meaning of Article 6(3) AI Act, and further stipulating that providers may rely on the classification.

According to Article 6(4) AI Act, sentence 1, the provider of an AI system who manufactures an AI system for a purpose specified in Annex III but does not clas-

---

141 *Bronner*, KIR 2024, 55, 59; *Hilgendorf/Härtlein*, AI Act [KI-VO], 2025, Art. 6 para. 23; *Klawonn*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 6 para. 31.

sify it as high-risk in accordance with Article 6(3) AI Act must document this assessment before placing it on the market or putting it into service.[142] Furthermore, sentences 2 and 3 obligate the provider, in accordance with Article 49(2) AI Act, to register itself and the system in the database for high-risk AI systems and to present the assessment to the market surveillance authority upon request.[143] This is a very pragmatic provision that should effectively prevent the abuse of Article 6(3) AI Act and, at the same time, contribute to the establishment of uniform standards.

The practical significance of Article 6(3) AI Act is likely to be high. If the standard is not interpreted too narrowly, it can effectively help to avoid excessive classification of AI systems as high-risk AI systems. This makes the specific risk assessment under Article 6(3) AI Act an essential step towards deregulation. This approach is undoubtedly correct, as otherwise overregulation would occur, ultimately impairing the development and use of AI systems without providing additional protection for citizens' rights.

b. Elements of risk management

The core element of the rules for high-risk AI systems is risk management, which is supplemented by a series of complementary measures. This includes the obligation to implement quality management as stipulated in Article 17 AI Act, the obligation to carry out conformity assessments and issue declarations of conformity, and the obligation to conduct post-market surveillance, including a reporting obligation in the event of incidents. The complex regulation spans several chapters of the AI Act.

aa. The substantive requirements for risk management

The substantive requirements for risk management are summarised in Chapter III, Section 2, Articles 8 - 15 AI Act. The principle is laid down in Article 9(1) AI Act, according to which risk management must be established and maintained for high-risk AI systems. The risk management system is defined in Article 9(2) AI Act as a continuous process throughout the entire life cycle of a high-risk AI system, which includes, as essential cornerstones, a risk analysis (para. 2 lit. a)) and the taking of appropriate measures to address the identified risks (para. 2 lit. d)). As clarified in

---

142 *Klawonn*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 6 para. 33.

143 *Klawonn*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 6 para. 37.

paragraphs 6–8, risk management includes continuous testing of the high-risk AI system.

Articles 10–15 AI Act contain specific rules on the key components of risk management. The data governance obligations set out in Article 10 AI Act are likely to be particularly challenging. According to Article 10(1) AI Act, training (including testing) must be carried out using data sets that meet the quality criteria specified in paragraphs 2–5. These include the requirements for data governance and management practices appropriate for the intended use of the high-risk AI system, including, for example, the avoidance of bias (para. 2 lit. f)).

Article 11 AI Act lays down the particularly important obligations concerning the technical documentation of a high-risk AI system. According to paragraph 1, subparagraph 2, sentence 1, the documentation must demonstrate that the AI system meets the requirements of Chapter 3, Section 2 AI Act.

Article 12 AI Act regulates recording-keeping. According to paragraph 1, high-risk AI systems must enable the automatic recording of certain events (logging) specified in paragraphs 2 and 3 throughout their entire life cycle. The records are intended to fulfil certain risk management measures.

Article 13 AI Act lays out transparency obligations intended to enable the deployer to properly operate the AI system. This includes, in particular, the provision of operating instructions for the deployers (Art. 13(2) AI Act), which must contain the essential information specified in paragraph 3 lit. a)–f) on the system, its function and the associated risks. According to Article 14 AI Act, high-risk AI systems must be designed in such a way that they can be effectively overseen by natural persons. To achieve this goal, AI systems must, for example, offer natural persons the possibility of intervening in or interrupting the system's operation, as specified in paragraph 4 lit. e). Article 15 AI Act sets out the requirements for the accuracy, robustness and cybersecurity of high-risk AI systems.

Risk management is supplemented by a quality management system, to be set up by the provider pursuant to Article 17 AI Act. According to Article 17(1) AI Act, a strategy for regulatory compliance, techniques and procedures for development, quality control and assurance, examination procedures, and data management procedures, *inter alia*, must be established. The provision is further supplemented by the provider's obligations to monitor the AI system after it has been placed on the market in accordance with Article 72 AI Act and to report serious incidents to the market surveillance authorities in accordance with Article 73 AI Act.

bb. The obligations of providers and deployers of high-risk AI systems

The AI Act imposes obligations on providers and deployers of high-risk AI systems that correspond to their respective roles and their importance for risk management.[144]

The obligations of the provider of high-risk AI systems are summarised in a comprehensive catalogue in Article 16 lit. a)–l) AI Act. The central obligation of the provider is set out in Article 16 lit. a) AI Act. According to this, the provider must ensure that its high-risk AI system meets the requirements set out in Section 2 (Art. 8 - 15 AI Act) on risk management. Articles 16 lit. b)–l) establish further obligations relating to risk management and the other requirements of the AI Act concerning high-risk AI systems.

For example, the provider must: provide its name and contact address (lit. b)); establish, in accordance with Article 17, a quality management system for high-risk AI systems (lit. c)); comply, pursuant to Article 18, with the documentation requirements for high-risk AI systems (lit. d)); retain, in accordance with Article 19, the logs automatically generated by high-risk AI systems (lit. e)); ensure, pursuant to Article 43, that the relevant conformity assessment procedure is carried out (lit. f)); issue, in accordance with Article 47, an EU declaration of conformity (lit. g)); affix the CE marking to the high-risk AI system or its documentation (lit. h)); comply, in accordance with Article 49(1), with the registration requirement (lit. i)); take the necessary measures required under Article 20 to correct high-risk AI systems and provide relevant information (lit. j)); demonstrate, at the request of a competent authority, the high-risk AI system's conformity with Articles 8–15 (lit. k)); and, finally, ensure that the high-risk AI system meets the accessibility requirements set out in the relevant EU directives (lit. l)).

The obligations of the deployer of a high-risk AI system are regulated in Article 26 AI Act. The obligations are narrowly defined:[145] According to Article 26(1) AI Act, the deployer must take appropriate technical and organisational measures to ensure that high-risk AI systems are used in accordance with the operating instructions and the obligations under paragraphs 3 and 6. Paragraph 3 points out that Article 26 does not affect the obligations under other Union or national law. Paragraph 6 obliges deployers to keep the logs automatically generated by their high-risk AI system.

---

[144] See a tabular overview of the obligations in *Rohrßen,* ZfPC 2024, 111, 117 ff.

[145] *Ahskar/Schröder,* BB 2024, 771, 773.

According to paragraph 4, deployers shall ensure that the input data, insofar as it is under their control, is relevant for the intended purpose of the high-risk AI system and "sufficiently representative". According to paragraph 5, sentence 1, the deployer must monitor the operation on the basis of the instructions for use. If the deployer has reason to believe that use in accordance with the instructions may result in the system posing a risk within the meaning of Article 79(1) AI Act, the deployer must suspend the use of the system and notify the provider and the relevant market surveillance authority. If the deployer identifies a serious incident, they must immediately inform the provider, then the importer or distributor, and the relevant market surveillance authorities.

The remaining paragraphs essentially regulate supplementary, in some cases very specific obligations, as well as references to obligations under other legal Acts. For example, the deployer must use the information provided in accordance with Article 13 AI Act to carry out a data protection impact assessment in accordance with the GDPR (para. 9). Paragraph 10 obliges the deployer of a high-risk AI system to obtain authorisation within 48 hours for post-remote biometric identification in the context of investigations.

The central element of the deployer's obligations is thus the instructions for use to be issued by the provider. These specify the deployer's obligations, which primarily involve cooperation with the provider and the relevant authorities.

cc. Conformity assessment

An important element of risk management is the conformity assessment to be carried out by the provider, which is regulated in more detail in Section 5, Articles 40–48 AI Act.

Article 43 AI Act provides for different conformity assessment procedures that apply to different types of high-risk AI systems. For the high-risk AI systems listed in Annex III (except for systems listed in Annex III No. 1, to which Article 43(1) AI Act are covered), internal control as described in more detail in Annex VI is sufficient in accordance with Article 43(2) AI Act. In the cases listed in Annex I, Section A, the rules of the respective European product safety law apply in accordance with Article 43(3) AI Act.

The provider must issue an EU declaration of conformity stating, in accordance with Article 47(2), sentence 1, that the system meets the requirements of Articles 8–15 AI Act. With the declaration of conformity, the provider assumes "responsibility" for compliance with the requirements, as is customary in product safety law, in accordance with Article 47(4) sentence 1 AI Act. The rules on CE marking apply,

which, according to Article 48(3) sentence 1 AI Act, must generally be affixed to a high-risk AI system.

Furthermore, providers and deployers of high-risk AI systems listed in Annex III (see 1. b. bb. above) (exception: No. 2) must register in the EU database for high-risk AI systems in accordance with Article 49 AI Act before placing them on the market or putting them into service. For this purpose, an EU database must be established and maintained in accordance with Article 71 AI Act.

This brief overview shows that the AI Act provides for comprehensive measures to control the risks posed by high-risk AI systems, including demanding obligations for providers. Notably, specifying requirements—for example, for data governance—and developing appropriate procedures for testing and conformity assessment of AI systems are likely to pose major challenges in many areas.

Whether and how quickly the mechanisms provided for in the AI Act will produce practical results is likely to depend heavily on the specific area of application. In view of the uncertainties that currently exist, the rules for providers of high-risk AI systems are likely to lead to a considerable need for technical and legal advice.

5. The rules for AI models

Chapter V (Art. 51 - 56) AI Act contains rules on risk management for so-called general-purpose AI models. The regulation distinguishes between general-purpose AI models with systemic risk and others without. Accordingly, the chapter is divided into rules on the classification of general-purpose AI models (Art. 51 - 52 AI Act), obligations for providers of general-purpose AI models (Art. 53 - 54 AI Act) and obligations for providers of general-purpose AI models with systemic risk (Art. 55 - 56 AI Act). The rules exclusively address the provider of a general-purpose AI model and, where applicable, its authorised representative.

a. The concept of a general-purpose AI model

The term "general-purpose AI model" is defined in Article 3 No. 63 AI Act in a very complex and ambiguous manner.

In its communication of 18 July 2025,[146] the European Commission published draft guidelines on the obligations relating to general-purpose AI models (hereinafter,

---

146 *European Commission,* Communication to the Commission, Approval of the content of the draft Communication from the Commission – Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act) of 18 July 2025, C(2925) 5045 final.

the guidelines),[147] intended to clarify a number of terms used in the AI Act. The term "general-purpose AI model" is defined in section 2.1. (para. 13 ff.) of the Guidelines. According to this, an indication of the wide range of capabilities described in the definition is present if the computational resources used to train the model exceed 10^{23} FLOP and if it can generate language, images, or videos from text input.

In paragraph 15, the guidelines refer in particular to recitals 98 and 99 AI Act, which describe the design of an AI model with general-purpose use and its ability to generate content in the form of text, sound, images, or video as characteristics of such a model with a wide range of distinctive capabilities.

The calculation of the relevant number of training compute, which is equally important for the calculation under Article 51(2) AI Act, is explained in the Annex to the guidelines (para. 117 ff.). This can be done using a highly simplified estimate, for which various alternatives are available.

This interpretation effectively rewrites the definition in Article 3(1) AI Act and restricts it in two ways: firstly, only models for generative AI systems are covered, and secondly, the focus is solely on simple size characteristics. The decisive advantage is the ease with which an AI model can be determined to be general-purpose. At the same time, this represents a significant step towards deregulation, as only a few models will ultimately be classified as general-purpose.

b. The rules for general-purpose AI models

The rules for general-purpose AI models are kept brief: Article 53 AI Act sets out the obligations of the providers of such models, while Article 54 AI Act contains special rules for providers based in third countries.

The obligations of providers are set out in Article 53(1) lit. a)–d) AI Act. They essentially concern technical documentation of the model with a focus on the training process and the training data used (lit. a)–b)). According to Art. 53(2) AI Act, these obligations do not apply to providers of open-source models, provided they are not general-purpose AI models with systemic risk.

Furthermore, providers must develop a policy for complying with Union copyright law (lit. c)) and create and publish a "sufficiently detailed summary" of the content used for training (lit. d)).

---

147 Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act).

The provider's obligations are to be further specified in the European harmonised standards. Until these standards are adopted, providers may rely on codes of practice pursuant to Article 53(4) AI Act to demonstrate compliance with the obligations under paragraph 1. The *codes of practice*, which are regulated in detail in Article 56 AI Act, should not be confused with the *codes of conduct* within the meaning of Article 95 AI Act. These codes are to be developed at the Union level by the industry itself, with the European AI Office (see section # below) providing support for their development. In accordance with Article 53(4) AI Act, compliance with the harmonised standards or the code of practice creates a presumption of conformity with the requirements set out in Article 53(1) AI Act.

Article 54 AI Act contains special rules for providers established in third countries. According to Article 54(1) AI Act, before placing a general-purpose AI model on the Union market, they must designate an authorised representative established in the Union.

According to Article 54(3) AI Act, the authorised representative must be mandated to perform the tasks specified in Article 54(3) lit. a)–d) AI Act. This includes verifying that the technical documentation has been drawn up in accordance with Annex XI and that the obligations referred to in Article 53 and, where applicable, Article 55 have been fulfilled (lit. a)), keeping a copy of the technical documentation (lit. b)), providing the AI office with the information and documentation required to demonstrate compliance with the obligations in Chapter V (lit. c)) and cooperating with the AI Office and competent authorities on matters relating to general-purpose AI model (lit. d)). Finally, Article 54 AI Act does not apply to open-source AI models, unless they pose systemic risks (Art. 54(6) AI Act).

c. The general-purpose AI model with systemic risk

Providers of general-purpose AI models with systemic risk are subject to additional obligations under Article 55 AI Act. The classification as a general-purpose AI model with systemic risk is governed by Article 51(1) AI Act. Pursuant to lit a), a general-purpose AI model is to be classified as one with systemic risk if it has high-impact capabilities. According to lit b), such classification may also be based on an *ex officio* decision by the EU Commission or the scientific panel alerting that the model has capabilities or impact equivalent to those within the meaning of lit. a).

According to Article 51(2) AI Act, the existence of a capability within the meaning of lit. a) is assumed if the cumulative amount of computation used for training exceeds 10^{25}. The term "AI system with systemic risk" is therefore intended to cover

particularly large AI models, especially the currently well-known "large language models (LLMs)", such as GPT, Llama and Gemini.

The obligations of providers of AI systems with systemic risk are regulated under Article 55 AI Act. Article 55(1) AI Act imposes risk management obligations on them, specifically to evaluate the models, including conducting tests (lit. a)), to assess and mitigate potential systemic risks (lit. b)), to collect information on serious incidents and promptly report them to the AI Office (lit. c)), and ensuring an adequate level of cybersecurity protection for the model (lit. d)).

Pursuant to Article 55(2) AI Act, and as in the case of Article 53 AI Act, the obligations under Article 55 AI Act are to be specified by a harmonised standard. Until such a standard is published, providers may rely on codes of practice within the meaning of Article 56 AI Act to demonstrate compliance.

6. Transparency obligations for providers and deployers of certain AI systems

Chapter IV AI Act ("Transparency obligations for providers and deployers of certain AI systems") consists solely of Article 50, which bears the same name. Despite its brevity, this chapter is an important element of the AI Act and has great practical significance, especially for generative AI systems.[148] Article 50 AI Act sets out the transparency obligations of providers in paragraphs 1 and 2, and those of deployers in paragraphs 3 and 4. Paragraphs 5 and 7 contain supplementary rules that apply to both.

Article 50(1) AI Act contains transparency obligations for AI systems that interact directly with natural persons, such as chatbots or robots designed for human interaction, including care robots.[149] In particular, according to paragraph 1, such systems must inform the natural person concerned that they are interacting with an AI system, unless this is obvious from the circumstances and context of use (as would typically be the case with a robot).

Article 50(2) AI Act obliges providers of generative AI systems to ensure that their outputs are recognisable as artificially generated or manipulated and are labelled

---

148 *Borges*, CR 2024, 497, 499 (para. 22).

149 *Kumkar*, in: Hilgendorf/Roth-Isigkeit, The new EU regulation on artificial intelligence [Die neue Verordnung der EU zur Künstlichen Intelligenz], 2023, p. 119; *Martini*, in: Martini/Wendehorst, AI Act [KI-VO], 2024, Art. 50 para. 46; *Merkle*, RDi 2024, 414, 418 (para. 30); on the concept of "interaction", see, for example, *Bomhard/Merkle,* RDi 2021, 276, 282 (para. 35); *Merkle,* RDi 2024, 414, 418 (para. 32).

accordingly in a machine-readable format. According to its wording, Article 50(2) AI Act therefore constitutes a technical requirement obliging a generative AI system to generate a machine-readable label accompanying the relevant output and to ensure that the output is recognisable to the human viewer as artificially generated or processed.[150] The subsequent handling of such labelling is only partially regulated in the AI Act, for example, in Article 50(4), and otherwise follows from the general rules of Union and national law, such as Article 35 of the Digital Services Act (see also recitals 120 and 136 AI Act).[151]

Article 50(3) and (4) AI Act sets out the transparency obligations for deployers of certain AI systems. Article 50(3) AI Act contains a transparency obligation regarding systems for emotion recognition or biometric categorisation. According to this, the deployer of such AI systems must inform the natural person concerned about the system's operation.

Article 50(4) AI Act imposes disclosure obligations on deployers of AI systems that generate "deepfakes" or texts intended to inform the general public about matters of public interest. The subject matter here is, therefore, the regulation of certain AI-generated content, including deepfakes, and matters of public interest. The obligation is addressed to the deployer of the AI system used to generate the content. The substance of the provision is the duty to label the content as a deepfake or as content of public interest. Deepfakes and matters of public interest raise legal questions in numerous areas of law.[152] Article 50(4) AI Act is obviously not intended to provide a comprehensive legal regulation of this issue, but rather to provide a building block for this purpose.

7. Supervision of AI systems and penalties

In addition to the substantive rules governing AI systems and models, the mechanisms in place for supervising the relevant obligations are of central interest. The

---

150 *Lauber-Rönsberg*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 50 para. 31, 34; *Molavi Vasse'i*, RDi 2024, 406, 407 (para. 10); *Kumkar/Griesel,* KIR 2024, 117, 124, take a different view, assuming only an obligation to provide machine-readable labelling; according to *Becker,* CR 2024, 353, 359 (para. 54), there is no requirement for "recognisability for everyone without aids".

151 On the interaction between Art. 50 AI Act and Art. 35 DSA, see *Oster*, in: Gersdorf/Paal, BeckOK, Information and Media Law [Informations und Medienrecht], 49th edition (as of 1 August 2025), Art. 35 DSA para. 49 ff.; also *Klass*, ZUM 2025, 485, 490 f.; *Tilson/Eichinger,* BKR 2024, 648, 654.

152 See, for example, *Kraetzig*, CR 2024, 207 and 276, on tortious protection of personality rights against deepfakes.

AI Act's rules on supervision are set out in the extensive Chapter IX (Art. 72 - 94) AI Act, which implements various supervision instruments across five sections, and in Chapter XII, entitled "Penalties" (Art. 99 - 101) AI Act. In addition, other instruments of Union law and the national law of the Member States are also relevant. A comprehensive presentation of these supervision procedures is beyond the scope of this article. The following section, therefore, provides an overview of the AI Act's provisions on supervision (section 3 (a)) and penalties (section 3 (b)).

a. An overview of the supervision of AI systems and general-purpose AI models

As is customary in European law, the supervision of AI systems and general-purpose AI models is carried out through the interplay of different regulatory levels and complexes. In particular, supervision is only partially regulated in the AI Act and is essentially subject to the general rules of European product safety law.

aa. Supervision of AI systems

The supervision of AI systems is regulated in Section 3 (Art. 74 - 84) AI Act, entitled "Enforcement". According to Article 74(1) AI Act, the Market Surveillance Regulation[153] applies to the supervision of AI systems under the AI Act. This integrates the supervision of AI systems into the product safety law supervision framework.

According to Article 74 AI Act, the subject of supervision is the AI systems. Since the purpose of supervision is to ensure compliance with substantive requirements, only AI systems that are prohibited, classified as high-risk, or subject to transparency obligations fall within its scope. For high-risk AI systems within the meaning of Article 6(1) AI Act, in conjunction with Annex I, supervision is carried out pursuant to Article 74(3) and (4) in accordance with the relevant legal act. The supervisory requirements under the AI Act, therefore, apply primarily to high-risk AI systems within the meaning of Article 6(2) AI Act in conjunction with Annex III.

According to Article 74(1) AI Act in conjunction with Article 11 of the Market Surveillance Regulation, responsibility for supervision under the AI Act lies with the national market surveillance authorities. According to Article 70(1) AI Act, each Member State must establish or designate a market surveillance authority.

---

153 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance).

Also, shall designate a market surveillance authority to act as the single point of contact for the AI Act (Art. 70(2) sentence 3 AI Act). Member States may concentrate the tasks of the two authorities into a single authority or assign them to different authorities.

In Germany, according to the draft bill[154] for an AI Act Implementation Act[155], the Federal Network Agency will act as the competent national authority (Art. 1, sec. 2(1) Draft AI Implementation Act). In the other EU Member States,[156] the approach seems quite similar, i.e., concentrating tasks in one authority. Differences primarily lie in the designation of the authorities. In some cases, a new authority is designated as the single point of contact, as in Spain.[157] More often, the task is assigned to an

---

154 See, for example, *Wünschelbaum,* MMR 2025, 259 f.

155 Draft law implementing Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144, as well as Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Regulation on Artificial Intelligence) (Act implementing the AI Act), available at https://bmds.bund.de/fileadmin/BMDS/Dokumente/Gesetzesvorhaben/CDR_Anlage1-250911_RefE_KIVO-Durchf%C3%BChrungsgesetz_Entwurf_barrierefrei.pdf (last accessed on 2 October 2025).

156 The Commission publishes a continuously updated list of single points of contact, available at https://digital-strategy.ec.europa.eu/de/policies/market-surveillance-authorities-under-ai-act#1720699867912-2 (last accessed on 10 November 2025).

157 *Spanish Agency for the Supervision of Artificial Intelligence [Agencia Española de Supervisión de Inteligencia Artificial]*, established by Royal Decree 729/2023 of 22 August, approving the Statute of the Spanish Agency for the Supervision of Artificial Intelligence, Official State Gazette No. 210 of 2 September 2023, Sec. I, p. 122289, available at https://aesia.digital.gob.es (last accessed on 10 November 2025).

existing authority with supervisory powers, as in Ireland[158], Italy[159], Latvia[160], Lithuania[161], Luxembourg[162], Slovenia[163], and Cyprus[164].

The supervisory procedure is governed by the rules of the Market Surveillance Regulation, thereby aligning with the European market surveillance system for products (see recital 156 AI Act).[165] Accordingly, Article 74 AI Act refers to the rules of the European Market Surveillance Regulation with regard to terminology, competence and cooperation, as well as the powers of market surveillance authorities. This integrates the supervision of AI systems into the general regime of product safety supervision.

The AI Act also contains a whole series of additional rules to address the specific risks of AI systems and ensure effective monitoring of AI systems. In particular, pursuant to Article 79(2) AI Act, sentence 1, the market surveillance authority has a duty to intervene if an AI system "present a risk [...]". The term "product presenting a risk" is defined in Article 3 No. 19 of the Market Surveillance Regulation by means of a complex risk assessment and refers to products bearing unreasonable risk, i.e., "[…] having the potential to affect adversely health and safety of persons in general […], to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose").

