6

Legal Requirements for Design and Development of Edge AI Systems

Edge AI as defined in this book combines AI, IoT and edge computing. By decentralising AI models and algorithms on-device, edge AI can support the emergence of models of AI deployments that are more privacy-preserving and afford users more control over their data. Edge AI systems are domains of active research. This means that there is, for the moment, limited consensus and standardized approaches. For the purpose of legal analysis, edge AI remains, therefore, an umbrella term capable of encompassing different technologies, design choices, and architectures.

Existing Union laws provide a comprehensive and robust framework for the design and development of edge AI technologies. However, there is, for the moment, limited guidance on their practical implementation by edge AI providers. Indeed, Union laws and their corresponding official guidelines make no mention of "Edge AI". This means that edge AI systems and models are subject to a fragmented legal landscape, predominantly formulated in technologically neutral terms or, in the case of Regulation (EU) 2024/1689 (Artificial Intelligence Act), in the form of general objectives subject to further technical specification.

The following sections provide a first attempt to identify the corpus of laws and legal requirements relevant for providers of edge AI systems focusing on Union laws of general application[1] setting out *design requirements* and *human rights safeguards* for AI systems and models. Legal considerations relating to *lawfulness* are not reviewed in detail in this contribution.

[1] This means that regimes of *lex specialis* are excluded from the scope of analysis. This refers, for example, to legal rules and requirements that apply to certain regulated products such as medical devices, toys, etc.

6.1 General Data Protection Regulation - Regulation (EU) 2016/679

Regulation (EU) 2016/679 ("General Data Protection Regulation") applies whenever personal data is processed, regardless of the means used, and pursues the double objective of protecting natural persons and fundamental rights, while ensuring the free movement of personal data [109][2]. Processing operations involving personal data are subject to basic design principles, rights to be afforded to data subjects and, depending on the risks, certain additional safeguards for fundamental rights and freedoms. Compliance with these legal requirements is the responsibility of the data controller, i.e., the natural or legal person determining the purposes and means of processing[3]. For this purpose, the Regulation establishes obligations ensuring that appropriate technical and organisational measures and required safeguards are in place (see Table 6.1)[4].

The European Data Protection Board ("EDPB") is an essential body for the implementation of data protection laws, empowered to issue guidance on the consistent application of data protection rules in the Union. The EDPB has begun work on data protection aspects of Artificial Intelligence but has not issued official guidelines yet. It has, however, published an Opinion on certain data protection aspects related to the processing of personal data in the context of AI models and a report on the investigations led at European level on ChatGPT [113, 114]. Most of the Board's analysis in these documents focuses on particular technological applications (i.e., chatbots using LLMs, web scraping) and legal issues (i.e., controllers' legitimate interests and secondary uses of personal data).

The Board, however, recalled and specified the design objectives enshrined in the legal concept of "anonymisation" and the principle of privacy by design in the context of AI models. First, the Board clarifies that AI models trained on personal data can be considered to be anonymous only following

[2] Personal data is defined under article 4(1) of Regulation (EU) 2016/679 as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

[3] As defined in article 4(7) of Regulation (EU) 2016/679.

[4] For the precise formulation of these requirements, see articles 5, 9, 12-22, 25, 32, and 35 of Regulation (EU) 2016/679.

Table 6.1 Concise Overview of the Main Design Requirements Imposed by the General Data Protection Regulation

Data Protection Principles.	**Data Subjects' Rights.**	**Processing Operations Subject to Additional Safeguards.**	**Conrollers' Obligations.**
• Lawfulness, fairness, and transparency. • Purpose limitation. Data minimisation. • Accuracy. • Storage limitation. • Confidentiality and integrity. • Accountability.	• Information to be provided to data subjects. • Right of access. • Right to rectification. • Right to erasure. • Right to restriction of processing. • Right to data portability. • Right to object. • Automated individual decision-making, including profiling.	• Processing of special categories of personal data. • Individual decisions obtained from fully automated processing. • Processing presenting a high risk to individuals' fundamental rights and freedoms.	• Data protection by design and by default. • Security. • Data protection impact assessment.

a strict assessment ascertaining that the likelihood of direct extraction of instances of training data and the likelihood of obtaining such data through queries, using reasonable means, is insignificant for any data subject whose data is part of the training data set. Residual likelihood of identification is to be assessed considering direct access to the model and an evaluation of the appropriateness and effectiveness of the measures ensuring anonymity. This evaluation may consider (i) the model's design, evaluation, testing and resistance to attack as well as its documentation or (ii) any other approaches offering an equivalent level of protection [113][5].

Second, the Board explained some of the implications of the principle of data protection by design identified during the investigations on ChatGPT. The Board recalls that "the principle of data protection by design [. . .] shall be taken into account at the time of the determination of the means for processing and at the time of the processing itself", and provides examples of measures that can be taken (e.g., filtering criteria for data collection and deletion measures, information of data subjects about the collection and accuracy of the processing, modalities to facilitate the exercise of rights, etc.) [114][6].

[5] See pp. 16-19.
[6] See pp. 5-9.