If the market surveillance authority suspects such risks, it shall evaluate the system in question (Art. 79(2) subparagraph 1 AI Act) and request the relevant operator (cf.

---

158 *Department of Enterprise, Tourism and Employment*, available at https://enterprise.gov.ie (last accessed on 10 November 2025).

159 *National Cybersecurity Agency [Agenzia per la cybersicurezza nazionale]*, established by Decree-Law No. 82 of 14 June 2021, published in the Official Gazette of the Italian Republic, No. 140 of 14 June 2021.

160 *Consumer Rights Protection Center* [*Patērētāju tiesību aizsardzības centrs]*, available at https://www.ptac.gov.lv (last accessed on 10 November 2025).

161 *Communications Regulatory Authority of the Republic of Lithuania [Lietuvos Respublikos ryšių reguliavimo tarnyba]*, available at https://www.rrt.lt (last accessed on 10 November 2025).

162 *National Data Protection Commission*, available at https://cnpd.public.lu/de.html; appointment as market surveillance authority planned in Art. 7(1) of the draft law.

163 *Agency for Communication Networks and Services of the Republic of Slovenia [Agencija za komunikacijska omrežja in storitve Republike Slovenije]*, available at https://www.akos-rs.si (last accessed on 10 November 2025).

164 *Office of the Commissioner for Electronic Communications and Postal Regulation [Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων (ΓΕΡΗΕΤ)]*, available at https://www.ocecpr.ee.cy (last accessed on 10 November 2025).

165 *Borges*, CR 2024, 497, 501 (para. 34); *Djeffal*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 74 para. 1.

Art. 3 No. 8 AI Act) to take corrective actions (Art. 79(2) subparagraph 2 AI Act). Pursuant to Article 79(5) AI Act, if these corrective actions are not taken within the specified period, the market surveillance authority shall prohibit or restrict the availability of the AI system or the product containing the AI system in the national market. Furthermore, Article 79(9) AI Act obliges the market surveillance authority to withdraw the product or AI system from their market if necessary, without undue delay.

The market surveillance authorities also possess a number of additional powers. For example, pursuant to Article 74(12) AI Act, the market surveillance authority has unrestricted access to documentation and to the training, validation and testing data sets used for the development of high-risk AI systems. In accordance with Article 76 AI Act, the market surveillance authority also monitors tests conducted under real-world conditions, within the meaning of Article 60.

Finally, pursuant to Article 80(1) AI Act, the market surveillance authority has a duty to review the classification of AI systems designated as non-high-risk by the provider pursuant to Article 6(3) and to take further measures if necessary. In particular, if the authority concludes from its evaluation that the AI system qualifies as high-risk, it must require the provider to comply with the applicable requirements for high-risk AI systems (Article 80(2) AI Act). Any breach of this obligation is punishable by a fine pursuant to Article 80(4) AI Act.

Pursuant to Article 83 AI Act, the market surveillance authority also monitors the formal obligations of providers, such as issuing a declaration of conformity in accordance with Article 47 AI Act, affixing the CE marking in accordance with Article 48 AI Act, registration in accordance with Article 71 AI Act, and the availability of technical documentation in accordance with Article 11 AI Act.[166]

bb. Supervision of general-purpose AI models

The supervision of general-purpose AI models is regulated in Chapter IX, Section 5 (Art. 88 - 94) AI Act. According to Article 88(1) AI Act, the Commission has the exclusive authority to supervise general-purpose AI models,[167] and the tasks are carried out by the AI Office. The Commission has the usual supervisory powers, such as the right to request documentation (Art. 91 AI Act), to carry out assessments

---

166 See further, *Djeffal*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 83 para. 13 f.

167 *Borges*, CR 2024, 497, 502 (para. 45); *Cornelius*, in: Schefzig/Kilian, BeckOK, AI Law [KI-Recht], 3rd edition (as of 1 August 2025), Art. 88 para. 12.

(Art. 92 AI Act), and to take measures to monitor and order compliance with the regulation (Art. 89 and 93 AI Act).

b. Penalties

Chapter XII ("Penalties") with Articles 99-101 AI Act sets out the rules on penalties for infringements of the AI Act. Article 99(1) AI Act requires Member States to lay down rules on penalties and other enforcement measures. For example, pursuant to Article 99(3) AI Act, infringements of the prohibitions in Article 5 AI Act are punishable by fines of up to €35 million or 7% of global annual turnover in the case of an offending undertaking, whichever is higher. According to Article 99(4), in the event of violations of certain other obligations – for example, the obligations of providers of high-risk AI systems under Article 16 AI Act, deployers' obligations under Article 26 AI Act, or the transparency obligations under Article 50 AI Act, the fine shall be up to €15 million or 3% of global annual turnover, whichever is higher.

A separate standard applies to providers of general-purpose AI models, Article 101 AI Act. Here, the fine framework applies as in Article 97, i.e. 3% of global annual turnover or €15 million.

A separate standard applies to providers of general-purpose AI models (Article 101 AI Act). In this case, the fine corresponds to that set out in Article 97, i.e. up to 3% of global annual turnover or €15 million, whichever is higher.

8. The impact of the AI Act on Japanese providers and deployers of AI systems and providers of general-purpose AI models

The AI Act is of considerable importance for providers and deployers of AI systems outside the European Union. Under the AI Act, there is direct applicability (see section 1(a) below). In addition, the AI Act also has an indirect applicability to providers and deployers insofar as they are part of a supply chain that falls partially within the scope of the AI Act (see section 1(b) below).

However, the international applicability of the AI Act is of practical relevance only to the extent that it imposes substantive obligations, namely, where it concerns general-purpose AI models, high-risk AI systems, or those covered by the prohibitions in Article 5 AI Act or the transparency obligations under Article 50 AI Act.

a. The applicability of the AI Act on Japanese Providers and deployers

The principles governing the international scope of the AI Act (see section 2(c) above) give rise to a number of important categories of cases in which providers and deployers of AI systems are directly subject to the AI Act:

aa. Supply of AI systems to customers in the EU

Where AI systems are supplied to customers within the EU, the AI Act will often already apply to the provider of the AI system under Article 2(1) lit. a) AI Act, since placing on the market in the Union is deemed to occur where the recipient of the AI system has its establishment in the EU.

Furthermore, the AI Act will also apply under Article 2(1) lit. c) AI Act, as in such cases, the results of the AI system are typically intended for use within the EU. This applies both to situations in which AI systems are integrated into products and to those in which the outputs of AI systems are used directly by humans. For example, where an AI system is integrated into a vehicle, the output of that system is used within the Union. The same applies where an AI system generates output for interaction or communication with humans.

bb. Services involving AI systems for customers in the EU

Another vital case group for the applicability of the AI Act to deployers and providers of AI systems arises when AI systems are used to provide services to customers in the EU. This can be illustrated by the example of an AI chatbot serving users in the EU, as is the case with ChatGPT. The same applies where analyses are performed by AI systems for customers in the EU, for instance in the situations listed in Annex III. If, for example, a service provider in a third country evaluates a job interview or a university application using an AI system on behalf of an employer or university in the EU, this also constitutes use of the output in the Union within the meaning of Article 2(1) lit. c) AI Act, thereby triggering the international applicability of the AI Act to the deployer.

If such an AI system (e.g. for evaluating job interviews) is manufactured by a provider in a third country that is intended to provide such services to EU customers, the provider is likewise subject to the rules of the AI Act pursuant to Article 2(1) lit. c) AI Act.

Providers and deployers of AI systems in third countries can, in any case, avoid the applicability of the rules governing high-risk AI systems by excluding either the

use of the AI system as a safety component of a product (Article 6(1) AI Act) or the use of its outputs in high-risk areas (Article 6(2) AI Act).

cc. Supply of general-purpose AI models to customers in the EU

The AI Act can be internationally applicable to providers of general-purpose AI models only under Article 2(1) lit. a) AI Act. The connecting factors set out in Article 2(1) lit. b) and lit. c) AI Act do not apply to providers of general-purpose AI models.

The AI Act is therefore only applicable to providers of general-purpose AI models if they place them on the market in the Union (Article 2(1) lit. a) AI Act), i.e. supply them to customers established in the EU (see section 2(c)aa) above).

b. The indirect impact of the AI Act

The AI Act will often have an indirect impact on providers and deployers of AI systems, as well as providers of general-purpose AI models. This is particularly the case in relation to the supply of general-purpose AI models or AI systems as components of products intended for use in the EU.

In these cases, the distributors of such AI system components are not directly addressed by the AI Act, as it applies only to the provider of an AI system, that is, the final link in the value chain for the creation of a general-purpose AI model or AI system. The provider of the general-purpose AI model or AI system is responsible for compliance with the requirements of the AI Act and must ensure such compliance throughout the entire value chain, insofar as the characteristics of the general-purpose AI model or AI system are determined at various stages of its development.

The same applies to the manufacturer of a product that integrates one or more AI systems. Insofar as the product is subject to European product safety law, the manufacturer must regularly ensure the conformity of the product as a whole, including all its components. In addition, pursuant to Article 25(3) AI Act, the manufacturer of a product in which a high-risk AI system within the meaning of Article 6(1) AI Act is integrated is itself regarded as the provider of that high-risk AI system if it places the system on the market together with the product under its own name or trademark, or if the high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market (Article 25(3) lit. a) AI Act). As this is typically the case, the manufacturer of the product must comply with all obligations of the AI Act in relation to the integrated AI systems.

In such cases, the distributor of an AI system and the manufacturer of a product will contractually transfer the obligations under the AI Act to their provider. Ultimately, these obligations will be passed along throughout the entire supply chain. For example, for high-risk AI systems, this extends to the selection of training data for the underlying model in order to meet the obligations under Article 10 AI Act. Providers will, therefore, as is customary in other areas of product safety law, regularly be contractually bound by the obligations under the AI Act.

To facilitate this task for providers of AI systems, the AI Act obliges providers of general-purpose AI models to document and provide information to providers of AI systems (cf. Article 53 AI Act). Furthermore, Article 25(4) AI Act requires cooperation between the provider of a high-risk AI system and third-party suppliers of AI systems used within high-risk systems. This cooperation must be set out in a written agreement specifying the necessary information that will enable the provider of a high-risk AI system to fulfil its obligations under the AI Act.

9. Recommendations for providers and deployers of AI systems and general-purpose AI models from third countries

A number of recommendations for action can be derived from the provisions of the AI Act and from their direct and indirect applications to providers and deployers of AI systems and general-purpose AI models from third countries:

- Analysis of impact

Providers of general-purpose AI models and AI systems, as well as deployers of AI systems, should assess whether and which provisions of the AI Act apply to them.

- Control of the distribution channel

Providers of general-purpose AI models and AI systems should establish clear provisions regarding their distribution and place of use in connection with placing on the market and putting into service within the EU. If this is not intended, such use should be explicitly excluded. These provisions should be contractually agreed upon with the recipients of the general-purpose AI models and AI systems.

Providers should also pay close attention to whether their general-purpose AI models and AI systems are being placed on the market in the EU. In the case of AI systems, it should additionally be monitored whether their outputs are used within the EU.

- Determination of the intended purpose and location of use of general-purpose AI models, AI systems and their outputs

Providers of general-purpose AI models and AI systems should establish clear contractual rules with their partners regarding the intended purpose and location of use of such systems, particularly with respect to prohibitions, use in high-risk areas, and interactions with customers in the EU within the meaning of Article 50 AI Act. Where use is not intended, it should be expressly excluded. These provisions should be clearly set out in the technical documentation and in the instructions for use.

- Contractual rules on the use of AI systems and their outputs

Providers of general-purpose AI models and AI systems should agree on clear contractual rules with their partners regarding the use of the models or systems, particularly with respect to prohibitions, use in high-risk areas, or interactions with persons within the meaning of Article 50 AI Act. In particular, use for prohibited purposes within the meaning of Article 5 AI Act should be expressly excluded, where applicable. Deployers of generative AI systems should, where appropriate, exclude the use of outputs from such systems for deepfakes or for informing the public about matters of public interest.

- Compliance with the AI Act's obligations

Insofar as the obligations under the AI Act apply, they should be complied with to avoid penalties and liability (see section 7(b) above), and compliance should be carefully documented.

- Cooperation with authorities in the EU

Providers of high-risk AI systems should consider cooperating with EU authorities in order to meet their relevant duties. In particular, an AI real-world testing plan is advisable, as it enables cooperation with the competent supervisory authority prior to market launch.

- Passing on obligations in the supply chain

Providers of general-purpose AI models and AI systems should require their distributors to comply with the AI Act and further require them to pass on the AI Act's requirements to their (sub)distributors.

- Cooperation in technical standardisation

Providers, trade associations, and standardisation bodies from third countries should, where appropriate and with government support, participate in the technical standardisation of AI models and AI systems in order to harmonise them with their own standards.

- Minimising compliance costs

Providers of general-purpose AI models and AI systems, as well as deployers of AI systems, should seek to minimise the costs associated with compliance under the AI Act. Government agencies and trade associations in third countries can provide effective support in this respect, for example, by issuing guidelines for assessing the applicable obligations and their fulfilment. Cooperation with EU agencies may also be beneficial in this regard.

10. Evaluation of the EU AI Act

a. AI regulation under the EU AI Act

Contrary to its title, the AI Act is not a comprehensive regulation on artificial intelligence or even on AI systems.[168] Rather, it is primarily a special product safety law for AI systems.[169] Overall, the AI Act is a complex piece of legislation with very diverse content.[170] Its central characteristic is its restriction to AI systems as the subject of regulation, specifically software generated using machine learning methods and large AI models as the central components of some AI systems.[171] Accordingly, the AI Act is cross-sectoral, i.e., a horizontal regulation,[172] and thus constitutes a technology-specific framework that addresses particular aspects of AI, primarily the risk management obligations of AI system providers.

Numerous legal issues relating to the manufacture and use of AI systems are – rightly – regulated elsewhere or are still awaiting regulation, such as liability for AI systems.[173] The gaps in the legal framework are almost impossible to predict, given the possible areas of application for AI systems, including automated decisions, assessments, content generation, etc.[174]

---

168 *Borges*, CR 2024, 497, 506 (para. 99); see also *Rohrßen*, ZfPC 2025, 6.

169 *Borges*, CR 2024, 497, 506 (para. 99); see also *Hecht*, KIR 2025, 30, 37; *Krönke*, NVwZ 2024, 529, 531; *Lejeune*, ITRB 2025, 99, 104; *Rohrßen,* ZfPC 2025, 6, 13; *Spindler,* CR 2021, 361, 362; *Stieper/Denga,* GRUR 2024, 1473, 1481.

170 *Borges*, CR 2024, 497, 506 (para. 100).

171 *Borges*, CR 2024, 497, 506 (para. 100).

172 *Borges*, CR 2024, 497, 506 (para. 101); *Rohrßen*, ZfPC 2025, 6, 8; see also, *Chibanguza/Steege*, NJW 2024, 1769, 1773 (para. 41).

173 *Borges*, CR 2024, 497, 506 (para. 99).

174 *Borges*, CR 2024, 497, 506 (para. 99).

The AI Act brings important innovations to European product safety law.[175] Overall, risk management for AI systems is a tremendous task of enormous complexity.[176] In this respect, the AI Act provides the legal basis for new institutions and mechanisms to establish material conditions for AI systems, set out procedures for evaluating AI systems, thereby facilitating the application of product safety law to AI systems.

In addition, the AI Act extends product safety law, including the supervision of privacy protection. This application is highly interesting from a scientific point of view, as rules safeguarding privacy rights have thus far applied only to the use of results, but not to the earlier stages of software development where outputs with implications for privacy are generated. Whether this legislative experiment will succeed is undoubtedly one of the most exciting scientific questions in connection with the AI Act.

The AI Act is not limited to product safety law but also contains a diverse, though somewhat loosely connected, set of additional provisions, ranging from obligations to promote AI literacy to prohibitions, transparency obligations, and a general right of appeal.[177] In this area, the AI Act loses much of its persuasive force.[178]

b. The EU AI Act from the Japanese perspective

Whether the AI Act can serve as a model for legislation in other countries, in particular for Japan, is a difficult question. Since its main area of regulation, namely the rules on risk management for high-risk AI systems, is closely linked to European product safety law, and Japan, like most countries, does not rely on a comparable frameworks, the question appears at first glance to be answered in the negative.

However, the main regulatory objectives and principles of product safety law, namely the manufacturer's responsibility for product quality, the obligation to carry out conformity assessments, and the existence of state supervision with powers of intervention, such as ordering a product recall, are correct and also apply to AI systems as products or their components. Nonetheless, it cannot be denied that the AI Act's regulatory framework is enormously complex, if only because of the large number of institutions involved and the complex procedures required. Another

---

175 *Borges*, CR 2024, 497, 506 (para. 102).

176 *Borges*, CR 2024, 497, 506 (para. 103).

177 *Borges*, CR 2024, 497, 506 (para. 105).

178 *Borges*, CR 2024, 497, 506 (para. 105).

problem is the enormous amount of compliance duties that the AI Act imposes on providers and deployers of products with software components.

For this reason alone, not all countries will be able to afford such a regulatory model, at least in the form of the European example. However, industrialised countries with high levels of international integration, which already have intensive industry regulation, must, like the EU, consider how to regulate the safety requirements for AI systems and integrate them into existing law.

The AI Act has an almost global scope of application, if only because of its far-reaching international scope. In addition, it is likely to have a significant indirect impact through contractual obligations required to comply with the regulation in international supply chains.

Competition between numerous national and regional regulations governing AI systems can significantly hinder their development and deployment due to the associated costs, thereby severely undermining the anticipated economic and social benefits of artificial intelligence. Altogether, dispensing with legal regulation of AI system safety is not an option, as ensuring citizens' safety is one of the state's central responsibilities. The solution, therefore, lies in efficient regulation that minimises competition between diverging legal and technical requirements as far as possible. A key component of this solution undoubtedly lies in the harmonisation of technical requirements for AI systems through international standardisation.

c. The AI Act from the perspective of providers and deployers

From the perspective of providers and deployers of AI systems, the AI Act entails additional effort in terms of testing and, where necessary, compliance with its obligations. However, its substantive provisions apply only to a very limited group of AI systems, meaning that most AI models and AI systems can be developed, distributed, and used without restriction.

The AI Act also enhances legal certainty by regulating aspects that are already largely, but not entirely, covered by product safety law. Moreover, it has indirect significance beyond product safety law. It is widely assumed that the requirements of the AI Act will also be relevant to liability for damage caused by AI systems (see below V.).

For providers and deployers in Japan, as well as those based in the EU, it will be essential to minimise the costs of evaluating and ensuring compliance with the AI Act, where appropriate, with government support or through trade associations.

III. Data protection challenges for providers of AI systems and AI models

Data protection law poses considerable challenges for providers, operators and users of AI systems. In many cases, data protection requirements are seen as a major obstacle to the development and use of AI models and AI systems.

The extensive issues involved cannot be analysed comprehensively here. First, the regulatory concepts of the European General Data Protection Regulation (GDPR) (see 1. below) and the main points of the current data protection debate on AI models and AI systems are outlined below (see 2. below). Three core aspects of the GDPR relating to the development and use of AI models and AI systems will then be discussed: the applicability of the GDPR to the development, distribution and use of AI models and AI systems (below 3.), data protection responsibility (below 4.) and the data protection justification for these processes (below 5.)..

The discussion is based on four key processes:

(1) the development of an AI model.

This process involves numerous different data processing operations, from data collection to testing the AI model. This refers only to the direct data processing involved in development, specifically the storage of data for training and the use of data for training and testing the model.

(2) the provision of an AI model or AI system.

This process includes storage on a server and provision, for example on a platform or website, in such a way that third parties, such as customers, can access the model or data in order to download it and use it themselves.

(3) Operating an AI system. This process refers to the operation, i.e. running the system, on one's own responsibility, for example within the meaning of Article 3(4) of the AI Regulation.

(4) Using an AI system.

This process refers exclusively to the initiation of inputs to the AI system, for example through a prompt, the generation of an output by the system and the receipt or retrieval of this output.

1. The GDPR at a glance

The GDPR is the central data protection law in the European Union (EU). It has been applicable since 25 May 2018 and applies directly throughout the EU. In addition, there are numerous other legal rules on data protection both at the level of Union law and in the national law of the Member States. At EU level, Directive

(EU) 2016/680[179] is particularly important, as it regulates data protection requirements in the area of law enforcement. Numerous sector-specific legal acts contain data protection provisions.

The GDPR is expected to undergo significant changes in the near future. According to the draft Digital Omnibus Regulation[180] , the GDPR is to be amended in specific areas. The amendments concern important fundamentals, such as the concept of personal data (see 2. b. below), the rules of Art. 9 GDPR on special categories of personal data, in particular health data, and various areas relating to information obligations (Art. 13 f. GDPR). New rules are also planned for the processing of personal data on end devices (Article 88a GDPR-E) and for the consideration of machine-readable consent signals (Article 88b GDPR-E), which are primarily intended to regulate the use of cookies in a practical manner. Of particular interest in connection with AI is the proposed provision on the justification of the processing of personal data for AI development (Art. 88c GDPR-E; see 5. a. below).

The subject matter of the GDPR is the (partially) automated processing of personal data. The central legal principle of the GDPR is the requirement of justification (see 5 below) for any automated processing of personal data (see 2. a. below). This principle is accompanied by a series of obligations imposed on those involved in data processing. , the obligations are primarily imposed on the controller (see 4. a. below), as well as on the bodies involved in data processing on behalf of the controller (see 4. a. below). The obligations include, for example, informing the data subject (Art. 13 f. GDPR), documenting data processing and assessing its consequences, and ensuring the security of data processing (Art. 32 GDPR). Further obligations arise from the conditions for justification together with the principles of data processing set out in Art. 5 GDPR, such as limiting data processing to what is necessary (principle of data minimisation).

Enforcement of the GDPR is ensured by the legal rights of the data subject whose data is being processed, but above all by a state data protection authority with strong

---

179 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ (EU) L 119, 4.5.2026, p. 89.

180 *European Commission*, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final.

powers of intervention. The data protection authorities are located in the Member States. They are responsible for supervision in their respective Member States. The coordination of data protection authorities is carried out by rules of the Union and its institutions, such as the European Data Protection Board, which cooperates with the European data protection supervisory authorities and develops common positions on important legal issues. With regard to supervision, a one-stop shop principle applies (cf. Art. 56(6) GDPR)[181] ; the competent supervisory authority is generally responsible for the (specific) data processing in all Member States in accordance with Art. 56(1) GDPR[182] .

The powers of the supervisory authority regulated in Art. 58 GDPR include, among other things, requiring the parties involved to provide information (Art. 58(1)(a) GDPR), to investigate compliance with data protection requirements (Art. 58(1)(b) GDPR) and also to prohibit data processing in the Union (Art. 58(2)(f) GDPR).

The GDPR provides for special restrictions on the transfer of data to third countries in Art. 44 et seq. GDPR. A transfer to a third country in this sense, which triggers the special rules, already exists if the possibility of accessing data in the EU is provided. For example, in cloud computing, if the cloud providers operate this service according to the follow-the-sun principle, this constitutes a transfer to a third country.[183]

The special restrictions on third-country transfers[184] do not apply if the European Commission has issued an (effective) adequacy decision for the country in question (Article 45(1) GDPR). The Commission has made such a decision for 15 countries

---

181 *Ambrock/Karg*, in: von dem Bussche/Voigt, Konzerndatenschutz (Group Data Protection), 2nd edition 2019, Part 8, margin note 44; *Bavarian State Office for Data Protection Supervision*, EU General Data Protection Regulation (GDPR) – The BayLDA on the way to implementing the Regulation, as of 12 December 2016, available at https://www.lda.bayern.de/media/baylda_ds-gvo_13_one_stop_shop.pdf (last accessed on 28 November 2025); *Dieterich*, ZD 2016, 260, 264; *Schneider*, Data Protection under the EU General Data Protection Regulation, 2nd edition 2019, p. 90; *Wagner*, ZD-Aktuell 2019, 06546; for details on the one-stop-shop concept, see *Dix*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 56 para. 5 ff.

182 *Ambrock/Karg*, in: von dem Bussche/Voigt, Group Data Protection, 2nd edition 2019, Part 8 para. 44; *Bavarian State Office for Data Protection Supervision*, EU General Data Protection Regulation (GDPR) – The BayLDA on the way to implementing the Regulation, as of 12 December 2016, p. 1, available at https://www.lda.bayern.de/media/baylda_ds-gvo_13_one_stop_shop.pdf (last accessed on 28 November 2025); *Nguyen*, in: Gola/Heckmann, GDPR, BDSG, 3rd ed. 2022, Art. 56 para. 17 f.; *Wagner*, ZD-Aktuell 2019, 06546.

183 *Borges*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rechtshandbuch, 3rd ed. 2019, Part I, Chapter 3 para. 102 f.

184 See *Paal*, NJW 2024, 3681, on data transfers to third countries under the GDPR.

and one international organisation to date.[185] The USA is also particularly relevant with regard to data that is significant under the rules of the DPF. However, the effectiveness of the adequacy decision for the USA is controversial.[186] The commission has made an adequacy decision regarding Japan in 2019[187] Therefore, European entities may transfer data to Japan to the same extent as within the European Union.

In the event of violations of the provisions of the GDPR, the supervisory authority may impose fines. The fines are extremely high and, depending on the severity of the violation, can range up to €20 million or up to 4% of annual turnover for serious violations, and up to €10 million or up to 2% of annual turnover for the group of companies for other violations (Art. 83 GDPR).

In recent years, European supervisory authorities have imposed heavy fines in numerous cases,[188] including on companies from third countries.

For several years now, there has been increasingly intense discussion about reforming the GDPR. The main thrusts of this discussion are, on the one hand, the use of modern technologies such as AI and big data and, on the other hand, efforts to deregulate. The planned Digital Omnibus Regulation is a first step towards an immediate reform of the GDPR and Directive 2016/680. In addition, there are special rules in sector-specific legislation. For example, the European Health Data Space contains provisions on the processing of personal data that take precedence over the GDPR and, in essence, entail serious restrictions on data protection.

---

185 See the *European Commission's* list, available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last accessed on 27 November 2025); see also *Juarez*, in: Wolff/Brink/von Ungern-Sternberg, BeckOK-Datenschutzrecht, 53rd edition (as of 1 August 2025), Art. 45 GDPR, para. 53 et seq.

186 The General Court considers the adequacy decision on the DPF to be valid: General Court, judgment of 3 September 2025, T-553/23 – Latombe v Commission, operative part published in OJ (EU) C, C/2025/5446 of 20 October 2025; see, for example, on the validity of the DPF, *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 45 para. 84 ff.; *Glocker*, RDi 2023, 465; *idem*, ZD 2023, 189; *Hanßen*, DB 2023, 1777; *Hessel*, NJW 2023, 2969; *Johnson/Kornbrust*, ITRB 2023, 238; *Roßnagel*, MMR 2023, 64.

187 COMMISSION IMPLEMENTING DECISION (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, O.J. 2019 II L 76/1.

188 An overview of the fines imposed by German supervisory authorities in 2023 and 2024 is provided by *Ihwas*, CCZ 2025, 33.

2. Processing of personal data in the development of AI models and use of AI systems

The following section examines the conditions under which personal data is processed in the context of the development of AI models and AI systems.

a. The material scope of the GDPR

The material scope of the GDPR is regulated in Art. 2 GDPR. According to Art. 2(1) GDPR, the GDPR applies to the processing of personal data wholly or partly by automated means, and also to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

The term "data" is to be understood in the sense of information[189] and is broadly defined in this respect[190] . Processing is any form of handling information, from collection, storage and transmission to content analysis or modification (cf. Article 4(2) GDPR).[191]

Data processing is considered to be at least partially automated if data is stored, transmitted or analysed by a computer.[192] This is the case whenever a device is used to create text, process sensor data, or store or transmit data electronically.

The provision of the technical infrastructure also constitutes processing within the meaning of the GDPR. The provider of a cloud service, for example, is involved in the storage and other processing that takes place on the infrastructure. Similarly, the operator of an AI system is involved in the data processing carried out by the AI system. The storage of an AI model also constitutes relevant involvement in data processing and is therefore to be classified as partially automated data processing.

---

189 See *Ernst*, in: Paal/Pauly, DS-GVO BDSG, 3rd ed. 2021, Art. 4 GDPR margin no. 3; *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 4 No. 1 GDPR margin no. 2.

190 See *Ernst*, in: Paal/Pauly, DS-GVO BDSG, 3rd ed. 2021, Art. 4 GDPR marginal no. 3; *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2nd ed. 2025, Art. 4 No. 1 GDPR marginal no. 3.

191 For information on the individual processing operations, see *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 4 GDPR margin note 32 et seq.

192 See *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 2 GDPR marginal no. 6; *Kühling/Raab*, in: Kühling/Buchner, DS-GVO BDSG, 4th edition 2024, Art. 2 GDPR margin note 15.

b. The concept of personal data

The GDPR does not apply to all data processing, but rather, according to Art. 2(1) GDPR, to the processing of personal data. The term "personal data" is defined in Art. 4(1) GDPR and comprises information about the circumstances of a natural (living)[193] person whose identity is known or can be determined.

aa. Information about natural persons

Personal data within the meaning of Art. 4 No. 1 GDPR is only information about natural persons. Information about the circumstances of legal persons or other legal entities (e.g. companies)[194] , other entities (animals, etc.) or objects[195] is not personal data.

The circumstances of a (natural) person include their characteristics, such as physical characteristics[196] , and, in principle, their actions and relationships with other persons or objects[197] . These relationships include both actual and legal relationships.

Legal relationships with other persons, such as contractual relationships, are therefore to be regarded as personal data of the persons involved.[198] Legal or actual relationships of a person to things and other objects are also personal data of the person concerned. Possession and ownership of an object are personal data of the possessor or owner,[199] if this is an identified or identifiable natural person. The Article

---

193 *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 4 GDPR marginal no. 5; *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th edition 2024, Art. 4 No. 1 GDPR marginal no. 5; *Schild*, in: Wolff/Brink/von Ungern-Sternberg, BeckOK-Datenschutzrecht, 53rd edition (as of 1 August 2025), Art. 4 marginal no. 9.

194 Recital 14(2) GDPR; *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 4 GDPR marginal no. 6; *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th edition 2024, Art. 4 No. 1 GDPR para. 4.

195 *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 4 GDPR margin no. 7 f.

196 *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Data Protection Law, 2nd edition 2025, Art. 4 No. 1 GDPR margin note 57.

197 *Ernst*, in: Paal/Pauly, DS-GVO BDSG, 3rd edition 2021, Art. 4 GDPR margin note 14.

198 See OLG Cologne, 26 July 2019 – 20 U 75/18, BeckRS 2019, 16261 para. 62; *Ernst*, in: Paal/Pauly, DS-GVO BDSG, 3rd ed. 2021, Art. 4 GDPR para. 14; *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 4 No. 1 GDPR para. 8.

199 See, for example, *Ernst*, in: Paal/Pauly, DS-GVO BDSG, 3rd ed. 2021, Art. 4 GDPR para. 14; *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 4 No. 1 GDPR para. 8.

29 Data Protection Working Party has developed a concept that assesses information primarily related to an object as personal information on the basis of several (alternative) criteria.[200] According to this concept, which is also relied upon by the ECJ,[201] information refers to a person and not just to an object if there is a content element, a purpose element or a result element that refers to a natural person. This concept has also found approval in the literature[202] .

It is unclear to what extent information relating to a majority of natural persons is to be regarded as personal data. However, essential principles are also recognised here: legal relationships involving several persons are personal data of all identified or identifiable natural persons involved in the legal relationship in question.

bb. Knowledge or determinability of identity

The second essential characteristic of personal data is that the identity of the natural person to whom the information relates is known or at least ascertainable. The decisive – and highly controversial – aspect in this respect concerns the question of whose perspective the person in question must be identified or identifiable from.

In this respect, there are traditionally two basic positions:[203] According to the concept of relative personal reference, it depends on whether the data controller knows or can determine the identity, whereas according to the concept of absolute personal reference, the decisive factor is whether any person can determine the identity.[204] Since the concept of absolute personal reference leads to an unforeseeably wide range of personal data, it is no longer advocated today. However, there are numerous positions, not least in statements by supervisory authorities, which are based on this concept.[205] In addition, there are exceptions, for example in the transfer and, in

---

200 *Article 29 Data Protection Working Party*, Opinion 4/2007 on the concept of "personal data", WP 136, p. 10 ff.

201 ECJ, judgment of 4 May 2023, C–487/21 – CRIF para. 24; still under the DS Directive, ECJ, judgment of 20 December 2017, C– 434/16 – Nowak, para. 35.

202 In agreement, for example, *Klabunde/Horváth*, in: Ehmann/Selmayr, General Data Protection Regulation, 3rd ed. 2024, Art. 4 GDPR para. 10; *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 4 No. 1 GDPR para. 14.

203 See a brief description in *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), BeckOK-IT-Recht, Art. 4 GDPR marginal no. 14 et seq.

204 See also *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 4 No. 1 GDPR margin note 25.

205 *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 4 No. 1 GDPR margin note 25; cf. *Article 29 Data Protection Working Party*, Opinion 4/2007 on the concept of "personal data", adopted on 20 June 2007, WP 136, 01248/07/EN, p. 17 et seq.; *id.*, Opinion 02/2013 on apps on smart devices, adopted on 27 February 2013, p. 10; *Düsseldorf Circle*,

particular, the publication of information. The ECJ has adopted the concept of relative personal reference, but has by no means ruled out exceptions.[206]

The fundamental relevance of relative personal reference leads to the further question of under what conditions identifiability exists. Here, according to the generally agreed opinion, albeit expressed in very different terms, all identification measures that the controller would reasonably take to determine the identity of the data subject must be included in the assessment.[207] This may also include inadmissible and even criminally prohibited measures.[208] Insofar as data is stored, future possibilities for identification must also be considered.[209] This is particularly important in the case of encryption of long-term stored data and is the subject of controversial legal debate.

This means that, for the purposes of identification, all additional information available to the controller or which the controller can obtain with "reasonable" effort must be taken into account. This can vary greatly depending on the circumstances of the case and is highly controversial in many individual cases.[210]

Whether the information is accurate is irrelevant to the personal reference of the information.[211] Therefore, false or misleading information about natural persons may constitute personal data of the person concerned. The possible existence of characteristics, relationships or actions of a natural person is also (according to general understanding) personal data. Rumours about a person are therefore personal data of the person concerned. The objective observer is decisive in this respect. It

---

Guidance on data protection requirements for app developers and app providers (as of 16 June 2014), p. 5; *Pahlen-Brandt*, DuD 2008, 34; for details on the various approaches, see *Bergt*, ZD 2015, 365; *Borges*, in: Borges/Meents, Cloud Computing, Legal Handbook, 2016, § 6 Rn. 20 ff.

206 See ECJ, 19 October 2016, C-582/14 – Breyer, para. 45 ff.

207 See, for example, LG Berlin, ZD 2013, 618, 619 et seq.; *Brink/Eckhardt*, ZD 2015, 205, 210 et seq.; *Karg*, DuD 2015, 520, 525.

208 *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 4 GDPR para. 20; *Klabunde/Horváth*, in: Ehmann/Selmayr, General Data Protection Regulation, 3rd edition 2024, Art. 4 GDPR margin no. 17; *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th edition 2024, Art. 4 No. 1 GDPR margin no. 29.

209 *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 4 GDPR marginal no. 21; for details, see *Hornung/Wagner*, CR 2019, 565, 566 ff.

210 See, for example, *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th edition 2024, Art. 4 No. 1 GDPR margin note 35 et seq.

211 See also *Klabunde/Horváth*, in: Ehmann/Selmayr, General Data Protection Regulation, 3rd ed. 2024, Art. 4 GDPR para. 9; *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 4 No. 1 GDPR para. 8.

therefore depends on whether a reasonable person would understand the information in question as relating to a specific natural person.

According to these principles, the personal reference of a piece of information may change over time. Non-personal information may become personal data due to the changed availability of additional information or other findings.

cc. Anonymisation and pseudonymisation

The personal reference of information can also be removed. This process is called "anonymisation".[212] Anonymous data no longer has any personal reference.[213] In this respect, too, the person responsible must be taken into account. Unfortunately, this actually compelling idea is disputed by numerous bodies, including supervisory authorities, which apparently assume an absolute principle in this respect.

Data can be anonymised, for example, by encryption if the key is no longer accessible to the controller afterwards.[214] In some cases, this (encryption and destruction of the key) is also referred to as erasure. This is not entirely accurate, but it makes it clear that the data is no longer personal data.

Anonymisation can also be achieved by aggregating data.[215] Data relating to a majority of persons is not personal information, provided that the information does not "permeate" to an individual person,[216] i.e. information relating to an individual person cannot be derived from the group-related information.

Anonymisation must be distinguished from pseudonymisation of data. Pseudonymised data is information that the responsible body, but not a third party, can assign to an identifiable natural person. This is important, for example, in the case of encrypted data or data that is assigned to a pseudonym. This data is personal for anyone who can make the assignment. For everyone else, it is non-personal data.

---

212 Recital 26 p. 5 GDPR.

213 *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 4 GDPR margin note 61; *Steidle*, in: Jandt/Steidle, Datenschutz im Internet, 2nd edition 2025, III. margin note 25.

214 See *Schultze-Melling*, in: Taeger/Gabel, GDPR – BDSG – TTDSG, 4th edition 2022, Art. 32 para. 16.

215 Similarly, see *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 4 No. 1 GDPR para. 15 f.

216 See also *Klar/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 4 No. 1 GDPR para. 15.

c. The processing of personal data in the development and provision of AI models and AI systems

In the context of the development and provision of an AI model or AI system, the processing of personal data may occur in various ways.

When data is collected, processed and passed on for training purposes, this often involves the processing of personal data[217] , especially when data is linked to unique identifiers such as the names of natural persons.

The conditions under which and the cases in which personal data is processed when training an AI model are the subject of intense debate. However, the discussion is often confused with the closely related question of whether the trained model stores personal data.

The prevailing view in the discussion is that a model can indeed store personal data.[218] This is justified primarily by the consideration that, when integrated into an AI system and used to generate output, the model can generate information relating to a natural person through an input (a prompt).[219]

In an early statement on generative AI systems[220] , the Hamburg Data Protection Commissioner took the opposite view[221] , essentially arguing that the model does not contain any specific information, but only individual tokens as language frag-

---

217 See *Moos*, CR 2024, 442 (para. 2).

218 *Hansen/Walczak*, KIR 2024, 82, 85 et seq.; *Pesch/Böhme*, MMR 2023, 917, 920; *Schwartmann/Benedikt/Köhler*, Expertenwissen KI und Datenschutz, 2025, p. 15; *Weiden*, in: Bomhard/Pieper/Wende, AI Regulation, 2025, Art. 16 para. 35 et seq.

219 See *Hansen/Walczak*, KIR 2024, 82, 86; *Pesch/Böhme*, MMR 2023, 917, 920, disagree.

220 *The Hamburg Commissioner for Data Protection and Freedom of Information*, Discussion Paper: Large Language Models and Personal Data, p. 6 f., available at https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf (last accessed on 28 November 2025); for details, see *Moos*, CR 2024, 442; see also *Schneider*, in: Bomhard/Pieper/Wende, AI Regulation, 2025, Art. 3 para. 463.

221 *The Hamburg Commissioner for Data Protection and Freedom of Information*, Discussion Paper: Large Language Models and Personal Data, p. 6 f., available at https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf (last accessed on 28 November 2025). See also *Moos*, in: Bernzen/Heinze/Steinrötter, DSRI Autumn Academy 2025, 2025, Data Protection, Data Protection Update 1.2.4; *ibid.*, CR 2024, 442, 444 (para. 15).

ments and so-called embeddings, which are relationships between tokens as mathematical representations of the data processed during training.[222] Neither the former nor the latter contain individual information about natural persons that could be used for identification purposes.[223] Even if information about natural persons could be extracted from a model , it does not necessarily follow that this information is stored in the model. Rather, text could be generated that coincidentally matches training data.[224]

The prevailing view is to be agreed with: according to the general principles of the GDPR, personal data is present if the responsible body, possibly with the aid of technical means and further information, can extract information relating to an identifiable natural person from the data in question with reasonable effort.

This is often the case with AI models, depending on the subject of the training. A crucial problem is that the developer of the model can, at best, only predict to a limited extent whether and, if so, which personal data can be extracted. This is where a key feature of personal reference becomes relevant, which must be assessed from the perspective of the responsible bodies: A piece of data may be personal for one entity, but not for another that cannot reasonably be assigned to a specific natural person. Accordingly, data may not be personal for the developer of an AI model, but it may be personal for the subsequent user of the AI system based on the model. The solution to this problem, which is rarely discussed explicitly, follows from a differentiated consideration of the respective processing operations: as long as the developer uses an AI model exclusively in their own sphere, only their own possibilities of knowledge need to be taken into account; the decisive factor is therefore whether they themselves can make the assignment to a specific person. As soon as the developer passes the model on to a third party, the latter's possibilities of gaining knowledge must also be taken into account. The developer must therefore assess whether the recipient or persons to whom the recipient makes the model accessible

---

222 *The Hamburg Commissioner for Data Protection and Freedom of Information*, discussion paper: Large Language Models and Personal Data, p. 6 f., available at https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf (last accessed on 28 November 2025).

223 *The Hamburg Commissioner for Data Protection and Freedom of Information*, Discussion Paper: Large Language Models and Personal Data, p. 7, available at https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf (last accessed on 28 November 2025).

224 *The Hamburg Commissioner for Data Protection and Freedom of Information*, Discussion Paper: Large Language Models and Personal Data, p. 7, available at https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf (last accessed on 28 November 2025).

can obtain personal data from the model. This essentially leads to the same results as the absolute concept of personal reference, particularly in the case of free publication of the model, and is likely to correspond to the unanimous opinion. The differentiation made here is nevertheless important, as the developer can avoid the applicability of data protection law according to the opinion represented here if they control the use of the model.

The comments on the processing of personal data through the development and dissemination of AI models apply accordingly to AI systems.

d. The processing of personal data when using AI systems

When using AI systems, a distinction must be made between the involvement of the user and the operator of the AI system. The scenario considered here is that of a user from the EU accessing an AI system operated by a provider in a third country.

When accessing an AI system, the user typically transfers personal data to the AI system, and thus to its operator. If the user is a natural person acting on their own responsibility, the GDPR does not apply with regard to their personal data. Insofar as it is for private use, the so-called household exception of Art. 2 (3) GDPR applies, and the GDPR is then not applicable to the transfer as a whole.

Whether personal data is present from the perspective of the operator of the AI system must be considered on a case-by-case basis. The operator may process personal data, in particular with regard to the user's data.

Personal data of the user is present if the user acts within the framework of a user account or has otherwise been identified by the operator or is identifiable to the operator. In this case, all data transferred by the user is also considered personal data, as it can be attributed to the user.

Even if the user is anonymous to the operator, which is typically the case with free services that do not require registration, the operator will often have personal data. This is the case if the entries and other data transmitted by the user contain information about identifiable natural persons.

Even if the existence of personal data must be checked in each individual case according to the legal concept, the operator must in any case expect to process personal data. Therefore, the practice is to assume the processing of personal data as a precautionary measure.

For operators of AI systems, this means that the GDPR may be applicable. This may be based on the operator's own data processing or on data processing initiated by the user. If the operator of the AI system identifies users or stores user data that

enables them to be identified, they themselves initiate the processing of personal data. In addition, the operator of the AI system is involved in the processing of personal data initiated by the user, as they maintain the AI system.

3. The applicability of the GDPR to the development and use of AI systems in Japan

The international scope of the GDPR is regulated in Art. 3 GDPR. Paragraphs 1 and 2 of this provision contain two different connecting factors. According to Art. 3(1) GDPR, the GDPR applies to data processing operations carried out by establishments in a Member State. According to Article 3(2) GDPR, the GDPR applies to data processing carried out by establishments outside the Union if data subjects from the Union are processed for specific purposes, namely the offering of goods or services (lit. a.) or the observation of behaviour (lit. b.).

a. The connection to the establishment (Article 3(1) GDPR)

According to Art. 3(1) GDPR, the GDPR applies to data processing operations carried out by establishments in a Member State. The term "establishment" is not defined in the operative part of the GDPR, as was already the case in the Data Protection Directive[225] . However, Recital 22, sentence 2 of the GDPR states that the existence of an establishment requires "the effective and actual exercise of an activity through a fixed establishment". This explanation is widely regarded as the relevant definition of an establishment for the purposes of Art. 3(1) GDPR.[226]

If the controller has several establishments, the allocation of data processing to an establishment depends on which body controls the data processing in question. The location of servers is irrelevant in this respect.[227] The legal status is irrelevant for the existence of an establishment. The term therefore covers subsidiaries and dependent branches alike.

---

225 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ (EC) L 281 of 23 November 1995, p. 31.

226 References in *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 3 para. 29.

227 *Däubler*, Das Kollisionsrecht des neuen Datenschutzes, p. 4, available at https://www.daeubler.de/wp-content/uploads/2020/11/1804Kollisionsrecht-Datenschutz.pdf (last accessed on 27 November 2025); *Pabst*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, 3rd edition 2024, Art. 3 GDPR para. 16.

b. The connection according to the market location principle (Art. 3(2) GDPR)

According to Art. 3(2) GDPR, the so-called market location principle, the GDPR is applicable if data of data subjects located in the Union is processed and the data processing serves the distribution of products (lit. a.) or the observation of their behaviour (lit. b.).

The first prerequisite is that the processing relates to data of data subjects who are in the Union.[228] In this respect, it is not the habitual residence that matters, but simply the place of residence.[229]

According to Art. 3(2)(a) GDPR, the GDPR is applicable if the data processing is related to the intention of the controller to offer goods or services to data subjects in the Union. This can be assumed, for example, in the case of data processing on websites that serve the purpose of distribution in the Union. According to Art. 3(2)(b) GDPR, the decisive factor is whether the data processing is related to the monitoring of the behaviour of data subjects in the Union. According to Recital 24 GDPR, this can be assumed to be the case, for example, with tracking or profiling.

c. The applicability of the GDPR in the case groups

According to the general principles, the following applies to the case groups mentioned at the beginning: If a branch in the EU is involved in data processing, Article 3(1) GDPR applies and the GDPR is applicable. In the case of the development of AI models, this applies, for example, if the training is carried out by a branch in the EU. According to the principles of the ECJ's Google Spain ruling, supporting activities are sufficient in this respect. If, for example, training data is provided by a branch in the EU, this is likely to lead to the application of the GDPR. The same applies to the provision of an AI model, the operation or use of the AI system. In the opinion of the ECJ, Art. 3 No. 1 GDPR is likely to be fulfilled if the activity in question is supported by a branch, for example if the distribution of models or AI systems or their operation is supported by a branch located in the EU.