The implications of certain data protection provisions for AI models have not yet been examined in detail by the Board, including the processing of special categories of data, automated-decision making, data protection impact assessment, and a general and systematic analysis of the principle of data protection by design and by default [113][7].

There is, therefore, limited guidance on key data protection aspects of edge AI models and systems, namely their operation in close proximity to data sources and use-cases relying on local decision-making in real-time.

6.2 Artificial Intelligence Act - Regulation (EU) 2024/1689

Regulation (EU) 2024/1689 ("Artificial Intelligence Act") establishes rules for the development, the placing on the market, the putting into service and the use of AI systems[8] in the Union and a particular regime for General Purpose AI ("GPAI") Models,[9] based on the risks they pose to health, safety, and fundamental rights [115].

Besides the prohibited AI practices which must, in all cases, be observed by AI providers,[10] the risk-based approach relies on AI systems' capabilities and intended purposes to modulate the set of requirements that must be

[7] As explained on p. 10.

[8] An AI system is understood as '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 inputs it receives, how to generate outputs* such as *predictions, content, recommendations or recommendations* that *can influence physical or virtual environments*' (emphasis added on the seven criteria of the legal definition). See art. 3(1) of Regulation (EU) 2024/1689. On the seven criteria see the development below.

[9] A general-purpose AI model is defined in article 3(63) of Regulation (EU) 2024/1689 as 'an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market'.

[10] The prohibited practices are not reviewed in detail herein. These refer to the placing on the market, the putting into service and use of AI systems that are deemed to pose unacceptable risks by the legislator, including AI enabled manipulation and exploitation, social scoring, individual risk assessment and prediction of criminal offences, untargeted scraping of facial images, biometric categorization for certain 'sensitive' characteristics, and the use of real-time remote biometric identification systems for law enforcement purposes, emotion recognition. Note that AI practices prohibited under other Union laws also apply. See article 5 of Regulation (EU) 2024/1689.

implemented by AI providers[11]. For that purpose, the Act sets out classification rules to identify high-risk AI systems and GPAI models with systemic risks and designates AI systems presenting specific transparency risks. This means that the Act establishes distinct legal requirements for high-risk AI systems, AI systems interacting with individuals or generating content, GPAI models and GPAI models posing systemic risks (See Table 6.2)[12]. The Act also foresees the possibility for providers of low-risk AI systems to comply with all or parts of the requirements applicable to high-risk AI systems on a voluntary basis.

Table 6.2 Concise overview of the main design requirements imposed by the Artificial Intelligence Act

High-risk AI systems.	**Transparency requirements for AI systems interacting with individuals or generating content.**	**GPAI models.**	**GPAI models posing systemic risks.**
• Risk management system. • Data and data governance. • Technical documentation. • Record keeping. • Transparency. • Human oversight. • Accuracy, robustness and cybersecurity. • Quality management system.	• Provision of information to natural persons interacting with the AI system. • Marking in a machine-readable format and detectability of the system's output as artificially generated or manipulated.	• Technical documentation. • No other specific technical requirement.	• Technical documentation. • Model evaluation following state-of-the-art standardized protocols and tools, including adversarial testing of the model. • Mitigation of possible systemic risks stemming from the development, the placing on the market or the use of the model. • Tracking, documentation and reporting of serious incidents and possible corrective measures. • Adequate level of cybersecurity protection for the model and its physical infrastructure.

[11] Other risk categories are delineated in articles 6, 50, 51, 95 and Annex III and XIII of Regulation (EU) 2024/1689.

[12] For the precise formulation of these requirements, see articles 9-15, 17, 50, 53, and 55 of Regulation (EU) 2024/1689.

The Artificial Intelligence Act's implementation is, at the time of writing, still ongoing[13]. The European Commission recently published official guidelines on the definition of AI systems and prohibited AI practices [117, 118]. On the legal definition of "AI systems", the Commission has clarified that it "should not be applied mechanically" and, instead, consider the specific characteristics of each system. This assessment must, therefore, examine all the criteria set out in the definition and ascertain whether the considered system display these elements at the pre-deployment or the post-deployment phases, without the need to demonstrate that they persist across both phases. The criteria of adaptiveness (i.e., self-learning capabilities) is, however, "facultative and thus not a decisive condition for determining whether the system qualifies as an AI system" [117][14].

The Commission also provided clarifications on systems falling outside the scope of the definition. This concerns systems that "have the capacity to infer in a narrow manner" but have "limited capacity to analyse patterns and adjust autonomously their outputs". This refers to (i) systems for improving mathematical optimization, (ii) basic data processing, (iii) systems based on classical heuristics, and (iv) simple prediction systems [117][15].

Future implementation efforts by the European Commission include the development of guidelines on the requirements applicable to high-risk AI systems and transparency obligations for certain AI systems. Other ongoing initiatives for the implementation of the Act include (i) the development of harmonised standards addressing the requirements applicable to high-risk AI systems by CEN-CENELEC [119], and (ii) the development by the AI Office of a code of practice for providers of GPAI models and GPAI models with systemic risk [120][16].