---

228 In this context, the scope of application of Art. 3(2) GDPR is to be understood as complementary to Art. 3(1) GDPR in that paragraph 2 does not refer to the general absence of an establishment in the Union, but only to the absence of an establishment relevant within the meaning of paragraph 1; cf. *Piltz*, in: Gola/Heckmann, GDPR, BDSG, 3rd ed. 2022, Art. 3 para. 46 f.

229 *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 3 GDPR para. 74; *Hanloser*, in: Wolff/Brink/von Ungern-Sternberg, BeckOK-Datenschutzrecht, 53rd edition (as of 1 August 2025), Art. 3 GDPR para. 27; *Zerdick*, in: Ehmann/Selmayr, General Data Protection Regulation, 3rd edition 2024, Art. 3 GDPR para. 21.

If only establishments in Japan are involved, the GDPR is only applicable in accordance with Article 3(2) of the AI Regulation.

aa. The development of an AI model or AI system

The training of an AI model by an establishment in Japan does not lead to the application of the GDPR pursuant to Art. 3(2) GDPR, as the activity is not directed at the EU.[230] This also applies if personal data of EU citizens is used for training purposes.

The conditions under which the mere provision of an AI model or AI system is subject to the GDPR pursuant to Art. 3(2) GDPR has hardly been discussed to date. The question is particularly relevant for AI models and AI systems that are made available as such in a repository for use by third parties, for example on GitHub[231] or another platform[232] .

In this respect, a distinction must be made in several respects. First, provision in this sense must be distinguished from mere delivery to a platform. The decisive factor in this respect is who decides on the provision. If the developer himself decides which object is to be provided and under what conditions, he is also responsible for the process under data protection law.

Provision often involves the processing of personal data of persons who interact with the provider or operator of the platform in this context. The GDPR applies to this pursuant to Art. 3 (2) GDPR if the AI model or AI system is also to be distributed to entities in the EU and data of data subjects in the EU is processed in this context. However, this activity, which is no different from the distribution of other products, does not have any special features with regard to AI models or AI systems and will not be considered further below.

Of interest is whether the storage of personal data in an AI model is covered by the GDPR pursuant to Art. 3(2) GDPR if the model in question is to be distributed to entities in the EU. This crucial question is hardly ever discussed explicitly, but seems to be implicitly affirmed. However, this conclusion is questionable. Article 3(2)(a) GDPR requires that the processing be carried out in order to offer goods or

---

230 *Franke*, RDi 2023, 565, 566 (para. 7).

231 https://www.github.com (last accessed on 26 November 2025).

232 Examples of other software development platforms include Bitbucket at https://www.bitbucket.org, GitKraken at https://www.gitkraken.com, GitLab at https://www.gitlab.com and SourceForge at https://www.sourceforge.net (all last accessed on 26 November 2025).

services to "data subjects" in the EU. This provision undoubtedly covers the processing of data relating to the persons to whom the goods or services are to be distributed. The processing of data relating to other persons is therefore not covered.

It should also be noted that Art. 3(2)(a) GDPR, with its reference to distribution to "data subjects", covers only distribution to natural persons, but not to other entities. However, it would be illogical if the processing of data relating to other persons were only covered if it were carried out in relation to natural persons, but not in the case of distribution to other entities. This leads to the conclusion that the provision of an AI model or AI system is not subject to the GDPR simply because the AI model or the AI system based on it stores data from persons in the EU, even if the model or system is to be distributed to persons in the EU.

bb. The operation of an AI system

The applicability of the GDPR to the operation of an AI system by a branch of the responsible body in Japan pursuant to Art. 3(2) GDPR must be considered in a differentiated manner.

In principle, the GDPR does not apply to this activity, even if personal data of data subjects in the Union is processed. However, the GDPR applies pursuant to Art. 3(2)(a) GDPR if the AI system is operated to provide services to natural persons in the EU.

The applicability is unclear if services are provided exclusively to legal entities. If data of natural persons, such as employees of a company, is processed in this context, this is sufficient for the GDPR to apply. However, if this is excluded, Art. 3(2) GDPR does not apply in our opinion. However, it cannot be ruled out that data protection supervisory authorities may take a different view here if data of persons in the EU is processed. Ultimately, however, this question has no practical significance insofar as the GDPR is applicable to the use of the AI system in any case. This will often be the case when providing services for the European market.

cc. The use of an AI system

The use of an AI system by a controller located in the EU is subject to the GDPR with regard to the activities of that controller pursuant to Article 3(1) GDPR. The use then implies the applicability of the GDPR insofar as personal data of third parties is processed. In this case, if the AI system is operated by a branch located in Japan, there is also a transfer to Japan.

The operator of the AI system is involved in the processing. Several relevant processing activities take place: the receipt of the data, its temporary or permanent storage, its processing to generate an output, and finally the transfer of the output to the user.

According to Art. 3(2) GDPR, the GDPR is applicable in any case if, within the scope of this involvement in the data processing triggered by the user, data of natural persons on the user's side is processed, i.e. data of the user's employees or of the user themselves, if they are a natural person.

If this is excluded, the requirements of Art. 3(2) GDPR are not met in our opinion, even if data of other natural persons in the EU is processed. However, it cannot be ruled out that data protection supervisory authorities may take a different view here if data of persons in the EU is processed.

dd. Conclusion

The GDPR applies to data processing operations in connection with the provision, operation and use of AI models and AI systems, insofar as establishments in the EU are involved. Supporting activities are sufficient in this regard.

The development of AI models and AI systems by establishments in Japan is not subject to the GDPR, even if data of EU citizens is processed.

Insofar as the provision, operation and participation in the use of AI systems is carried out by establishments in Japam, the associated data processing operations are subject to the GDPR pursuant to Art. 3 (2) GDPR, insofar as data of natural persons from the EU is processed in connection with the distribution of AI models, AI systems or services based on them. Otherwise, it is highly unclear in which cases and under what conditions the data protection supervisory authorities assume the applicability of the GDPR.

4. Joint processing and commissioned processing when using AI systems

a. The principles of data protection responsibility

The determination of the responsible body, or controller for short, is of central importance in European data protection law. The controller is the addressee of the obligations under the GDPR and an essential point of reference for all key concepts of data protection law. For example, the justification for data processing must be

determined for the respective controller. In addition, according to the relevant concept of relative personal reference, even the personal reference of data, i.e. the existence of personal data, is determined from the perspective of the controller.

The term "controller" is defined in Art. 4 No. 7 GDPR. According to this, the controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

In this sense, the controller is the legal entity.[233] This is generally the respective legal entity, i.e. a natural or legal person or a company with legal capacity, but it can also be a legally dependent entity. It is unclear to what extent subdivisions of legal entities can themselves be controllers , such as a department or institution (e.g. works council[234]) of a company or authority, or individual branches.[235]

b. Joint responsibility and contract processing

Several entities are often involved in a data processing operation. This is particularly true when data processing is carried out using a technical service, as is the case with cloud computing, for example. The use of AI systems also often takes place by way of a service. This applies not only to services such as ChatGPT, but also to other AI systems. When several parties are involved in a uniform data processing operation, they can act as joint controllers or as clients and contractors in a contract processing operation.

Where several controllers work together, joint responsibility under Art. 26 GDPR regularly applies. The requirements for justifying data processing under joint responsibility are controversial in detail. According to the prevailing opinion, there must be a justification for the respective processing contribution of each of the joint controllers.[236] As an additional requirement, Article 26 GDPR requires that the joint

---

233 *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 4 GDPR margin note 74; *Gola*, in: Gola/Heckmann, GDPR, BDSG, 3rd edition 2022, Art. 4 GDPR marginal no. 63; *Hartung*, in: Kühling/Buchner, GDPR BDSG, 4th edition 2024, Art. 4 No. 7 GDPR marginal no. 9.

234 Now clarified by Section 79a sentence 2 BetrVG (employer as controller); see a brief summary of the discussion in *Hartung*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 4 No. 7 GDPR para. 11 f.

235 See *Hartung*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 4 No. 7 GDPR para. 9 ff.

236 *Bertermann*, in: Ehmann/Selmayr, General Data Protection Regulation, 3rd ed. 2024, Art. 26 para. 23; *Dovas*, ZD 2016, 512, 515; *Hartung*, in Kühling/Buchner, Art. 26 GDPR para. 62

controllers regulate their cooperation in an agreement and specify their respective obligations with regard to processing therein. The distinction between joint responsibility on the one hand and successive or parallel responsibility on the other is highly controversial[237] and will not be considered further here, as it is not relevant to the justification. The focus is rather on the possibility of justification under Article 6(1)(e) GDPR for the two main processing operations.

Data processing under data protection law enables data processing by one party for third parties. Its main area of application is the involvement of technical service providers, such as cloud service providers or data centres, in data processing.

Contract processing involves the controller and a processor who carries out the data processing on the controller's instructions. Several processors may also be involved in data processing, in which case a contractual relationship between the controller and the respective processor is required. The processor may, in turn, involve third parties by way of subcontracting (Art. 28(2), (4) GDPR). Sub-processors, as "other processors" (Art. 28(2), (4) GDPR), may also engage sub-processors.[238] Therefore, numerous sub-processors at several levels may be involved in contract processing.

Contract processing may justify the involvement of third parties in data processing by the controller. Can it justify this, or is it the result of justification? The dogmatic interpretation of these legal consequences is controversial.[239] According to the prevailing and convincing view, if the requirements for contract processing are met, the third party acting as the processor does not need any additional justification for its involvement in data processing, but can rely on the justification applicable to the controller.[240]

The requirements for contract processing are regulated in Art. 28 GDPR. According to this, contract processing must be based on a written (para. 9) contract with the content specified in Art. 28 para. 3 GDPR. Furthermore, the processor must comply with the data security requirements set out in Article 32 GDPR, and the controller must satisfy itself that this is the case (Article 28(1) GDPR). It is crucial that the

---

with further references; likewise, on the DS Directive, ECJ, judgment of 29 July 2019 -C-40/17 – Fashion ID, para. 96. A.A. *Martini*, in Paal/Pauly, Art. 26 GDPR para. 3a.

237 See, for example, *Borges*, in: Borges/Hilber, BeckOK-IT-Recht, 20th edition (as of 1 October 2025), Art. 26 GDPR, para. 17 et seq.

238 *Hartung*, in: Kühling/Buchner, DS-GVO BDSG, 4th edition 2024, Art. 28 GDPR, para. 85.

239 See an overview of this in *Hartung*, in: Kühling/Buchner, DS-GVO BDSG, 4th edition 2024, Art. 28 GDPR, para. 20 ff.

240 See *Hartung*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 28 GDPR para. 15 with further references.

processor's activities are carried out in accordance with the controller's instructions (see Article 28(3)(2)(a) GDPR). The controller's instructions to the processor may be given on an ad hoc basis in individual cases, but may also be set out conclusively in the underlying agreement. They may also be specified in the processor's general terms and conditions, which is common practice for technical services such as cloud computing.

c. Responsibility for the development and use of AI systems

With regard to data protection responsibility, a distinction must be made between the development of AI models and AI systems, their provision and their use.

If personal data is processed in the context of training an AI model, the entity responsible for the training is also the controller with regard to the associated processing.

When providing a trained model or an AI system to third parties, the entity that initiates the provision, i.e. transmits a model or makes it accessible via the internet, is responsible under data protection law for the associated storage and transmission of personal data.

When using an AI system, the entity responsible for its use is the controller, i.e. the entity that enters a prompt and receives the output or is responsible for the operation of a machine in which AI systems are integrated.

The question is what role is played by the entity that provides the technical basis, i.e. operates the AI system in question or influences its activity. As described above, providing the technical basis is a participation in data processing that is relevant under data protection law, as it involves deciding on the means of data processing. The entity that provides this basis is therefore also regularly a controller, unless it acts as a processor.

If another entity influences data processing, for example by transferring data from a machine, this entity is also regularly a controller or a processor. This is assumed, for example, in the case of the manufacturer of a self-driving car or a production machine if personal data is transmitted to the manufacturer during driving or production operations.

5. The justification for the processing of personal data

a. An overview of the grounds for justification

The general principles of justification are set out in Art. 6 GDPR. Art. 6(1)(a) to (f) lists several grounds for justification, which are equivalent and can in principle also coexist.[241]

These are consent (lit. a.), processing for the performance of a contractual obligation (lit. b.), processing for compliance with a legal obligation to which the controller is subject (lit. c.), processing to protect vital interests (lit. d.), processing to fulfil a public task (lit. e.), and processing to safeguard legitimate interests (lit. f.).

The processing of personal data is permissible under data protection law pursuant to Art. 6(1)(a) GDPR if the data subject consents to it. This requires prior, sufficiently clear information; in addition, consent must be voluntary (cf. Art. 4(11) GDPR).

Consent may also be deemed to be voluntary if the data subjects are in an employment relationship with the controller (cf. Recital 155 GDPR, Section 26(2) BDSG). In such cases, the existing relationship of dependency must be taken into account when assessing the voluntary nature of the consent. As a result, the supervisory authorities often deny that consent is voluntary. Above all, consent pursuant to Art. 7(3) sentence 1 GDPR can be revoked at any time. Therefore, consent cannot in any case lead to comprehensive justification and will therefore not be considered further.

Processing is permissible under Article 6(1)(b) GDPR if it is necessary for the performance of a contract to which the data subject is party. Processing is permissible under Article 6(1)(c) GDPR if it is necessary for compliance with a legal obligation to which the controller is subject. Such a legal obligation exists in particular in the case of a statutory obligation,[242] but not in the case of a contractual obligation.[243] Justification pursuant to Art. 6(1)(d) on the grounds of protecting the vital interests of the data subject is clearly not applicable. The processing of personal data is permissible pursuant to Art. 6(1)(e) GDPR if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Processing is permissible under Art. 6(1)(f) GDPR if the controller

---

241 *Buchner/Petri*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 6 GDPR para. 22.

242 *Buchner/Petri*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 6 GDPR para. 76; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 3rd ed. 2021, Art. 6 GDPR para. 16.

243 *Buchner/Petri*, in: Kühling/Buchner, DS-GVO BDSG, 4th ed. 2024, Art. 6 GDPR margin no. 77; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 3rd ed. 2021, Art. 6 GDPR margin no. 16.

or a third party has a legitimate interest in it and if there are no overriding interests of the data subject in protecting their personal data.

The planned Digital Omnibus Regulation will bring about a change in the legal situation in this respect. According to this, a new Article 88c is to be added to the GDPR. The provision reads as follows:

"Article 88c

Processing in the context of the development and operation of AI

Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'

The standard is based on the existing special rule for research under Art. 89 GDPR. On the one hand, it contains a modification of the interests within the framework of Art. 6(1) subpara. 1 lit. f GDPR, but on the other hand, it also contains additional requirements for the use of data for training and operating AI systems.

The draft appears to be unbalanced. The wording of draft Article 88c(2) GDPR is tailored to the needs of large providers and goes far beyond the intended objective. It does not differentiate between the requirements for additional safeguards according to the type and risk assessment of the AI model or AI system. An AI system used for machine control should be assessed differently in this respect than a generative AI system based on a large language model. Therefore, a proportionality clause that takes into account the differentiated level of protection should be explicitly added to avoid legal uncertainty.

The modification of the balancing of interests in draft Art. 88c(1) GDPR is significant insofar as the interests in the development and use of AI systems generally justify the processing, provided that the processing is necessary and does not outweigh the specific protection interests of the data subjects vis-à-vis the interest in using the AI system.

b. The justification for the processing of personal data in the development of AI models and AI systems

The processing of personal data when training an AI model can essentially be justified for the developer under Art. 6 para. 1 subpara. 1 lit. f GDPR.[244] Training an AI model for research purposes is a legitimate purpose, as is training an AI model for legal commercial purposes.[245] It is controversial whether restrictions arise from the aspect of necessity. This requires an examination of whether the legitimate interest in processing the data cannot be achieved in a reasonably effective manner by other means that interfere less with the fundamental rights and freedoms of the data subjects.[246] In this respect, some data protection supervisory authorities are of the opinion that there is no necessity if the processing of pseudonymised or synthetic data is reasonable.[247]

This, of course, raises the question of under what conditions such reasonableness can be assumed. So far, the discussion has been lost in vague hints. The demand for the pseudonymisation of data is rightly countered by the argument that changing data can have consequences for the quality of the model[248] that are difficult to assess reliably. The same applies to synthetic data[249] . Since the generation of synthetic data and the pseudonymisation of data involve considerable effort, the ques-

---

244 See *The State Commissioner for Data Protection and Freedom of Information Baden-Württemberg*, Discussion Paper: Legal Basis for Data Protection in the Use of Artificial Intelligence, Version 2.0 dated 17 October 2024, p. 21, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/10/Rechtsgrundlagen-KI-v2.0.pdf (last accessed on 28 November 2025); *Franke*, RDi 2023, 565, 567 (para. 10); *Paal*, ZfDR 2024, 129, 154; *Schwartmann/Benedikt/Köhler*, Expertenwissen KI und Datenschutz, 2025, p. 43 f.; *Werry*, MMR 2023, 911, 912 sees this as the "only possibility for lawful data processing" when training an AI model.

245 *The State Commissioner for Data Protection and Freedom of Information Baden-Württemberg*, Discussion Paper: Legal Basis for Data Protection in the Use of Artificial Intelligence, Version 2.0 of 17 October 2024, p. 21 f., available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/10/Rechtsgrundlagen-KI-v2.0.pdf (last accessed on 28 November 2025).

246 ECJ, judgment of 4 July 2023, C-252/21, para. 108, juris.

247 *The State Commissioner for Data Protection and Freedom of Information Baden-Württemberg*, Discussion Paper: Legal Basis for Data Protection in the Use of Artificial Intelligence, Version 2.0 of 17 October 2024, p. 22, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/10/Rechtsgrundlagen-KI-v2.0.pdf (last accessed on 28 November 2025).

248 See *Kaulartz/Matthiesen*, RDi 2025, 141, 144 (para. 19).

249 For a detailed assessment of the data protection implications of unsupervised machine learning with synthetic data, see *Raji*, DuD 2021, 303.

tion also arises as to whether this resolution is reasonable. In this respect, a distinction will have to be made according to the sensitivity of the data processing. In the case of everyday data, such as training based on data from public websites, the requirement to pseudonymise this data is probably unreasonable.

When training a limited amount of disease data, for example in medical research, a certain degree of pseudonymisation (removal of names) prior to use for training purposes will be reasonable, but not complete anonymisation. In any case, these measures are not reasonable if they restrict usability.

Conflicting interests of the data subjects are obvious insofar as there is a risk of a memorisation effect. Furthermore, there is also a conflicting interest of the data subjects insofar as data can be extracted from the model. From the perspective of the data subject, there is no significant difference in the result compared to a traditional data collection.

The interest in developing a model regularly outweighs the interests of the data subjects insofar as the data is otherwise publicly available, for example, can be extracted from the internet or social networks.

If the GDPR is amended, as planned in the Commission's draft Digital Omnibus Regulation, the legal basis will be simplified in part in favour of developers. According to draft Art. 88c subpara. 1 GDPR developers can generally assume that the processing is justified if the necessity of the data use can be demonstrated.

c. Justification for the processing of personal data when using AI systems

When using AI systems, the activities of those involved must be examined, including with regard to the justification for the processing of personal data.

The use of an AI system and thus also the associated processing of personal data originates from the user. This may be the user of software or a physical machine in which AI systems are integrated, or the user of an AI system who makes inputs, or the user of a service that uses one or more AI systems. For example, when a user enters a prompt in "ChatGPT" or a similar service, the user initiates the associated data processing and is therefore responsible for the associated transfer of data and, if applicable, further processing.

The justification must therefore be assessed from the user's point of view, insofar as the user is subject to the GDPR at all. A legal basis may arise for various reasons; in this respect, it is no different from the classic use of a search engine via the in-

ternet (e.g. Google). From the point of view of the service provider, the same questions arise here as with a search engine. As a result, the use will generally be justified.

When processing data for the control of machines, insofar as personal data is processed at all, a legal basis will typically exist in accordance with Art. 6(1)(f) GDPR.

The situation is different if the operator of the AI system uses data transmitted in the context of the use of a service, software or physical machine for other purposes, such as the further development of the system, the provision of a service to the user or for its own purposes, such as advertising or disclosure to third parties. A distinction must be made here. The further development of the system will regularly be classified as research or development activity.

Under current law, Art. 6(1)(f) or, where applicable, Art. 9 GDPR is particularly relevant; in future, Art. 88c GDPR-E will apply and justify the special processing. Processing for other, additional purposes may also be justified if the changes in purpose are appropriate in accordance with Article 6(4) GDPR. Use for advertising purposes or for data trading will typically not be justified.

Insofar as the activities of the operator of the AI system are carried out by way of order processing, the operator of the AI system may, as a contractor, rely on the purposes of the order placement.

6. Conclusion and recommendations for Japanese providers and deployers of AI models and AI systems.

The GDPR does not apply to the training of AI models in Japan. It is currently unclear whether and in which cases the GDPR applies to the provision of an AI model or an AI system in Japan. In any case, it does not apply if the provision is not also made for the EU market but is limited to markets in Japan or other countries outside the European Union. Providers of AI models and AI systems in Japan should therefore clarify whether distribution on the EU market is to take place and, if this is not the case, exclude it.

The operation of an AI system by Japanese entities may be subject to the GDPR. This applies not only if a branch in the Union is involved, but also if services are provided to persons in the Union. However, it is also unclear under what conditions the GDPR is applicable in this respect. In any case, it can be argued that the GDPR is not applicable if no personal data of users is processed.

Insofar as the GDPR is geographically applicable, it is often also materially applicable if personal data is processed when using the AI system. This will often be the

case if the system is used via a user account through which natural persons can be identified.

In this case, the operator of the AI system is – in addition to the user – the responsible body, unless it acts as a processor. It may therefore be advisable to agree on a processing contract.

The processing of personal data in the development of an AI system is often justified under Article 6(1)(f) GDPR. The same applies to data processing in the context of the use of AI systems. If the planned Article 88c will be inserted into the GDPR, the justification is to be assumed with greater legal certainty. In both cases, however, it is a prerequisite that the processing of personal data is limited to what is necessary for development or use and that the data is not used for other purposes.

As a result, the GDPR does not pose an obstacle to the development of AI models or AI systems in Japan. Nor does it pose an insurmountable obstacle to the provision of services using AI systems to European customers.

IV. Copyright challenges to Japanese providers and deployers of AI models and AI systems

Copyright issues relating to the development, provision and use of AI models and AI systems are of paramount importance and are the subject of intense debate worldwide.[250] The numerous copyright issues can be divided into three main areas[251] : the infringement of copyright and other intellectual property rights through the development and use of AI systems, the copyright protection of the products of AI systems, and the protection of AI models and AI systems.

In recent years, the international discussion has focused on the infringement of copyright and other intellectual property rights through the training of AI models and the use of AI systems. This set of issues is the focus of the following discussion, as it may give rise to significant challenges for the development, distribution and use of AI models and services in Europe.

In practical terms, a distinction must be made between three groups of processes: (1) the training of an AI model, (2) the (storage and) provision of an AI model or AI system to third parties, and (3) the generation of outputs by an AI system.

The current discussion on copyright infringements by AI models and AI systems (see 1. below) and the copyright framework in the European Union (see 2. below) are briefly outlined below. On this basis, the copyright aspects of training and providing AI models and AI systems (below 3.) and the use of AI systems (below 4.) are discussed. Finally, recommendations for action for Japanes providers and deployers are derived from the analysis (below 5.).

1. The current discussion on copyright infringement by AI models and AI systems

The question of whether and to what extent the development, provision and use of AI systems leads to copyright infringement is being discussed almost worldwide.[252]

---

[250] See overview articles on aspects of the protection of AI models and their output in Leistner/Jussen, "The Flattening of Creative Industries? A Closer Look at Copyright Protection of AI-Based Subject Matter," available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5080250; for an overview of the discussion on copyright infringements during training, see, for example, Leistner/Antoine, "TDM and AI training in the European Union – from 'LAION' to possible ways ahead?", GRUR Int 2025 (forthcoming), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5178237.

[251] See also Leistner, GRUR 2025, 1123 et seq.

[252] See excerpts from *Dornis*, KIR 2024, 156; *Käde*, ZUM 2024, 174; *Leistner*, GRUR 2025, 1123, 1124 ff.; *Petersenn/Kühn*, GRUR-Prax 2025, 615; *Sesing-Wagenpfeil*, ZGE 2024, 212; *The-*

In the USA, a large number of court cases are pending, with the first judgements published in 2025. According to a recent study, 57 copyright cases against AI companies were already pending by October 2025, the majority of them in the states of New York and California.[253] The first rulings were handed down in the cases of Thomson Reuters v. Ross Intelligence[254] , Andrea Bartz v. Anthropic PBC[255] and Kadrey v. Meta[256] .

The focus is on the question of the extent to which the established "fair use" doctrine is applicable to the training of AI models. According to the rule laid down in Section 107 of the U.S. Copyright Act, the question of whether the use of copyrighted material is justified must be determined by weighing the interests of the rights holders against those of the users on a case-by-case basis, using four non-exhaustive, defined factors. [257]

The first court rulings have also been handed down in the United Kingdom. On 4 November 2025, the High Court of England and Wales largely dismissed copyright infringement claims brought by the Getty Images photo agency against Stability AI, but upheld trademark claims.[258]

---

odoridis, NJW 2025, 689; on US law, see *Maffioli*, Copyright in Generative AI training: Balancing Fair Use through Standardisation and Transparency, 21 August 2023, available at: http://dx.doi.org/10.2139/ssrn.4579322 (last accessed: 21 November 2025); *Murray*, 26 SMU SCI. & TECH. L. REV. 259 (2023) Vol 26, 259; *Samuelson*, 71 UCLA L. Rev. 1484 (2024), 1484.

253 See Updated Map of US copyright suits v. AI (27 October 2025) Total = 57 suits, available at: https://chatgptiseatingtheworld.com/2025/10/27/updated-map-of-us-copyright-suits-v-ai-oct-27-2025-total-57-suits/ (last accessed: 21 November 2025).

254 *U.S. District Court for the District of Delaware,* Thomson Reuters v. Ross Intelligence, judgment of 11 February 2025 (No. 1:20-cv-613-SB), available at: https://www.ded.uscourts.gov/sites/ded/files/opinions/20-613_5.pdf (last accessed: 21 November 2025).

255 *U.S. District Court for the Northern District of California*, Andrea Bartz et al v. Anthropic PBC, Judgment of 23 June 2025 (No. C 24-05417 WHA), available at: https://docs.justia.com/cases/federal/district-courts/california/candce/3:2024cv05417/434709/231 (last accessed: 21 November 2025).

256 *U.S. District Court N.D. California*, Kadrey et al v. Meta Platforms, Inc., judgment of 25 June 2025 (No. 23-cv-03417-VC), available at: https://law.justia.com/cases/federal/district-courts/california/candce/3:2023cv03417/415175/598/ (last accessed: 21 November 2025).

257 *de la Durantaye*, GRUR 2025, 1550, 1551; *Reinholz*, RDi 2025, 497, 498 f.; *Samuelson*, 71 UCLA L. Rev. 1484 (2024), 1484, 1488 f.

258 See press coverage on this topic *Booth*, AI firm wins high court ruling after photo agency's copyright claim, available at: https://www.theguardian.com/media/2025/nov/04/stabilty-ai-high-court-getty-images-copyright (last accessed: 21 November 2025); *Krempel/Sokolov*, Copyright vs AI: London court does not help Getty Images photo agency, available at: https://www.heise.de/news/Copyright-vs-KI-Londoner-Gericht-hilft-Bildagentur-Getty-Images-nicht-11067223.html (last accessed: 21 November 2025).

The first ruling in an EU member state on the copyright assessment of AI training, as far as can be seen, was handed down in Germany by the Hamburg Regional Court[259] in the "Laion" case. Particular attention is paid to the ruling of the Munich Regional Court[260] in the legal dispute between GEMA, the German collecting society, and OpenAI, which commented on several copyright issues in connection with the training of AI models. At the heart of the legal dispute was the question of whether OpenAI's language models use copyright-protected song lyrics in an impermissible manner. GEMA asserted claims for injunctive relief, information and damages, basing these on the fact that OpenAI's models memorised various well-known German song lyrics and reproduced them almost word for word in response to simple user input. The court essentially followed this line of argument and upheld the vast majority of the claims asserted.

2. The copyright framework for AI systems and AI models (overview)

The legal framework for intellectual property (IP) rights consists of a historically developed, multi-layered system of international treaties, supranational regulations and national laws. At the international level, there are a number of international agreements, most of which are administered or influenced by the World Intellectual Property Organisation (WIPO) and the World Trade Organisation (WTO).

The main historical foundations of intellectual property law at the international level are the Paris Convention for the Protection of Industrial Property of 1883, which contains basic regulations for patents, trademarks and designs, and the Berne Convention for the Protection of Literary and Artistic Works of 1886, which lays down the central principles of copyright law. The most important international agreement at present is the TRIPS Agreement (Trade-Related Aspects of Intellectual Property Rights) concluded within the framework of the WTO, which harmonises minimum standards for almost all areas of IP law.

The European Union has a number of directives that harmonise copyright and other intellectual property rights. In the field of copyright, the 2001 InfoSoc Directive[261] and the 2019 DSM Directive[262] are of central importance. The InfoSoc Directive is

---

259 *Hamburg Regional Court*, judgment of 27 September 2024 – 310 O 227/23.

260 *Munich Regional Court I*, final judgment of 11 November 2025 – 42 O 14139/24.

261 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10

262 Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market, OJ L 130, 17.5.2019, p. 92.

the central basis of EU-wide copyright law. It regulates the concept of a work as an object of copyright protection, the concept of the author as the owner of copyright, the central rights of the author, and so-called limitations that legitimise/justify the use of works. The central rights of the author include the exclusive right to exploit the work. The InfoSoc Directive regulates, among other things, the right of reproduction, which also covers temporary storage, for example in the working memory of a computer, and the right of communication to the public as the two most important exploitation rights of the author. The DSM Directive introduces new legal limitations, namely the so-called text and data mining limitation, as well as limitations for the exploitation of works in the field of education and preservation. With regard to the development of AI models, the data mining limitation is of central importance (see 5.b below).

The 2009 Software Directive[263] applies to computer programmes. It also applies to AI systems within the meaning of the AI Regulation, as these are computer programmes within the meaning of the Software Directive. It does not apply to AI models within the meaning of the AI Regulation, as AI models are not executable and therefore do not constitute computer programs within the meaning of the Software Directive. AI models are therefore subject to the general rules of the InfoSoc Directive.

The European directives have been implemented differently in the EU Member States. In Germany, all three directives mentioned above have been integrated into the German Copyright Act (UrhG).

3. The applicability of EU Member States' copyright law to Japanese providers and deployers of AI systems

From the perspective of Japanese providers of AI models and providers and operators of AI systems, the question ais of crucial importance under what conditions the copyright law of EU member states applies to the development and use of AI systems in Japan. Therefore, the rules of conflict of laws for intellectual property rights in EU member states are briefly outlined below (see a) below), followed by an explanation of the territorial applicability of member state copyright law to the development and use of AI models and AI systems in Japan (see b) below).

---

263 Directive 2009/24/EC on the legal protection of computer programs, OJ L 111, 5.5.2009, p. 16.

a. The regulation of conflict of laws in intellectual property law in the European Union

Conflict of laws in intellectual property law is based on the principle of territoriality.[264] According to this principle, the effects of intellectual property rights are limited to the territory of the state under whose rules they arise.[265] As a consequence of this principle, a specific object, such as a work, is protected in different states according to the law applicable there.[266] The right holder therefore typically receives a bundle of property rights that are often similar in content but legally separate.[267] The conflict-of-law manifestation of these principles of territorial limitation of intellectual property rights is referred to as the country of protection principle.[268] This principle is uniformly prescribed for all EU Member States with regard to claims arising from the infringement of intellectual property rights in the Rome II Regulation, the European Regulation on conflict of laws in tort law. According to Art. 8(1) of the Rome II Regulation, non-contractual claims arising from their infringement are governed by the law of the country whose protection is claimed. This means that claims, such as for injunctive relief or damages, are governed by the law of the country in which the infringed right exists.

With regard to the infringement of rights to AI models or AI systems, this means that the infringement of any rights in the European Union is governed by the various legal systems of the European Member States.

The intellectual property law of the respective country is applicable if the infringement occurs in that country. In the case of infringements of intellectual property rights by content on the internet, it is difficult to localise the infringement. In this respect, national copyright law is applicable under two conditions: firstly, access from the country in question must be technically possible, and secondly, the offer of access must be directed at the Member State in question.

b. The application of national copyright law to AI models and AI systems

As just explained, the applicability of the national copyright law of EU Member States to Japanese AI models and AI systems s is based on the so-called country of

---

264 *McGuire*, in: BeckOGK, as of 1 July 2023, Art. 8 Rome II Regulation, paras. 27, 34.

265 *McGuire*, in: BeckOGK, as of 1 July 2023, Art. 8 Rome II Regulation, para. 27.

266 See *McGuire*, in: BeckOGK, as of 1 July 2023, Art. 8 Rome II Regulation, para. 27.

267 See *McGuire*, in: BeckOGK, as of 1 July 2023, Art. 8 Rome II Regulation, paras. 27, 35.

268 *McGuire*, in: BeckOGK, as of 01.07.2023, Art. 8 Rome II Regulation, para. 36.

protection principle, which is laid down in Article 8 of the Rome II Regulation. Therefore, insofar as claims arising from copyright infringement by AI models or AI systems are asserted, the existence and scope of any claims pursuant to Article 8 of the Rome II Regulation are governed by the law of the Member State under whose law copyright protection of the object in question is claimed. Claims can therefore be asserted under the law of any Member State in accordance with that law.

The prerequisite is that the infringement in question takes place in the respective Member State. In this respect, a distinction must be made between the individual infringements that may be considered. As outlined above, the training of an AI model, the provision of an AI model or an AI system to third parties, and the use of the AI system are of particular interest here.

With regard to the training of an AI model, a relevant copyright-related act of use is the storage of data in the training data corpus, which is a copyright-relevant act of use.[269] Another relevant act of use is the training itself, as this involves short-term storage in any case.

The localisation of these acts of use is controversial. In some cases, the location of the server on which the training data is collected and curated is used as a basis.[270] According to the opposing view, these acts are to be located where the act was performed to start the training.[271] This is the seat of AI development.[272] The opposing view is to be agreed with. The location of the server is often unknown[273] and has no substantive connection to the training, so it is rather random in terms of the use of the model and can also change easily when data is transferred from one server to another.

This means that German intellectual property law (in line with the law of other EU Member States) is only applicable if the training is carried out by developers based in Germany. With regard to the "registered office" in this sense, various connections are conceivable, in particular the so-called statutory registered office, i.e. the registered office of the developer as defined in the articles of association, as well as the

---

269 *Stieper/Denga*, GRUR 2024, 1473, 1477.

270 *Baumann*, NJW 2023, 3673, 3675 f.

271 *Dregelies*, GRUR 2024, 1484, 1488.

272 *Dregelies*, GRUR 2024, 1484, 1488; *Schack*, NJW 2024, 113, 115.

273 *Dregelies*, GRUR 2024, 1484, 1488; *Schack*, NJW 2024, 113, 115; likewise *Beurskens*, RDi 2025, 1, 4.

place of business where the developer's business activities are carried out. Irrespective of this, training in Japan is not covered by the author of the European standards.

The link to the provision of an AI model or an AI system is particularly controversial. The discussion focuses on provision via the internet. From the perspective of EU copyright law, the provision of protected content via the internet constitutes a communication to the public within the meaning of Article 3 of the InfoSoc Directive or, in the case of AI systems, within the meaning of the Software Directive. Under German copyright law, the provision of AI models or AI systems via the internet constitutes making available to the public within the meaning of Sections 15(2)(2) and 19a of the German Copyright Act (UrhG). [274]

So far, there has been little discussion as to whether provision on the internet is always global, i.e. in every EU Member State. In any case, technical accessibility from the relevant country will be necessary. If access from a particular country is made significantly more difficult by technical access barriers, there can be no question of public communication in that country.

Of particular interest is whether technical accessibility is sufficient, or whether it is also necessary for the provision of the AI model or AI system to address the market of the Member State concerned. This question has hardly been discussed to date. Court proceedings and discussions in the literature refer to the provision of AI systems for use, namely generative AI works such as ChatGPT. In the author's opinion, in addition to technical accessibility, it is also necessary that the market of the country concerned is addressed. This is the case when AI models or AI systems are offered worldwide, especially in English or one of the languages of the European Member States, but not, in our opinion, when the model or system is recognisably offered exclusively to users outside the EU.

The discussion focuses on the provision of an AI system by its operator for use by third parties, as is particularly the case with services such as ChatGPT, Google Search, etc.

According to the prevailing view in German literature, enabling access to an AI system establishes a sufficient territorial connection under two conditions: first, access must be technically possible from the Member State in question, and second, the offer of use must be directed at the market of the Member State in question. [275]

---

274 *Dornis*, CR 2024, 830, 835; *Dornis/Stober*, Copyright and Training Generative AI Models, 2024, p. 164.

275 *Dornis/Stober*, Copyright and Training Generative AI Models, 2024, p. 165.

The discussion is often intertwined with the substantive legal question of whether and to what extent providing access to an AI system constitutes an act of copyright use at all (see below). Some argue that the mere offering of an AI model does not in itself affect copyright exploitation rights and that there is no domestic act of exploitation.[276] However, this question must be strictly separated from the conflict of laws issue at hand here, since the existence of copyright use only arises from the applicable national copyright law.

It should therefore be noted that German copyright law applies to the provision of an AI system for use if such use is technically possible from Germany and, according to the prevailing opinion represented here, the offer of use is recognisably aimed at the German market.

This group of cases is at the forefront in practice, as the provision for use can be easily demonstrated and proven and has the greatest economic significance compared to the specific use by individual users. Nevertheless, the connection must be considered separately for each group of cases.

With regard to the use of an AI system, a distinction must be made between the actions of the user and the involvement of the operator of the AI system. The actions of the user will probably be localised where the user is actually located when entering and retrieving content. For example, if users from Germany use a service such as ChatGPT, they are subject to German copyright law in this respect.

The involvement of the operator of the AI system offering the use in this use is only subject to the copyright law of the country concerned, in this example German copyright law, if it also has a sufficient territorial connection. In this respect, the provision for use must be taken into account, i.e., in accordance with the above, whether the operator of the AI system addresses the relevant market with its offer of use, i.e., specifically offers users from the relevant country.

4. Infringement of copyrights through training of AI models

a. Actions relevant to copyright

When training AI models and AI systems, actions relevant to copyright law can arise in several respects. First of all, when the corpus of training data is created, the content is stored in any case. This constitutes a reproduction relevant to copyright

---

276 *Stieper/Denga*, GRUR 2024, 1473, 1477.; *Schmid*, KIR 2025, 69, 72.

law within the meaning of the InfoSoc Directive. Under German law, this constitutes reproduction within the meaning of Sections 15 and 16 of the German Copyright Act (UrhG). The training itself also involves the temporary storage of training data, which also constitutes reproduction relevant to copyright law within the meaning of the Directive or, under German law, Section 16 of the UrhG.

Of particular importance is the question of whether the trained AI model contains a reproduction of protected content. This question, which is at the heart of the global debate, is highly controversial. In German literature, reproduction is widely rejected, but the voices assuming reproduction now predominate. Opinions are also divided in German case law. The Hamburg Regional Court, albeit in an obiter dictum. The ruling of the Munich Regional Court of is therefore of particular importance.

The assumption that an AI model stores all content that it can reproduce is only convincing to a limited extent. Since content cannot be perceived without being output, it would be appropriate to focus on the generation of such output. However, given the trend in the discussion, it can be assumed that the discussion will move towards viewing the trained model itself as a reproduction of the retrievable content. This practice must therefore be adapted to this assessment.

b. Justification

All copyright restrictions apply to the justification of individual actions. However, the discussion focuses on the so-called TDM restriction in Articles 3 and 4 of the DSM Directive, which was implemented in Germany in Section 44b of the Copyright Act (UrhG).

Article 4 of the DSM Directive reads as follows:

Article 4

Exception or limitation for text and data mining

1. Member States shall provide for an exception or limitation to the rights provided for in Article 5(a) and Article 7(1) of Directive 96/9/EC, Article 2 of Directive 2001/29/EC, Article 4(1)(a) and (b) of Directive 2009/24/EC and Article 15(1) of this Directive for reproductions and extractions of lawfully accessible works and other subject matter for the purposes of text and data mining.

2. Reproductions and extractions made pursuant to paragraph 1 may be retained for as long as is necessary for the purposes of text and data mining.

3. The exception or limitation provided for in paragraph 1 shall apply on condition that the use of works and other subject matter referred to in that paragraph has not been expressly reserved by their rightholders in an appropriate manner, such as machine-readable means in the case of content made publicly available online.

4. This Article shall not affect the application of Article 3 of this Directive.

It is highly controversial whether and to which of the relevant acts the TDM exception applies. The discussion is, in some cases, not particularly precise with regard to the reference point of the exception.

From a practical point of view, the most important question is whether the storage of content in a trained model is covered by the TDM exception. Some of the literature affirms this. However, the now prevailing view in the literature rejects this.

The Munich Regional Court has concurred with this view.

In the author's opinion, the training and the mere storage of the trained model, which is necessary as part of the training, must be distinguished from the storage in the context of making the trained model available to third parties. In our opinion, the storage of data for its own purposes, i.e. during training and to back up the training content, is covered by the TDM limitation, even if machine learning was probably not on the minds of the historical legislators.

The storage of a trained model or AI model on a server in order to use it or pass it on to third parties is obviously not training and equally obviously not storage for the purpose of obtaining knowledge or results. Therefore, with regard to this reproduction process, the question arises as to whether the TDM barrier also justifies the subsequent storage of results that are identical to the content used for the analysis, i.e. that constitute a reproduction of the source material. This is clearly not the case, so that in any event the outputs of an AI system cannot be covered by the TDM barrier.

If, contrary to the view preferred here, the model is seen as a reproduction of the works used for training, it is clear that this process is in a sense intermediate between the two, since, from a technical point of view, there is no distinction between storage for training purposes and subsequent storage for use or distribution. However, it is perfectly possible to proceed on the basis of the purposes of storage and to differentiate with regard to the views of the TDM exception. The TDM exception aims to protect the acquisition of knowledge that is the resource of the researcher. This suggests that the provision of source material in a trained AI model should be treated in the same way as other forms of storage in which, if one wishes to argue technically, storage takes place in loading states that are only reassembled into perceptible content on the basis of an application.

This is countered by the fact that the developer of the AI model cannot directly influence which content is reassembled in its original form. In this respect, storage is completely different from other forms of content storage on a hard drive or other

external data carriers. Therefore, there are better reasons to consider the "storage" of content in a model as such to be covered by the TDM exception.

Practitioners must, of course, be prepared for the fact that the courts, such as the Munich Regional Court recently, will in any case deny the application of the TDM exception with regard to the storage of content.

The justification for the public communication within the meaning of Article 3 of the Infosoc Directive, or in German law, the making available to the public within the meaning of Section 19a of the German Copyright Act (UrhG), in the provision of an AI model or AI system via the internet is governed by the general limitations.

The TDM exception does not apply in this respect. The provision of the use of an AI system as a service, which also qualifies as public communication of the protected content, cannot be covered by the TDM exception either.

5. Copyright aspects of the use of AI systems

a. Actions relevant to copyright

When using AI systems, protected content may be output by the AI system. This may constitute the reproduction of a work. This is the case if the output content represents a reproduction of the corresponding work from the perspective of an outside third party who perceives the output. Generative AI systems such as ChatGPT often output protected texts, sounds and images verbatim. This constitutes a reproduction of the work in question.

The crucial question is who is to be regarded as the perpetrator of these acts of reproduction. German copyright law distinguishes between the direct perpetrator and the indirect perpetrator, who is often also referred to as the interferer. European directives also make this distinction. According to these directives, the direct perpetrator is the person who directly carries out the relevant infringing act. The indirect perpetrator is anyone who makes a relevant causal contribution to this act of use that is relevant under copyright law.

It is undisputed that the user who retrieves the content is to be regarded as the perpetrator as the direct initiator of this reproduction. However, it is questionable how the involvement of the operator of the AI system should be classified. The Munich Regional Court classified the operator of the AI system as the perpetrator, not merely as an indirect perpetrator or interferer.

In any case, the provider of the AI system or the underlying AI model is not the direct perpetrator with regard to copyright infringements caused by the output of an AI system.

The question of whether and, if so, under what conditions they can be held liable as an indirect perpetrator or interferer has apparently not been discussed as such to date. This question is likely to remain open for the time being.

According to the general principles governing the liability of indirect perpetrators for copyright infringements by third parties, which have been developed in German law particularly in connection with the provision of internet access to third parties, indirect perpetrators are only liable if they fail to take reasonable measures to prevent copyright infringements. Such reasonable measures may include filtering measures, insofar as these can be provided by the provider. However, the question of the scope of such security mechanisms on the part of the provider remains completely unresolved.

b. Justification

The general rules apply to the justification of interventions in the use of AI systems. The TDM limitation does not apply in this respect.

The reproduction of a work by the user of the AI system may be covered by a variety of limitations. In particular, reproduction for private purposes (Art. 5(2)(b) , for research or teaching (Art. 5(3)(a) InfoSoc Directive) or for other privileged purposes (Art. 5 InfoSoc Directive) may be considered. This also means that reproduction in the context of a business activity is generally not justified and infringes the rights of the author.

With regard to the involvement of the operator of the AI system, the decisive factor is whether the operator can invoke the justification of the user's action. This is generally the case. In this respect, the situation cannot be any different from the provision of other technical aids.

However, it is questionable whether the involvement should be assessed independently of the justification of the user's behaviour. This is linked to the question of whether the operator is regarded as the direct or indirect perpetrator of the infringing act. In the case of direct perpetration, the use requires justification in accordance with the applicable limitations. This will not normally be the case if the user's action is not justified . In the case of indirect perpetration, however, it should be sufficient for the party involved to take adequate precautions to prevent copyright infringements. This can be achieved in particular through filtering measures,

such as those implemented by the operators of large services, for example by OpenAI as the provider of ChatGPT.

Insofar as the provider of an AI system is considered an indirect perpetrator due to its causal contribution to the output of copyright-protected content, the question arises as to the justification of a causal contribution. In this respect, the provider can invoke any justifications for the direct action of the user.

6. Legal consequences of any copyright infringements

The legal consequences of any copyright infringements are governed by the national copyright law from which the infringement arises. In this respect, European directives require strict legal consequences, in particular sanctions (Art. 8(1) InfoSoC Directive) and legal remedies for rights holders (Art. 8(2) InfoSoC Directive). Under German law, the perpetrator of a copyright infringement is liable for the removal of the infringement (Section 97 (1) UrhG), for the cessation of future infringements (Section 97 (1) UrhG), and for damages (Section 97 (2) UrhG). A number of other legal consequences may apply, such as a claim for the destruction of an illegal product (Section 98 UrhG). In addition, criminal liability may apply (Sections 106 et seq. UrhG) and fines may be imposed (Section 111a UrhG).

7. Conclusion and recommendations for Japanese providers and deployers

This brief analysis shows that Japanese providers of AI models and AI systems and their operators face considerable copyright risks if these are trained with protected material or if an AI system outputs protected content.

From the perspective of Japanese providers and operators, the first consideration is whether the applicability of copyright law by EU member states can be avoided.

The training of AI models in Japan is not subject to the copyright laws of EU member states. However, making AI models available on the internet may already trigger the applicability of European copyright laws. This applies in any case if an AI model is distributed to customers in European member states. It is unclear whether mere accessibility is sufficient, but this cannot be completely ruled out.

Insofar as the use of an AI system is made available for the EU market, European copyright law also applies. In this case, the operator of the AI system must comply with European copyright law.

As an immediate recommendation for action, Japanese providers and operators of AI systems should only distribute AI models, AI systems or provide AI solutions

for use by customers in the European Union in compliance with copyright requirements in order to avoid liability. Depending on the type of AI system and its use, the consequences of liability can be significant.

V. Liability for AI systems and AI models exported to the European Union

1. Overview of the European legal framework for liability

Liability on the part of providers of AI models and providers, operators and users of AI systems may arise from various legal norms. A distinction must be made between contractual liability, which generally only applies in the relationship between contracting parties, and tortious liability, which can arise in relation to anyone who suffers damage as a result of an AI system. The following analysis is limited to tortious liability.

a. The discussion on liability for AI systems

There is no specific European liability regime for AI systems and AI models. Responsibility and liability for AI systems have been the subject of intense debate in Europe for around 10 years.[277] With its resolution of February 2017[278] , in which numerous fundamental questions were raised, including the creation of an "e-person", the EU Parliament gave the starting signal for a legal policy discussion that attracted global attention but was unjustly reduced to the question of legal capacity for robots.

In its 2018 strategy "Artificial Intelligence for Europe", the EU Commission already explicitly focused on ethical and legal issues in addition to the technical and economic aspects.[279] The EU Commission established several expert groups to support

---

277 See, for example*, Borges,* CR 2016, 272 ff.; *idem*, in: Borges/Sorge, Law and Technology in a Global Digital Society, 2022, p. 51 ff.; *European Parliament*, European Parliament resolution of 16 February 2017 with recommendations to the Commission on civil law rules on robotics (2015/2103(INL)) C 252/249 ff. (in preparation: *EP*, Civil law rules in the field of robotics)), available at: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017IP0051 (last accessed: 19 November 2025); *Oechsler*, NJW 2022, 2713 (2174 ff.); *Sommer*, Liability for autonomous systems, 2020, p. 50 ff.; *Thöne*, Autonomous Systems and Tort Liability, 2020, p. 157 ff.; *Wagner,* AcP 217 (2017), 707 (708 ff.); *Zech,* in: Proceedings of the 73rd German Lawyers' Day Volume I 2020/2022, p. A.1-A 112.

278 Fn. 1.

279 *European Commission*, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, AI for Europe, COM(2018) 237 final, p. 3 f, available at: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018DC0237 (last accessed: 17 November 2025).

the commission in these tasks. In the field of ethical aspects of AI, the High- -Level Expert Group on AI[280] developed ethical guidelines for trustworthy AI, which were published in June 2018.[281] Regarding the regulation on liability and security, the Expert Group on Liability and New Technologies, consisting of a Product Liability Directive formation and a "New Technologies" formation, was established.[282]

In October 2020, the European Parliament published a resolution on liability for AI systems which, clearly inspired by the Expert Group's report, even contains a complete draft regulation on liability for the operation of AI systems with far-reaching reform proposals.[283] However, the European Commission did not respond to this. Instead, it presented the draft AI Regulation in April 2021.[284] However, the AI Regulation does not contain any rules on liability for AI systems, as these are to be reserved for a separate legal act.

On 28 September 2022, the European Commission published two proposals relevant to liability for AI systems: a draft directive on liability for AI systems[285] and a draft revised product liability directive[286] .

---

280 For more information on the High-Level Expert Group on Artificial Intelligence, see: https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai (last accessed: 17 November 2025).

281 *High Level Expert Group on Artificial Intelligence*, Ethical Guidelines for Trustworthy AI, 2019, available at: https://op.europa.eu/de/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1 (last accessed: 17 November 2025).

282 For further information, see: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3592 (last accessed: 17 November 2025).

283 *European Parliament*, Regulation of civil liability in the use of artificial intelligence – European Parliament resolution of 20 October 2020 with recommendations to the Commission on the regulation of civil liability in the use of artificial intelligence (hereinafter referred to as *EP*, Resolution on the regulation of civil liability in AI) (2020/2014(INL)), available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_DE.pdf (last accessed: 17 November 2025).

284 *European Commission*, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legal acts of 21 April 2021, COM(2021) 206 final, available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A52021PC0206 (last accessed: 17 November 2025).

285 *European Commission,* Proposal for a Directive of the European Parliament and of the Council on adapting the rules on non-contractual civil liability to artificial intelligence (AI Liability Directive) of 28 September 2022, COM(2022) 496 final, available at: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022PC0496&from=DE (last accessed: 17 November 2025).

286 *European Commission,* Proposal for a Directive of the European Parliament and of the Council on liability for defective products of 28 September 2022, COM(2022) 495 final, available at:

In November 2024, a new Product Liability Directive (see 2.b. below) was adopted. This is intended to adapt product liability law to technical progress, not least to the special features of artificial intelligence.[287]

The legislative process for the proposed directive on liability for AI systems was not completed during the last legislative period of the European Parliament and has not been taken up again since the new European Parliament was elected. It is therefore unlikely that such a specific European liability regulation will be enacted in the near future.

b. Special features of AI systems and tortious liability

The special features of AI systems pose challenges for current liability law. AI systems have special features that are relevant to liability law. AI systems are often attributed with "autonomy"[288] or the ability to "behave"[289] . This refers to the fact that the actions of the system are not specifically predetermined by humans.[290] The behaviour, i.e. the actions of the system, is sometimes only a reaction to a perceived situation.[291] For example, the highly automated, self-driving car (based on commands from the integrated AI systems) behaves in road traffic depending on the

---

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022PC0495&qid=1666017366383&from=DE (last accessed: 17 November 2025).

287 *European Commission*, Proposal for a Directive of the European Parliament and of the Council on liability for defective products of 28 September 2022, COM (2022) 495 final, Section 1.3.

288 For a detailed discussion of the concept of autonomy in relation to systems, see *Reed/Kennedy/Silva*, Queen Mary University of London Legal Studies Research Paper No. 243/2016, p. 4 ("black box systems"); *Schulz*, Responsibility in Autonomously Operating Systems, 2015, p. 43 ff.; for a distinction between different levels of autonomy depending on the extent to which humans are involved in machine decision-making, see *Reichwald/Pfisterer*, CR 2016, 208 (210 f).

289 *Brunotte*, CR 2017, 583 (585); *European Commission*, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, AI for Europe, COM(2018) 237 final, p. 1; *High-Level Expert Group on Artificial Intelligence*, Defining AI: Key Capabilities and Scientific Fields, 2019, p. 1, available at: https://elektro.at/wp-content/uploads/2019/10/EU_Definition-KI.pdf (last accessed: 20 November 2025); *Lorse*, NVwZ 2021, 1657 (1658); *Sommer*, Liability for Autonomous Systems, 2020, p. 34 et seq.; *Sosnitza*, CR 2016, 764 (765).

290 *Borges*, NJW 2018, 977 (978); *Dettling/Krüger*, MMR 2019, 211 (212); *Thöne*, Autonomous Systems and Tort Liability, 2020, p. 6 ("Emancipation of the machine from humans").

291 *Ballestrem/Bär/Gausling/Hack/von Oelffen*, Artificial Intelligence, 2020, p. 1; *Borges*, CR 553 (561); *Geminn*, ZD 2021, 354 (354 f.); *Linke*, MMR 2021, 200 (201); *Sommer*, Liability for Autonomous Systems, 2020, p. 37; *Stiemerling*, in: Kaulartz/Braegelmann, Legal Handbook on Artificial Intelligence and Machine Learning, 2020, p. 27; *Thöne*, Autonomous Systems and Tort Liability, 2020, p. 6 ff.

traffic situation[292] , and the chatbot generates a response depending on the question and its context.[293]

Another special feature of AI systems, sometimes referred to as "opacity", concerns the limited ability to understand and comprehend how the AI system works. An essential aspect of this property concerns the so-called "black box" effect[294] of machine learning.

aa. Gaps in fault-based liability

These special features of AI systems have a significant impact on liability law. The autonomy of machines designed with AI is probably most significant in relation to the requirement of fault. Both contractual liability and traditional tortious liability are based on fault as a central prerequisite for liability. However, this refers to human fault.[295] However, insofar as a machine acts autonomously, the execution of this mechanical "action" cannot be regarded as human behaviour,[296] which could be the subject of an accusation of fault.

Consequently, there is no fault in this respect. At most, human fault may be attributed to the activation of the machine as such or to a lack of supervision. However, as long as a machine is used permissibly and operates within its autonomous

---

292 On the different degrees of automation in self-driving cars*, see,* for example*, Betz,* in: Oppermann/Buck-Heeb, Autonomous Driving, 3rd ed. 2024, chap. 1.1 para. 26 ff.; *Lange*, NZV 2017, 345 (346); *Roshan*, NJW-Spezial 2021, 137 (137).

293 Particular attention was paid to the chatbot "ChatGPT" published in November 2022 by the start-up OpenAI, see, for example, *Lobo*, Das Ende der irrelevanten künstlichen Intelligenz (The End of Irrelevant Artificial Intelligence), as of 7 December 2022, available at: https://www.spiegel.de/netzwelt/web/chatgpt-markiert-das-ende-der-irrelevanten-kuenstlichen-intelligenz-kolumne-a-b2afeb69-083d-4e69-8920-da5cad549d5f (last accessed: 17 November 2025); *Mehlan*, MMR-Aktuell 2022, 454722; *Weßels*, ChatGPT – a milestone in AI development, as of 20 December 2022, available at: https://www.forschung-und-lehre.de/lehre/chatgpt-ein-meilenstein-der-ki-entwicklung-5271?utm (last accessed: 18 November 2025).

294 *High-Level Expert Group on Artificial Intelligence*, A Definition of AI: Key Capabilities and Scientific Fields, 2019, p. 6; *Lauscher/Legner*, ZfDR 2022, 367 (375); *Thöne*, Autonomous Systems and Tort Liability, 2020, p. 9; *Zech*, in: Lohsse/Schulze/Staudenmayer, Liability for Artificial Intelligence and the Internet of Things, 2019, p. 187 (190, 192).

295 BGH, judgment of 12 February 1963 – VI ZR 70/62, NJW 1963, 953 (953); OLG Hamm, judgment of 15 September 2009 – 9 U 230/08, NJW-RR 2010, 450 (450); *Wagner,* in: Säcker/Rixecker/Oetker/Limperg/Schubert, Münchener Kommentar zum BGB, vol. 7, 9th ed. 2024, section 823 BGB marginal no. 66.

296 *Borges,* NJW 2018, 977 (978); *ibid.*, CR 2022, 553 (553); *Riehm,* RDi 2020, 42 (43); *Samuelson,* 47 U. Pitt. L. Rev 1985-1986, 1185 (1192 ff.).

range without a human being having to be able to intervene in the event of a malfunction, there is no human fault that could trigger fault-based liability.

Once again, highly automated driving provides an intuitive example: insofar as the driver is permitted to leave the control of the vehicle to the vehicle and turn his attention away from the traffic, he cannot be blamed for any fault if the vehicle causes an accident.

In this area of autonomy of the machine, liability on the part of the user or operator of the machine is therefore excluded under Section 823(1) of the German Civil Code (BGB), as is liability for violation of protective laws under Section 823(2) BGB, since this also presupposes fault.

With regard to liability for breach of a duty of supervision, there are no fundamental dogmatic peculiarities, but it is largely unclear what requirements exist in this respect.

bb. Liability for fault of the AI system ("vicarious liability")

The possible solution proposed by the European Parliament in 2017, namely to designate the machine itself as the liable party in the sense of a legal entity or even an "electronic person" ([297]), has met with strong opposition ([298]) and plays no role in the current legal policy discussion.

De lege lata, various models of attribution based on the model of vicarious liability are being discussed. Unlike German contract law (§ 278 BGB), German tort law does not include liability based on the attribution of fault to the machine, however that fault may be determined, known as vicarious liability. For this reason, some advocate the analogous application of § 278 BGB to AI systems.[299] According to Section 278 BGB, the principal is liable for the fault of the persons he employs to fulfil a contractual obligation. In addition, an analogous application of Section 831

---

297 *EP*, Civil law provisions in the field of robotics, C 252/250.

298 Expert *Group on Liability and New Technologies – New Technologies Formation*, Liability for Artificial Intelligence and Other Emerging Digital Technologies, 2019, p. 38, available at: https://op.europa.eu/de/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en# (last accessed: 17 November 2025); *Denga*, CR 2018, 69 (77); *Linke*, MMR 2021, 200 (202 f.); *Mayinger*, Die künstliche Person, 2017, p. 166 ff.; *Riehm*, RDi 2020, 42; *Wagner*, in: Säcker/Rixecker/Oetker/Limperg/Schubert, Münchener Kommentar zum BGB, vol. 7, 9th ed. 2024, before § 823 BGB margin no. 123.

299 *Hacker*, RW 2018, 243 (251 f.); *Keßler,* MMR 2017, 589 (592); *Linardatos,* Autonome und vernetzte Aktanten im Zivilrecht, 2021, p. 264 ff.; *Wulf/Burgenmeister,* CR 2015, 404 (407); likewise already in relation to "vending machines" *Wolf,* JuS 1989, 899 (901 f.); in relation to "IT systems", *Lieser*, JZ 1971, 759 (761).

BGB is being discussed,[300] which, however, does not include attribution of fault, but is ultimately limited to a reversal of the burden of proof with regard to fault in the selection and supervision of the assistant.

An analogy to Section 278 BGB, which could probably only be applied in contract law and not in tort law, is, however, largely rejected.[301] Incidentally, it could at best resolve partial aspects. Liability under Section 278 BGB presupposes fault on the part of the assistant. The question that must be asked before applying the analogy would therefore be whether an AI system can be regarded as capable of fault.

Insofar as liability depends on a machine's breach of duty of care, the question arises as to the duty of care requirements applicable to AI systems. Transferring the duty of care requirements applicable to humans is not convincing, as AI systems and humans act in fundamentally different ways.

cc. AI systems and strict liability

With regard to liability for damage caused by AI systems, strict liability is of great interest, not least because of the gaps in fault-based liability.

General strict liability does not exist in most European legal systems.[302] German law contains strict liability provisions for operators of vehicles, aircraft and rail vehicles, as well as for some installations, which also apply if AI systems are components of these machines or installations. There is currently no specific strict liability for AI systems in European legal systems that would cover all AI systems or at least those with particular risks.

Existing rules, in particular product liability, present difficulties with regard to AI systems. A central structural problem of product liability relates to the defectiveness of a product as a central prerequisite for liability. However, the concept of defect

---

300 See, for example, *Denga*, CR 2018, 69 (74 ff.); *Sommer*, Haftung für autonome Systeme, 2020, p. 303 ff.; *Wagner,* in: Säcker/Rixecker/Oetker/Limperg/Schubert, Münchener Kommentar zum BGB Vol. 7, 9th ed. 2024, Section 831 BGB marginal no. 30 ff.

301 *Grapentin*, Vertragsschluss und Verschulden, 2018, p. 130 et seq.; *Grundmann*, in: Säcker/Rixecker/Oetker/Limperg/Schubert, Münchener Kommentar zum BGB, vol. 2, 10th ed. 2025, § 278 BGB marginal no. 46; *Grützmacher*, CR 2016, 695 (697); *Günther/Böglmüller*, BB 2017, 53 (55); *Heuer-James/Chibanguza/Stücker*, BB 2018, 2818 (2829 f.); *Horner/Kaulartz*, CR 2016, 7 (7); *Kirn/Müller-Hengstenberg*, MMR 2014, 307 (311); *ibid.*, CR 2018, 682 (686).

302 *Borges*, CRi 2023, 1 (4); similarly, on German law: *Förster*, in: Hau/Poseck, BeckOK BGB, 75th edition (as of 1 August 2025), Section 823 BGB marginal number 78; *Leupold/Wiesner,* in: Leupold/Wiebe/Glossner, IT Recht, 4th edition 2021, Part 9.6.4 marginal number 104; *Wagner*, ZEuP 2021, 545 (560).

refers to the characteristics of the product, not its behaviour. If a machine causes damage through its behaviour, for example if a highly automated car causes an accident, the question arises as to whether such defective behaviour can be inferred from a defective characteristic.

dd. Proof of liability requirements

A key difficulty in practice lies in proving the conditions for liability, in particular the fault of the liable party and the causality of the fault for the damage incurred.

In tortious liability, the injured party bears the burden of proof for the fault and the causality of the fault for the damage. This is where difficulties arise, not least due to the opacity of AI systems. The injured party usually has no insight into the AI system, and even if they do have access, it is difficult to prove the existence of a defect in the sense of product liability.

With regard to the causality of a breach of duty of supervision for damage that has occurred, there is another problem that is also based on the black box effect or the opacity of AI systems. Since the damage in the situation at hand is caused by the function of the AI system (e.g. a command to control a vehicle), the chain of causality between the negligent behaviour (breach of duty of supervision) of the respective liable party and the damage must also include this intermediate link between the breach of duty of supervision and the damaging action of the AI system. However, given the autonomy of the AI system, it is often hardly possible to determine the causality of a breach of duty of supervision for a specific function of the AI system.

ee. Interim conclusion: gaps in liability law with regard to AI systems

The current liability law therefore has significant gaps with regard to AI systems.[303] It is therefore of particular interest to see what significance the new European Product Liability Directive will have for liability for AI systems and AI models. This is therefore the focus of attention. Liability under national law is then outlined using the example of German law (below 2.).

---

303 *Borges,* NJW 2018, 977 (982); *ibid.*, in: Lohsse/Schulze/Staudenmayer, Liability for Artificial Intelligence and the Internet of Things, 2019, p. 145 (149 f.); *Eichelberger,* in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, § 5 margin note 72 et seq.; *Schaub,* JZ 2017, 342 (346); *Wöbbeking,* in: Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Chapter 4.2 para. 2.

2. Liability for AI models and AI systems under European product liability law

In the context of tortious liability, liability under European product liability law, which is based on the European Product Liability Directive, and liability under the general rules of tort law, which follows the respective national law of the Member States, must be examined. Of particular interest here is the significance of the new European Product Liability Directive for liability for AI systems and AI models, which, as explained at the outset, is intended to modernise product liability with regard to new technologies, not least artificial intelligence. This is therefore the focus of attention. Liability under national law will then be outlined using German law as an example (see 3. below).

a. Overview of the characteristics of product liability

The concept of product liability originated in the 1970s. Developments in US law since the late 1960s were pioneers of product liability.[304] At the same time, liability for products was also the subject of intense debate in Europe, both at the level of the member states of the then European Economic Community and at the level of European Community law. The Product Liability Directive was adopted in 1985 as the first European basis for product liability. The central concept of product liability, which is clearly expressed in the 1985 Product Liability Directive, is legal liability for damage caused by defective products. Since, unlike tortious liability, product liability under European law is strict liability according to the general rules of civil law, it is classified as liability for risk (in the broader sense).

Liability for damage under European product liability law has four key requirements: (1) there must be compensable damage, (2) the damage must have been caused by a product that (3) has a defect that (4) caused the damage.

Product liability exclusively benefits natural persons. Only damage suffered by natural persons to their health or property is compensable, but not damage suffered by companies or legal entities. The party liable for damages is primarily the manufacturer of the (defective) product, but also the manufacturer of components or raw materials and, where applicable, other parties involved (see e. below).

Liability only applies if the product has a defect that causes the damage. The decisive factor is the justified safety expectations for the product (see d. below). The decisive factor for the existence of a defect is the time at which the product was

---

304 *Lorenz*, ZHR 151 (1987), 1 (6).

placed on the market. The subsequent placing on the market of an improved product does not render the product defective.

The international scope of product liability is not regulated by the Product Liability Directive, but is governed by the general rules of the Rome II Regulation[305] for tortious claims. Article 5(1) of the Rome II Regulation contains a special rule for claims arising from damage caused by products. According to this rule, the law of the country in which the injured person has their habitual residence at the time of the damage is decisive, provided that the product was placed on the market in that country (Article 5(1)(a) of the Rome II Regulation), otherwise the law of the country in which the product was purchased, if the product was marketed in that country (Art. 5(1) sentence 1 lit. b. Rome II Regulation), or otherwise the law of the country in which the damage occurred, if the product was marketed in that country (Art. 5(1) sentence 1 lit. c. Rome II Regulation). This connection typically leads to the law of the habitual residence of the injured person.

This means that, for example, if persons with their habitual residence in Germany suffer damage, liability is governed by German tort law. This applies regardless of the manufacturer's registered office or place of business. Accordingly, the respective national product liability law also applies to damage caused by AI systems developed by Japanese providers.

b. The new European Product Liability Directive at a glance

The new European Product Liability Directive (PLD)[306] was published in the Official Journal of the European Union on 18 November 2024 and entered into force on 8 December 2024. As a directive, it is not directly applicable, but must be transposed into national law by the Member States of the European Union by 9 December 2026 in accordance with Art. 22 PLD.

According to Article 3 of the PLD, the directive is fully harmonising, meaning that no deviations in content are permitted under the national law of the Member States. This means that from December 2026, uniform product liability law will apply throughout the EU.

---

305 Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations ("Rome II"), OJ (EC) L 199 of 31 July 2007, p. 40.

306 Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, OJ (EU) L 2024/2853 of 18 November 2024.

It must be transposed by the Member States by 9 December 2026 (Article 22(1) of the Product Liability Directive) and will replace the previous Product Liability Directive from 1985[307] (Product Liability Directive 1985) on that date (Article 21 of the Product Liability Directive).

The new Product Liability Directive introduces significant changes to European product liability law. The scope of compensable damages is only slightly expanded, and the new Product Liability Directive also exclusively favours natural persons. As before, damages suffered by natural persons to their health or property are compensable (Art. 6(1)(a) and (b) PLD). Unlike previously, damage to privately used data is now also eligible for compensation, Art. 6(1)(c) PLD.

The definition of a product has been expanded. According to Art. 4 No. 1 PLD, products include, in particular, goods as well as electricity, software and digital design documents,[308] i.e. digital templates for the production of movable goods by means of automatic control of machines, Art. 4 No. 2 PLD. This is intended to cover, in particular, electronic product templates for 3D printing.[309]

Of particular importance is the explicit inclusion of software, which means that AI systems are also classified as products (see c. bb. below). In addition, the Directive extends liability to updates (see f. aa. below) and even to the failure to perform security-related software updates (see f. bb. below). In addition to the manufacturer, it also holds third parties who modify a product after it has been placed on the market liable (see e. bb. below).

It also contains important evidence relief provisions in favour of the injured party (see g. bb. below), which should make it much easier to enforce claims. This is likely to result in significantly higher liability risks for manufacturers and other liable parties.

Member States have various options for implementing the Directive. Since most Member States have enacted specific product liability legislation in implementation of the 1985 Product Liability Directive, it makes sense to adapt this legislation to the new Directive. In Germany, the Directive is to be implemented by enacting a

---

307 Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ (EC) L 210 of 7 August 1985, p. 29.

308 Art. 4 No. 1 of the Product Liability Directive states: "Product" means any movable item, even if it is integrated into or connected to another movable or immovable item; "product" also includes electricity, digital design documents, raw materials and software.

309 See Recital 16 and, previously, on the *Borges* draft, DB 2022, 2650.

new Product Liability Act ([310]), which is to replace the previous German Product Liability Act.

c. Application of product liability to software, AI systems and AI models

aa. The material scope of the Product Liability Directive

According to Art. 2 PLD, the directive applies to products. According to Art. 4 No. 1 1st half-sentence PLD, a *product* is any movable item, even if it is integrated into or connected to another movable or immovable item. According to Art. 4 No. 1, second half-sentence of the Product Liability Directive, the term " " expressly includes electronics, digital design documents, raw materials and software. According to Art. 4 No. 2 of the Product Liability Directive, digital design documents are digital templates for the manufacture of a movable item. This is intended to cover templates for 3D printing in particular.[311]

Product liability therefore applies to the product as a whole, including all its components. The term "component" refers to "any physical or non-physical object, raw material or associated service that is integrated into or connected to a product" (Art. 4 No. 4 PLD).

Art. 4 No. 3 PLD defines the term "associated service" as "a digital service that is integrated into or connected to a product in such a way that the product could not perform one or more of its functions without it". The term "digital service" generally includes the provision of information. Recital 17, p. 4 PLD cites a navigation service as an example.

The extension of the concept of a product to include non-physical objects, which is unprecedented in the previous Product Liability Directive, is likely to be of particular significance. This means that information services can also constitute a component.

---

310 On 11 September 2025, the *Federal Ministry of Justice* (BMJV) published a draft bill for an amended Product Liability Act (ProdHaftG-RefE) (BMJV, Draft Bill for the Modernisation of Product Liability Law, available at https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_Produkthaftung.pdf?__blob=publicationFile&v=2 (last accessed: 19 November 2025)).

311 *Borges*, DB 2022, 2650 (2650).

bb. Software and AI systems as products

With the explicit inclusion of software, the new Product Liability Directive settles the decades-long dispute over the applicability of product liability to software.

The application of product liability to software has been controversial since the 1985 Directive was enacted. It was undisputed that product liability applies to defects in software integrated into a product (embedded software). However, it was unclear whether it also applied to software that was not integrated into a product, especially if it was delivered via the Internet rather than on a data carrier. In more recent literature, however, it has been unanimously recognised that product liability applies to any type of software that is intended in any way for use by the end consumer. However, the *European Commission* apparently took the view that the application of the Product Liability Directive to software would require an extension of the definition of "product" in the Directive.[312] Since there is still no case law, in particular no clarifying decision by the ECJ, on the applicability of the Product Liability Directive to software, there has been uncertainty in practice in this regard.

The term "software" is not defined in the Directive, but is to be understood in accordance with the ISO definition[313] and refers to instructions for controlling a machine.[314] With the explicit classification of software as a product, all AI systems are included in the scope of product liability, even those that are not high-risk AI systems within the meaning of the AI Regulation.

If an AI system is integrated into other software or into a physical product, such as a machine or plant, this product is subject to product liability. The AI system is then a component of this product, with the result that the manufacturer of the product is liable for defects in the product as a whole, including the AI system, and the manufacturer of the AI system is liable for defects in the AI system as the manufacturer of a component.

---

312 See *European Commission* , Evaluation of Directive 85/374/EEC concerning liability for defective products – Evaluation and Fitness Check (FC) Roadmap, C.2 ("Issues to be examined"), available at https://ec.europa.eu/smart-regulation/roadmaps/docs/2016_grow_027_evaluation_defective_products_en.pdf (last accessed: 19 November 2025).

313 ISO/IEC/IEEE 24765:2017, Definition 3.3783, available at https://www.iso.org/standard/71952.html (last accessed: 19 November 2025); contains three different definitions of the term "software" and essentially understands it to mean programs that serve to operate a computer; see, for example, *Kremer*, in: Taeger/Pohle, ComputerR-HdB, 40th EL March 2025, 32.4 margin note 4 ff.

314 *Borges*, CR 2023, 706 (710); *Gumm/Sommer*, Einführung in die Informatik, 10th ed. 2013, p. 16.

cc. The classification of AI models in product liability law

The AI Regulation has introduced the term "AI model" into European law. The term, which is not explicitly defined in the AI Regulation, essentially refers to the content of a neural network, i.e. the information stored in it.

An AI model is not software, as this information is not executable as such. It is therefore not a product within the meaning of the Product Liability Directive (PLD). However, as soon as it is connected to a computer program that uses the information stored in the model to control a machine, an AI system is created, which in turn constitutes a product within the meaning of the PLD.

This raises the question of whether the AI model can be included in product liability as a connected service or as a component. As explained above, the term "connected service" is defined as the ongoing provision of information. The term is clearly not tailored to AI models. However, a connected service also exists when it is integrated into a product. This can certainly be applied to an AI model if the AI system is understood to mean that information necessary for the functioning of the AI system is continuously extracted from the model. However, this view of the definition of a connected service is unlikely to do justice to the independence and separability of the service in contrast to the AI system, which essentially consists of the AI model.

It therefore seems more convincing to understand the AI model as a component of the AI system. According to Art. 4 No. 4 of the Product Liability Directive, a component is any movable or immovable object. The AI model as a file is an immovable object and can therefore be a component. It is also part of the AI system and should therefore be understood as its component.

This extends the cascade of responsibility described above to include liability for the AI model: if a product in which an AI system is incorporated causes damage, the AI system is a component of the product and the AI model is a component of the AI system.

dd. The exception for open source products

According to Article 2(2) of the Product Liability Directive, the Directive "shall not apply to free and open-source software developed or provided outside the scope of a business activity." This exempts open-source software from product liability. Given the comprehensive inclusion of software, AI systems and AI models in product liability, this exception from the material scope of the Directive is of particular interest.

Article 2(2) of the Product Liability Directive also applies to AI systems. However, it is questionable whether the exemption also applies to AI models. According to the wording, the standard applies to software, but not to AI models. However, according to the wording, the exemption already applies to AI systems as a whole, i.e. also to their components. Incidentally, the inclusion of AI models is required by the spirit and purpose of Art. 2 No. 2 PLD. The exemption from liability is intended to ensure that the development and provision of open source software is relieved of the liability risk arising from product liability, as society benefits considerably from open source software. This objective applies equally to AI models.

According to Article 2(2) of the Product Liability Directive, the Directive does not apply to free and open source software created or provided outside of *commercial activities*.[315] The term "outside the scope of commercial activity" is explained in Recital 14 of the Product Liability Directive. According to this, software provided by non-profit organisations is covered by the exemption (Recital 14, p. 6 of the Product Liability Directive) provided that this is not done within the scope of commercial activity. As Recital 14, p. 7 of the Product Liability Directive clarifies, provision within the scope of a business activity exists if the software is made available in return for a price or the disclosure of personal data[316] . The term "within the scope of a business activity" is therefore to be understood as provision in return for payment. This means that the exception benefits not only private individuals and organisations such as universities and other research institutions, but also companies. The decisive factor is therefore the licence under which the software is provided.

If software is provided under a classic open source licence such as GNU GPL, etc., the exception applies, but not in the case of agreements that provide for consideration in money or the disclosure of personal data.[317] If open source software is offered as an integral part of a paid service package, the exception does not apply, but it does apply if the provision of the software and the services are clearly separated.

Under these conditions, AI systems and AI models are therefore also excluded from the scope of product liability. Provision outside of a business activity is also deemed to exist if AI systems and AI models are provided free of charge by public research institutions.

---

315 The standard reads: "This directive does not apply to free and open source software that is developed or provided outside of a business activity." It has two prerequisites: It must be (1) "free and open source software" that is (2) provided "outside of a business activity."

316 The processing of personal data to improve security, compatibility or interoperability is not considered consideration (Recital 14 p. 7 PLD).

317 *Lejeune*, ITRB 2024, 102 (104) (on so-called dual licensing).

d. Faultiness of AI systems and AI models

The essential prerequisite for product liability is the existence of a product defect and its causality for the damage.

aa. Concept of defect

Article 7 of the Product Liability Directive defines the concept of a product defect essentially as before (Article 6(1) of the 1985 Product Liability Directive[318]): The decisive factor is the legitimate safety expectations of the product (Article 7(1) of the Product Liability Directive) at the time it is placed on the market. The subsequent placing on the market of a better product is irrelevant (Art. 7(3) PLD).

The legitimate safety expectations are to be determined on the basis of several circumstances (Art. 7(2) PLD), which also corresponds to the previous principles (cf. Art. 6(1) Product Liability Directive 1985). There are some new clarifications and additions regarding the determination of defectiveness and legitimate safety expectations. For example, according to Art. 7(1) PLD, legal requirements for the product are, unlike previously, expressly a criterion for determining defectiveness. This should be seen as a clarification, as legal requirements were already an essential element of legitimate safety expectations.[319]

Article 7(2) of the Product Liability Directive regulates the relevant circumstances in its subparagraphs (a) to (i) in much greater detail than the previous regulation. According to subparagraph (a), the presentation and characteristics of the product are particularly relevant. This is likely to correspond to the previous regulation, which referred to the "presentation" of the product in Art. 6(1)(a) of the 1985 Product Liability Directive. According to lit. b., the reasonably foreseeable use of the

---

318 See, for example, on the concept of defect in the previous Product Liability Directive, ECJ, EuZW 2015, 318 (319); Federal Court of Justice, NJW 2009, 1669 (1670); *Beierle*, Die Produkthaftung im Zeitalter des Internet of Things, 2021, p. 182 et seq.; *Borges*, in: Borges/Hilber, BeckOK IT-Recht, 20th edition (as of 1 October 2025), Section 3 ProdHaftG marginal number 1 et seq.; *Hofmeister*, JA 2022, 358 (360 et seq.).

319 H.M. LG Stuttgart, NJW-RR 2012, 1169 (1169 et seq.) (regarding violation of product safety law); *Borges*, in: Borges/Hilber, BeckOK IT-Recht, 20th edition (as of 1 October 2025), Section 3 ProdHaftG marginal number 26; *Kollmer*, NJW 1997, 2015 (2018); *König*, Produktsicherheitsgesetz und Produkthaftung, 2002, p. 157; *Sprau*, in: Grüneberg, Bürgerliches Gesetzbuch, 84th edition 2025, Section 3 ProdHaftG marginal number 4; *Taschner*, in: Taschner/Frietsch, Produkthaftungsgesetz und EG-Produkthaftungsrichtlinie (Product Liability Act and EC Product Liability Directive), 1990, margin note 15; dissenting opinion *Rolland*, Produkthaftungsrecht (Product Liability Law), 1990, margin note 43 (non-compliance merely an indication of a violation).

product is decisive, which corresponds to Art. 6(1)(b) of the 1985 Product Liability Directive.

According to point (c), the effects of the product's learning ability must be taken into account. This provision, which is tailored to AI systems, is new and, naturally, has no precedent in previous law. According to point (d), the foreseeable effects of other products on the product must be taken into account if it can be assumed that they will be used together with the product. This applies in particular to accessories, which was already recognised in practice.

According to lit. e, as well as according to Art. 6(1) lit. c. of the Product Liability Directive 1985, the date of placing on the market is significant. According to lit. f., the "relevant" requirements for product safety, in particular cybersecurity, are relevant. This means that, unlike Art. 7(1) of the Product Liability Directive, this refers not only to legal requirements but also to technical requirements that are not directly legally binding. This also corresponds to the previous law.

According to lit. g., product recalls and other relevant interventions are significant. This aspect requires interpretation, as the fact that an authority orders a product recall does not directly influence legitimate safety expectations, but may at most be an indication of a failure to meet legitimate safety expectations. The explicit mention of this indicative effect makes it easier for a court and the injured party to refer to it, so that the product recall in any case constitutes strong evidence of the actual existence of a product defect.

According to lit. h., the specific needs of the user groups for which the product is intended are important. This aspect seems redundant, as legitimate safety expectations must always be determined on the basis of the target user groups[320] and are already covered by lit. b. Subparagraph (h) can be seen as a clarification of the fact that the use of the product must also take into account the needs of users – namely all relevant user groups.

According to lit. i., in the case of products intended to prevent damage, the absence of such an effect must be taken into account. This seems redundant and dispensable and, at most, serves to clarify the meaning. As under the previous Product Liability Directive, the requirements of product safety law will continue to set no upper limit on safety expectations. A product may therefore be defective even though it complies with the requirements of product safety law.

---

320 *Borges*, in: Borges/Hilber, BeckOK IT Law, 20th edition (as of 1 October 2025), Section 3 ProdHaftG marginal number 6 with further references.

Overall, Article 7(2) of the Product Liability Directive summarises the principles recognised to date. At the same time, it highlights the considerable discretion that courts have in determining whether a product is defective.

The potential for diverging requirements in the individual Member States, even within the framework of product liability, therefore remains very high, despite full harmonisation. This makes it all the more interesting to see whether and to what extent the transparency provisions of the Directive, specifically the obligation to publish decisions and the European database of judgments (Article 19 of the Product Liability Directive), will lead to a harmonisation of product liability law in Europe.

From an academic point of view, the new directive does not bring about any material changes with regard to the concept of defect in software, as the aspects mentioned were already decisive in any case according to the prevailing opinion. From a practical point of view, the directive also provides important clarifications with regard to the concept of defect. This applies not least to the requirements for the cyber security of products. It is therefore clear that damage caused by a product as a result of an attack by a third party triggers product liability if the attack was possible due to inadequate protection (even if this occurred after the product was placed on the market).

bb. Determining defectiveness in products and AI systems

A major challenge of product liability for AI systems concerns the determination of the defectiveness of an AI system. Compared to traditional software, AI systems are typically characterised by a particular flexibility in their outputs, which enables them to respond to a variety of different situations (input values) or, more precisely, to generate output values for a variety of different inputs. This ability can be characterised as the "behaviour" of AI systems,[321] because AI systems can often behave very differently in different situations (and even similar situations).

For example, a self-driving car can drive a large number of kilometres without error, but then suddenly make a driving error and cause an accident.

---

321 See *Borges*, DB 2022, 2650 (2652); *European Commission*, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe, 25 April 2018, COM(2018) 237 final, p. 1, available at: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018DC0237&from=de (last accessed: 17 November 2025); *High-Level Expert Group on Artificial Intelligence*, Defining AI: Key Capabilities and Scientific Fields, 2019, p. 1, available at: https://fmos.link/18290 (last accessed: 17 November 2025); *Lorse*, NVwZ 2021, 1657 (1658); Sommer, loc. cit. (fn. 26), p. 34 et seq.

Such "behaviour", i.e. the output of certain values based on input values from an AI system, is not a property,[322] but rather an action of the system, which may not always be predictable.

This means that such behaviour on the part of an AI system does not necessarily constitute a fault in the AI system. A characteristic and thus a fault of the product can, at most, be its suitability or ability to react correctly in a given situation, or, more precisely, its suitability to generate output values of the desired type from input values.[323]

In view of the so-called "black box effect"[324] of machine learning, which makes it difficult or even impossible to predict the output values with complete certainty,[325] this suitability cannot be determined with certainty a priori.

If every undesirable output (faulty behaviour) of an AI system were assumed to be a product defect, product liability would be strict liability in the form of strict causal liability for the operation of an AI system.[326] However, this is expressly not the case with product liability.[327] Rather, it is limited to compliance with legitimate safety expectations.

The legitimate safety expectations of AI systems can therefore only refer to the predictable behaviour of an AI system, which is determined in particular by testing AI systems and excluding behaviour by filtering certain outputs or comparable measures to ensure safety.

The AI Regulation rightly attaches great importance to the risk management of AI systems, including conformity assessment. Given the extremely dynamic development of AI systems, determining safety requirements is a key challenge. This applies to product liability law no differently than to product safety law. The situation is particularly problematic for AI systems that are not classified as high-risk AI

---

322 *Beierle*, Die Produkthaftung im Zeitalter des Internet of Things, 2021, p. 242; *Borges*, CR 2022, 553 (558 f.); *ibid.*, DB 2022, 2650 (2654); *Sommer*, loc. cit. (fn. 26), p. 231; *Wagner*, AcP 217 (2017), 707 (734).

323 *Borges*, ICAIL '21: Proceedings of the Eighteenth International Conference on Artificial Intelligence and Law 2021, 32 (36); *idem*, CR 2022, 553 (559); *Gless/Janal*, JR 2016, 561 (564).

324 See, for example, *Ras/van Gerven/Haselager*, in: Escalante et al., Explainable and Interpretable Models in Computer Vision and Machine Learning, p. 19 (21); see also *Gaur/Faldu/Sheth*, IEEE Internet Computing, Vol. 25 No. 1 (2021), 51 (51 f.).

325 *Borges*, CR 2023, 706 (713).

326 *Borges*, CR 2022, 553 (559).

327 *Borges*, CR 2022, 553, (559).; *Hacker*, RW 2018, 243 (258 f.); *Horner/Kaulartz*, CR 2016, 7; *Lieser*, JZ 1971, 759 (761).

systems within the meaning of the AI Regulation, as there is no legally guaranteed infrastructure for defining the safety requirements for AI systems.

e. The group of liable parties

The parties liable under product liability are regulated in Art. 8 of the Product Liability Directive.

aa. Manufacturers and equivalent parties

According to Article 8(1)(a) of the Product Liability Directive, the main party liable is the manufacturer of the product. If a manufacturer is based outside the EU, the importer (Article 8(1)(c)(i) of the Product Liability Directive) and – newly added to the 1985 Product Liability Directive – the manufacturer's authorised representative (Article 8(1)(c)(ii) of the Product Liability Directive) are also liable. PLD) and (subordinately) the so-called fulfilment service provider (Art. 8(1)(c)(iii) PLD) are also liable. According to Art. 4 No. 11 PLD, an authorised representative is anyone who is authorised to act on behalf of the manufacturer on the basis of a written order, and according to Art. 4 No. 13 PLD, a fulfilment service provider is anyone who offers at least two of the specified services, namely storage, packaging, addressing and shipping of products not belonging to them. Finally, according to Art. 8 para. 3 PLD, the supplier of the product may also be a subsidiary addressee of liability, and according to Art. 8 para. 4 PLD, the provider of an online trading platform may also be a subsidiary addressee of liability.

The term "manufacture" is to be interpreted broadly and includes, in particular, the design and fabrication of a product. In the case of software, manufacture includes development and reproduction, and, where applicable, transfer to data carriers. In the case of an AI model, it refers to the training process.

The manufacturer is the person responsible for the production process, not the employees who actually manufacture the product. According to Art. 4 No. 10 lit. b. 2. This is particularly important for sellers who distribute products from a contract manufacturer under their own name ( ). This also applies to distributors who market a product under a private label.

bb. Product liability in the event of modification and change of purpose of AI systems by users

Traditionally, product liability only covers the manufacturer and parties with equivalent liability, but not the user of a product. This principle is significantly changed

by Art. 8(2) of the Product Liability Directive: according to this, anyone who "substantially modifies a product and then places it on the market or puts it into service" is considered a manufacturer and can be held liable by the injured party. This provision primarily addresses the user of a product.

The liability of the user under Article 8(2) of the Product Liability Directive exists alongside the liability of the original manufacturer and other liable parties, and therefore does not lead to the exclusion of liability. If the product was fault-free prior to the modification, the manufacturer's liability does not apply.

The term "significant modification" is defined in Art. 4 No. 18 of the Product Liability Directive. According to Art. 4 No. 18 lit. a. PLD, a modification is substantial if it is substantial in accordance with the applicable product safety law. In the absence of applicable criteria under product safety law, the modification is substantial according to Art. 4 No. 18 lit. b. Product Liability Directive if it changes the performance, purpose or nature of the product (Article 4(18)(a)(i) Product Liability Directive) and (significantly) changes the risk profile of the product (Article 4(18)(a)(ii) Product Liability Directive).

This provision is of particular interest in relation to software and AI systems. With regard to software, modifications that are frequently made to software used for business purposes are significant. If a modification is to be regarded as a substantial change within the meaning of Art. 4 No. 18 PLD, Art. 8 (2) PLD applies and extends product liability to the entity responsible for the modification. The AI Regulation is one of the relevant product safety laws within the meaning of Article 4(18)(a) of the Product Liability Directive. In the case of AI systems, a substantial modification within the meaning of Article 8(2) of the Product Liability Directive may exist, not least if an AI system continues to be trained after it has been placed on the market.

Art. 8(2) PLD could be of even greater significance, especially for AI systems, with regard to changes in purpose. A change in purpose in this sense occurs when the area of application of an AI system is changed and this changes the risk profile.[328] The decisive factor here is the intended use specified or at least approved by the manufacturer. If the user deviates from this in a way that changes the risk of the AI

---

[328] See *Borges*, CR 2025, 1 (7, para. 67); *Piovano/Hess*, Das neue europäische Produkthaftungsrecht, 2024, § 3 para. 107 f.; cf., on the draft, *Kapoor/Klindt*, BB 2023, 67 (69).

system, this constitutes a significant change that triggers a change of role to manufacturer under Article 8(2) of the Product Liability Directive.[329]

This creates serious liability risks for users of AI systems if they deviate from the objectives specified by the manufacturer. From the perspective of AI system manufacturers, it is in their interest to define the intended use of the system as precisely as possible.

f. Product liability in the event of changes after placing on the market

As clarified in Article 7(2)(e) of the Product Liability Directive, the decisive point in time for the existence of a product defect is the point in time at which the product was placed on the market. This principle is confirmed in Article 11(1)(c) of the Product Liability Directive, according to which product liability is excluded if the manufacturer can prove that the defect did not exist at the time the product was placed on the market or only arose after that time.

Something else may apply in the case of subsequent changes to the product (see below aa.). In the case of software, failure to make a change may also lead to liability (see below bb.).

aa. Changes to the product after it has been placed on the market – updates

The significance of changes to the product after it has been placed on the market is regulated in Art. 11 of the Product Liability Directive. If the manufacturer makes a significant change to the product after it has been placed on the market, Art. 11(2)(d) of the Product Liability Directive stipulates that the exclusion of liability for subsequent defects under Art. 11(1)(c) of the Product Liability Directive does not apply.

If third parties make a significant change to the product, they themselves become manufacturers under Article 8(2) of the Product Liability Directive. The date of the change is then decisive for assessing the defectiveness of the product in relation to its characteristics.

The term "significant change" is defined in Art. 4 No. 18 of the Product Liability Directive. Art. 4 No. 18 lit. a. of the Product Liability Directive refers primarily to the criteria of European product safety law. According to this, a change is significant if it is significant in accordance with the applicable product safety law. In the

---

329 *Borges*, in: Borges/Hilber, BeckOK IT-Recht, 20th edition (as of 1 October 2025), Section 1 ProdHaftG margin note 18h.

absence of applicable criteria under product safety law, the change is significant under Art. 4 No. 18 lit. b. PLD if it alters the performance, purpose or nature of the product (i) and (significantly) changes the risk profile of the product (ii).

With regard to software, the question arises as to under what conditions adjustments to the software are to be regarded as a significant change. According to Recital 40 sentence 1 of the Product Liability Directive, the same rules should apply to changes made by software updates or upgrades as to other changes. The decisive factor is therefore whether the risk profile changes.

In practice, the most important cases of changes to products after they have been placed on the market by the manufacturer are software updates and upgrades. Software updates can cause software that has already been placed on the market to become defective. This is not uncommon in practice.

Even under previous law, it was assumed that a product could become defective as a result of an update and that an update could therefore trigger product liability.[330]

This aspect is expressly regulated in the new Product Liability Directive. According to Art. 11(2)(b) of the Product Liability Directive, the exclusion of liability under Art. 11(1)(c) of the Product Liability Directive does not apply if the defectiveness was subsequently caused by software, in particular software updates or upgrades. Therefore, if an update causes software, and thus possibly also a product in which the software is integrated, to become defective, product liability applies.

bb. Liability for failure to perform security updates

Art. 11(2)(c) of the Product Liability Directive introduces a significant innovation in product liability: according to this provision, the exclusion of liability for product defects arising after the product has been placed on the market does not apply in the case of a "lack of software updates or upgrades necessary to maintain safety". The standard is to be understood in such a way that the absence of updates or upgrades necessary to maintain safety triggers product liability ( ).

This provision is particularly important for software and all products with an internet connection. The main risks associated with products connected to the internet include cyber attacks, i.e. attacks via the internet through which software (known as malware) is installed or settings or software are changed. However, resilience

---

330 *Borges*, CR 2022, 553 (558); *idem*, DB 2022, 2650 (2652); *De Bruyne/Tanghe*, JETL Vol. 8 No. 3 (2017), 324 (370); *Oechsler*, in: Staudinger BGB, revised edition 2021, Section 1 ProdHaftG marginal number 60b; *Reusch*, BB 2019, 904 (906); *Sodtalbers,* Softwarehaftung im Internet, 2006, p. 134 et seq. (marginal number 206 et seq.).

against such attacks is one of the security requirements for software.[331] This is also assumed to be the case for current product liability law.[332] Of course, only the absence of avoidable security vulnerabilities is considered a legitimate security expectation, the failure to meet which constitutes a product defect.[333] This applies in particular to known security vulnerabilities.[334]

The new Product Liability Directive requires, in Art. 11(2)(c) PLD, ongoing resilience against cyber attacks by closing security gaps through updates. This does not establish a legal obligation to provide updates, as clarified in Recital 51, p. 5 of the Product Liability Directive. However, if a reasonable security update is not provided, this constitutes a product defect under Article 11(2)(c) of the Product Liability Directive. The Product Liability Directive thus ultimately establishes an obligation to maintain software in relation to product safety.[335]

Art. 11(2)(c) of the Product Liability Directive does not contain any provision on the required duration of the provision of these improvements. This is based on the legitimate expectation of use. For products that are equipped with software and are therefore connected to the internet, cyber security must therefore be guaranteed for the typical useful life of the product.[336]

g. Fact-finding and burden of proof

In practice, it is crucial for product liability whether the injured party succeeds in proving the prerequisites for liability; specifically, whether, in addition to compensable damage, a defect in the product and the causality of the defect for the damage can be proven. Not least in the case of damage caused by software, the enforcement of product liability claims often fails in practice, as both proving a defect and proving causality pose considerable challenges for the injured party. This problem is exacerbated in the case of AI systems. In addition to the aforementioned problem that the requirements for AI systems are still largely unknown, it is often impossible

---

331 *Brenner*, RDi 2024, 345 (350); *Riehm/Leithäuser/Brenner*, in: Raue, Digitale Resilienz, 2024, p. 5 (6 f.).

332 See *Riehm/Leithäuser/Brenner*, in: Raue, Digitale Resilienz, 2024, p. 5 (7); *Wagner/Ruttloff/Römer*, CCZ 2023, 109.

333 On the merits, see also *Brenner*, RDi 2024, 345 (350).

334 See also *Raue*, NJW 2017, 1841 (1842).

335 *Borges*, in: Borges/Hilber, BeckOK IT-Recht, 20th edition (as of 1 October 2025), Section 2 ProdHaftG marginal number 50 (on the Commission draft); essentially the same view is taken by *Brenner*, RDi 2024, 345 (351) (obligation to carry out updates).

336 Similarly *Brenner*, RDi 2024, 345 (351 f.).

to reproduce the specific behaviour of an AI system from the past – at least if the source data has not been fully logged.

The new Product Liability Directive makes it easier to prove product defects and causality in favour of the injured party through two instruments: According to Art. 9 of the Product Liability Directive, innovative rules on the disclosure of evidence apply, which are intended to facilitate the clarification of facts, and according to Art. 10 of the Product Liability Directive, presumption rules apply in favour of the injured party.

aa. Disclosure of evidence

Article 9 of the Product Liability Directive contains rules on the disclosure of evidence in the event of a claim for damages by the injured party under the rules of product liability. According to Art. 9(1) of the Product Liability Directive, the court may require the defendant to disclose relevant evidence in its possession. Art. 9(2) of the Product Liability Directive contains an obligation on the plaintiff to disclose the evidence in its possession.

According to paragraph 3, the principle of proportionality applies to the disclosure under paragraphs 1 and 2. Paragraphs 4 and 5 regulate restrictions for the protection of trade secrets. Paragraph 6 contains the defendant's obligation to present the evidence in an easily accessible and comprehensible form, if this is proportionate in terms of costs and effort. Paragraph 7 clarifies that the provisions of national law on the clarification of facts remain unaffected.

The enforcement of the disclosure obligation is governed by national law. However, the defendant's obligation to disclose under Article 9(1) of the Product Liability Directive is linked to the burden of proof rule in Article 10 of the Product Liability Directive (see bb. below). According to Art. 10(2)(a) of the Product Liability Directive, the burden of proof is reversed for the defectiveness of the product if the defendant "fails" to make the required disclosure.

bb. Burden of proof

The burden of proof is regulated in Art. 10(1) of the Product Liability Directive. According to Art. 10(1) of the Product Liability Directive, as before, the injured party bears the burden of proving the defectiveness of the product, the damage and the causality of the defect for the damage. However, Art. 10(2)-(4) of the Product Liability Directive contains presumption rules that allow the burden of proof to be reversed in favour of the injured party. These presumptions are rebuttable (Art. 10(5) of the Product Liability Directive).

The defectiveness of a product is presumed under Art. 10(2)(a) PLD if the defendant fails to disclose information under Art. 9(1) PLD. According to Art. 10(2)(b) PLD, it is presumed if the product does not meet the legal requirements of product safety law, provided that these requirements relate to risks suffered by the injured party.[337]

According to Art. 10(2)(c) of the Product Liability Directive, the defectiveness of the product is presumed if the damage was caused by an obvious malfunction of the product. This provision is likely to be one of the most important in the entire Product Liability Directive. In any case, it is of particular importance for damage caused by software and AI[338] . According to Art. 10(2)(c) of the Product Liability Directive, the injured party only has to prove the malfunction in order to trigger the presumption of defectiveness of the product. This means that the manufacturer has the burden of proving that the malfunction was unforeseeable.[339] This will often not be possible, meaning that the manufacturer bears a higher liability risk than under the previous regulation.

According to Art. 10(3) of the Product Liability Directive, there is a presumption of causality between the product defect and the damage if the damage is "typically" attributable to the defect in question. The presumption requires proof of a product defect. It is sufficient if this proof is provided on the basis of the reversal of the burden of proof under Art. 10(2) of the Product Liability Directive. The presumption of causality under Article 10((3) of the Product Liability Directive is extremely important in practice, as it is often difficult to prove the causality of a product defect beyond doubt. This is particularly true for software due to the complex causal relationships involved.[340] Art. 10(3) of the Product Liability Directive 2024 thus solves a fundamental problem of liability in connection with software and AI systems[341] .

According to Article 10(4) of the Product Liability Directive 2024, the existence of a product defect or its causality for the damage, or even both, is presumed if the proof is "excessively difficult for the claimant due to the technical or scientific complexity" (Art. 10(4)(a) PLD) and the existence of a defect or the causality of the

---

337 See *Borges,* CR 2025, 1 (13, margin note 136); *Thöne*, MMR 2025, 499 (502).

338 For more on this, see *Borges*, CR 2025, 1 (13, para. 136 ff.); cf. also *Ebers,* KIR 2025, 252 (257); *Wendehorst,* EuZW 2024, 876 (880).

339 On the predictability of malfunction as a criterion for defectiveness, see *Borges*, CR 2025, 1 (13 f., para. 139 ff.); *Piovano/Hess,* Das neue europäische Produkthaftungsrecht, 2024, § 6 para. 44.

340 See *Borges*, CR 2025, 1 (14, para. 143); *Ebers,* KIR 2025, 252 (257 f.).

341 *Borges,* CR 2025, 1 (14, para. 144).

defect for the damage, or both, is "probable" (Art. 10(4)(b) PLD). This presumption ultimately leads to a reduction of the standard of proof to "probability"[342] . Therefore, a restrictive interpretation of Art. 10(4) PLD is required in two respects: The difficulties of proof "due to the technical or scientific complexity" presuppose that the risks posed by the product are unclear in such a way that it cannot be determined whether these risks could be reasonably accepted by the manufacturer.[343] From the point of view of the probability of the existence of a defect or its causality, a preponderance of probability is required[344] .

h. Scope of liability and internal compensation

Product liability is limited in several respects. The scope of compensable damages is regulated in Art. 6 PLD. According to Art. 6(1) of the Product Liability Directive, compensation ("damage") is limited to bodily injury (lit. a.) and damage to property, except for property used for professional purposes (lit. b. sublit. iii.). Damage to data not used for professional purposes (lit. c.) is also eligible for compensation.

According to Art. 6(1)(a) of the Product Liability Directive, damage to mental health may also be eligible for compensation. However, a more restrictive line should be taken here, as the wording of the provision and Recital 21 of the Product Liability Directive make clear with their reference to "medically recognised" or "medically recognised and medically certified" impairments. In contrast, violations of personal rights as such are still not covered by product liability. Recital 24, sentence 1 of the Product Liability Directive refers here to violations of privacy and discrimination as examples.

Art. 6 of the Product Liability Directive is thus one of the most important provisions of product liability law, as it limits liability, as before, to damage to natural persons and, in addition, in the case of damage to property and data, to damage in the private sphere.

The contributory negligence of the injured party must be taken into account as a mitigating factor in accordance with Art. 13 of the Product Liability Directive ("Reduction of liability").

---

342 *Becker/Bell/Meyer*, NJW 2024, 3745 (3749); *Borges*, CR 2025, 1 (14, para. 146); see also *Wagner*, VersR 2025 129 (144).

343 *Borges*, CR 2025, 1 (14, para. 147).

344 *Borges,* CR 2025, 1 (14, para. 148); *Piovano/Hess,* Das neue europäische Produkthaftungsrecht, 2024, § 6 para. 53; *Wagner*, VersR 2025, 129 (144).

Art. 16 PLD ("Limitation period") and Art. 17 PLD ("Exclusion period") regulate the time limits for liability. As before (Article 10 of the Product Liability Directive 1985), the limitation period is three years, beginning with the date on which the damage, defect and liable party became known (Article 16(1) of the Product Liability Directive). According to Art. 17 PLD, as before (Art. 11 Product Liability Directive 1985), a limitation period of ten years applies, beginning with the placing on the market or putting into service of the product or with the provision or putting into service of a substantially modified product (Art. 17(1) sentence 2 PLD).

The various liable parties are jointly and severally liable pursuant to Art. 12 PLD ("Liability of several economic operators"), as was already the case under Art. 5 Prodhaftungs-RL 1985. Art. 14 PLD ("Right of recourse") regulates one aspect of the internal settlement of liability between several liable parties. According to this, the party providing compensation may assert recourse claims against other economic operators in accordance with national law. Recourse under Art. 14 PLD is particularly important for manufacturers of components and is likely to be significant in relation to the liability of manufacturers of AI systems and AI models. Since damage to persons or property is mainly caused by physical products, injured parties will typically make a claim against the product manufacturer. However, pursuant to Art. 14 PLD, the manufacturer can seek recourse against the manufacturer of an embedded AI system if the damage was caused by a faulty embedded AI system.

3. Liability for AI systems and AI models under general tort law using German law as an example (overview)

As described above, tortious liability may arise under the rules of national law of the European Member States, which apply in addition to the rules of European product liability law.

The international scope of application of national tort law follows the rules of the Rome II Regulation. According to Art. 4(1) Rome II Regulation, the law of the country in which the damage occurs is generally applicable. This is typically the place of residence of the injured party at the time of the infringement of legal rights.

Article 5(1) of the Rome II Regulation contains a special rule for damage caused by products. According to this rule, the law of the country in which the injured person has their habitual residence at the time of the damage is applicable, provided that the product was marketed in that country (Article 5(1)(a) of the Rome II Regulation), otherwise the law of the country in which the product was purchased, if the product was marketed in that country (Art. 5(1) sentence 1 lit. b. Rome II Regulation), or otherwise the law of the country in which the damage occurred, if the

product was marketed in that country (Art. 5(1) sentence 1 lit. c. Rome II Regulation). This connection typically leads to the law of the habitual residence of the injured person.

This means that, for example, if persons with their habitual residence in Germany suffer damage, liability is governed by German tort law. In German tort law, liability under the general tort clause regulated in Section 823(1) of the German Civil Code (BGB) (see a) is of particular interest. It is also interesting to note whether liability arises under Section 823(2) BGB in conjunction with a so-called protective law (see b) below).

a. Liability under the general clause of tort law (Section 823 (1) BGB)

According to Section 823 (1) BGB, anyone who intentionally or negligently infringes one of the protected legal interests, i.e. an absolutely protected legal interest, is liable. Apart from cases of intentional violation, the central prerequisite for liability is the violation of a duty of care, often referred to as a duty of traffic safety ([345]) or, in older statements, as a duty to ensure traffic safety, which must be causal (in the sense of objective imputability) for the violation of legal interests. The focus of liability here is on the violation of a specific duty of care, i.e. conduct on the part of the liable party that is contrary to the duty of care.

However, it seems possible that case law will regard the obligations of the AI Regulation on risk management for high-risk AI systems as a duty of care. The literature already argues that these obligations should be classified as a concretisation of the tortious duty of care.[346]

In the event of a negligent breach of a protected legal interest, the person who caused it is liable to the injured party for the entire damage resulting from it. There is no limitation on the scope of liability.

In the case of damage caused by AI systems, liability under Section 823 (1) of the German Civil Code (BGB) has serious gaps, as described above, since liability only applies if there has been a culpable breach of duty by a natural person. This must also be proven by the injured party; there is no relaxation of the burden of proof in this respect.

For this reason, there has been intense debate for several years as to whether and, if so, how the gaps in this law (de lege lata) or future law (de lege ferenda) can be

---

345 *Wagner,* AcP 217 (2017), 707 (711).

346 *Grützmacher*, CR 2021, 433 (437 ff).

closed. Apart from the reform of product liability, however, no measures have been taken to date. It is therefore unclear whether and to what extent the rules of German tort law give rise to practically relevant risks of liability under Section 823 (1) BGB.

b. Liability under protective laws (Section 823 (2) BGB)

In the context of liability for damage caused by AI systems, it is of interest whether liability can arise from Section 823 (2) BGB. The significance of this question stems not least from the fact that Section 823(2) BGB is not limited to the violation of legal interests within the meaning of Section 823(1) BGB, but also allows for compensation for pure financial losses.[347]

Liability under Section 823 (2) BGB applies if the damage is based on a culpable violation of a so-called protective law. The Federal Court of Justice defines a protective law as a "norm which, according to its purpose and content, is intended at least in part to protect individuals or specific groups of persons against the violation of a specific legal interest"[348] . Due to the extension of tort law to compensation for pure financial losses associated with Section 823 (2) BGB, when qualifying a norm as a protective law, it must always be examined whether this extension of negligence liability for pure financial losses is objectively necessary and acceptable in the specific case.[349]

This coordination is achieved through the protective nature of the standard, the violation of which gives rise to liability under Section 823(2) of the German Civil Code (BGB). It is therefore important to determine whether the violated standard can be regarded as a protective law within the meaning of Section 823(2) BGB and whether it fulfils the material, personal and modal scope of application in the specific case.

There has been no comprehensive discussion of protective laws in connection with the production of AI models and AI systems or the operation or use of AI systems to date. The literature discusses whether and, if so, which standards of the AI Regulation are to be regarded as protective laws. The protective law characteristic is

---

347 Unstr., see only *Förster*, in: Hau/Poseck, BeckOK BGB, 75th edition (as of 1 August 2025), Section 823 BGB marginal number 267; *Hager*, in: Staudinger BGB, new edition 2021, Section 823 marginal number G 4.

348 BGH, NJW 1964, 396 (397); NJW 1992, 241 (242); NJW 2004, 356 (357); NJW-RR 2005, 673; NJW 2005, 2923 (2924); DAR 2015, 137; NJW 2018, 1671 (1673); NJW 2020, 1514 (1517); NJW 2022, 3156 (3157).

349 BGH, NJW 1976, 1740 (1741); *Wagner*, in: Säcker/Rixecker/Oetker/Limperg/Schubert, Münchener Kommentar zum BGB, vol. 7, 9th ed. 2024, § 823 BGB marginal no. 534.

assumed, for example, for the prohibition of using prohibited AI systems (Art. 5 AI Regulation)[350] or for the obligation to use relevant, representative, error-free and complete training data to avoid discriminatory decisions by high-risk AI systems (Art. 10(3) AI Regulation)[351] as well as generally for the obligations of providers and users.[352] Certain regulations on various reporting and information obligations of manufacturers and (commercial) users are also to be given protective law characteristics (Art. 22, 26(2), 27(2) and (4), 29(4) AI Regulation).[353] One of the reasons given for this is that the regulation is not intended merely as a reflex to protect European fundamental rights.[354] Other voices, however, reject the classification of AI Regulation standards as protective laws.[355]

For damages caused by AI systems, it may be important whether and which provisions of the GDPR are to be regarded as protective laws. This question is highly controversial. As far as can be seen, there is no case law on this issue yet. In isolated cases, reference is made to the GDPR as a protective law without differentiation.[356] In some cases, Articles 6 (1), 7, 8, 9 (2), 12, 13, 14, 17, 20 and 22[357] or other individual standards[358] are classified as relevant under tort law, and in some cases even all or almost all articles.[359] The protective nature of the law was also controversially discussed in relation to the previous version of the BDSG.[360] Sections 4, 6, 19, 20,

---

350 *Grützmacher*, CR 2021, 433 (438).

351 *Roos/Weitz*, MMR 2021, 844 (850).

352 *Linadartos*, GPR 2022, 58 (60).

353 *Grützmacher*, CR 2021, 433 (441); *Roos/Weitz*, MMR 2021, 844 (850).

354 ErwGr. 5 KI-VO; *Roos/Weitz*, MMR 2021, 844 (850).

355 *Borges*, in Borges/Keil, Legal Handbook Big Data, Section 7, margin note 268 et seq.

356 *Schmidt*, in: Taeger/Gabel, GDPR – BDSG – TTDSG, 4th ed. 2022, Art. 1 GDPR para. 34.

357 *Schmidt,* in: Taeger/Gabel, GDPR – BDSG – TTDSG, 4th ed. 2022, Art. 1 GDPR margin no. 35; in agreement *with de la Durantaye*, in: Borges/Hilber, BeckOK IT-Recht, 20th edition (as of 1 April 2023), Section 823 BGB margin note 68; and *Pötters*, in: Gola/Heckmann DS-GVO/BDSG Art. 1 DS-GVO margin note 13.

358 See *de la Durantaye*, in: Borges/Hilber, BeckOK IT-Recht, 20th edition (as of 1 April 2023), Section 823 BGB marginal number 68; *Spindler*, in: Gsell/Krüger/Lorenz/Reymann, BeckOGK BGB (as of 1 August 2025), Section 823 BGB marginal number 334.

359 *Strauß/Schweers*, DSRITB 2019, 111 (119) ("the standards of the GDPR"); see also *Wybitul/Haß/Albrecht*, NJW 2018, 113 (footnote 3) ("to the greatest extent possible").

360 See OLG Hamm, NJW 1996, 131; *Hermeler*, MMR 1999, 17 (18); *Pötters*, in: Gola/Heckmann, DS-GVO/BDSG, 3rd ed. 2022, Art. 1 GDPR marginal no. 13; *Wagner*, in: Säcker/Rixecker/Oetker/Limperg/Schubert, Münchener Kommentar zum BGB, vol. 7, 9th ed. 2024, § 823 BGB para. 691.

34 and 35 of the BDSG are sometimes referred to as protective laws.[361] In some cases, the protective nature of the GDPR and its standards as a whole is rejected.[362]

Regardless of this, the burden of proof for a violation of the protective law and causality lies with the injured party. The above-mentioned difficulties with regard to AI systems are also relevant in this respect. The practical relevance of liability is therefore unclear.

4. Conclusion and recommendations for Japanese providers and manufacturers

The new PLD introduces significant clarifications and innovations to European product liability law. Some legal literature refers to a new era of product liability. Regardless of this, the new PLD has a particular impact on AI users and AI models, which are included in the rules of product liability.

The ongoing responsibility for product safety poses considerable challenges for developers of AI systems and AI models. The inclusion of users as liable parties for the first time is also of particular significance for AI systems, as even use for an unintended purpose can trigger liability.

Since Japanese providers of AI models and AI systems as well as Japanese manufacturers of products that include AI systems may also be affected by the new Product Liability Directive, the Product Liability Directive is becoming increasingly important for all developers of AI systems and their components, as well as for deployers of AI systems whose results are used in the EU and could cause damage there.

From the perspective ofJ apanese providers of AI systems and AI models, it therefore makes sense to comply with the requirements of the AI Regulation in order to avoid liability risks, as some of its requirements, such as those in Art. 8(2) PLD, but also indirectly as a specification of safety expectations for determining a product defect and as a concretisation of traffic obligations within the meaning of general tort law.

The intended purpose of an AI model and an AI system is likely to be of crucial importance. Providers should clearly define the intended use of an AI system, as is

---

361 *Spindler*, in: Gsell/Krüger/Lorenz/Reymann, BeckOGK BGB (as of 1 August 2025), Section 823 BGB marginal number 333; *Wagner*, in: Säcker/Rixecker/Oetker/Limperg/Schubert, Münchener Kommentar zum BGB, Vol. 7, 9th edition, 2024, Section 823 BGB, margin note 691.

362 *Borges*, in: Borges/Keil, Rechtshandbuch Big Data, 2024, Section 7 marginal number 275 et seq.

the case under the AI Regulation. This applies not least to cases where AI systems are incorporated into products. Similarly, when using AI models and AI systems, clear liability rules are recommended in relation to purchasers who incorporate AI models and AI systems into their products and services.