The Artificial Intelligence Act sets out a general framework for AI systems and GPAI models and leaves its technical implementation to AI providers. In turn, the text does not address the specificities of edge AI

[13] The AIA will apply from 2 August 2026, with particular timelines for the application of certain provisions including, for example, prohibited AI practices which are in force since the 2 February 2025, General-Purpose AI Models (2 August 2025), and high-risk AI systems (2 August 2027).

[14] On pp. 1, 2, and 4.

[15] On pp. 8-10.

[16] Both initiatives are, at the time of writing, still ongoing and therefore not detailed here. On CEN-CENELEC's mandate, see the developments on pp. 113 et sq. below. The final version of the code of practice for GPAI models was published on 10 July 2025 and has yet to be assessed by Member States and the Commission. It is available at <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>.

systems and models in detail. This means that several legal assessments must be carried out on a case-by-case basis, including (i) the applicability of both the Act and the definitions of AI systems and GPAI models, and (ii) an assessment of the intended purpose of edge AI systems and the capabilities of GPAI models deployed at the edge for the purpose of ascertaining applicable risk classifications and requirements. Further reflection on the implementation of the Act's requirements is needed, considering the specificities of edge AI systems, such as their decentralized architectures, proximity to data sources and real-time decision making, as well as the use of local data for training purposes.

6.3 Data Act - Regulation (EU) 2023/2854

Regulation (EU) 2023/2854 ("Data Act") will set rules on access to certain IoT data and the sharing of private sector data and will define technical and organisational requirements for these operations in Business-to-Consumer ("B2C") and Business-to-Business ("B2B") contexts [121][17]. In particular, the regulation will secure and provide a framework for the exercise of user rights to access and share their data on the performance, use and environment of connected products and related services[18].

Users of connected products must be able to access their data, either directly from the connected product or indirectly by a simple request to the data holder. Users are also entitled to request from the data holder the sharing of their data to a third party of their choice, provided that the recipient does not qualify as a "gatekeeper"[19]. For these purposes, the Data Act defines the manner in which the data must be made available to users and data recipients,

[17] This refers to Chapter II and III of the Data Act. Other chapters and provisions are not examined in detail, including the conditions for data sharing in Business-to-Government ('B2G') contexts.

[18] This refers to 'product data' and 'related service data' defined, respectively, in articles 2(15) and 2(16) of Regulation (EU) 2023/2854 as 'data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer' and 'data representing the digitisation of user actions or of events related to the connected product, recorded intentionally by the user or generated as a by-product of the user's action during the provision of a related service by the provider'.

[19] A 'gatekeeper' is defined as an 'undertaking providing core platform services' that has a significant market impact, provides a core platform service enabling business users to reach end users, and enjoys an entrenched and durable market position. Gatekeepers are designated

Table 6.3 Concise overview of the main requirements relating to data access and sharing imposed by the Data Act

Accessibility	Format and Quality
• User access by design and by default and, where technically feasible, directly from the connected product. • User and data recipient access must be provided in an easy and secure manner, and free of charge. • The data holder must make data accessible to the user or data recipient without undue delay and, where relevant and technically feasible, in a continuous manner and in real-time.	• Users and data recipients must receive product data and related service data or readily available data, as well as the metadata relevant for their interpretation and use. • The data must be made available in a comprehensive, structured, commonly used, and machinereadable format. • Where the data is accessed from the data holder, it must be of the same quality as is available to the data holder.

as well as requirements on data quality and format that apply regardless of the party concerned (i.e., user and data recipient) and the type of user access (i.e., direct or indirect) (see Table 6.3)[20].

The Data Act entered into force on 11 January 2024 and will become applicable on 12 September 2025[21]. It is important to note that the user, in the sense of the Data Act, is not necessarily the data subject. Where such is the case, the data holder and the data recipients must comply with data protection laws. The data holder is, furthermore, subject to the safeguards of the ePrivacy Directive when applicable [121][22]. Further reflexion on the application of the Data Act and its relation to the abovementioned Union laws could be useful for manufacturers and users of edge AI systems.

6.4 Cyber Resilience Act - Regulation (EU) 2024/2847

Regulation (EU) 2024/2847 ("Cyber Resilience Act") imposes horizontal cybersecurity requirements for all products with digital elements made available on the market [123][23]. The concept of products with digital elements[24]

by the European Commission and include, at the time of writing, Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft [122].

[20] For the precise formulation of these requirements, see articles 3(1), 4(1), 5(1), 5(3) and 11 of Regulation (EU) 2023/2854.

[21] Note that the Act foresees a particular timeline for certain products, services, and contracts.

[22] As stated in articles 4(12), 5(7), and 6(1) of Regulation (EU) 2023/2854.

[23] For a detailed review of the Cyber Resilience Act, see [124].

[24] A product with digital elements is defined under article 3(1) of Regulation (EU) 2024/2847 as 'a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately'.

includes AI systems regardless of the risks they pose. Product manufacturers will be responsible for the implementation of security requirements as well as vulnerability handling processes that remain effective throughout products support period (Table 6.4)[25]. The implementation of these requirements is subject to a cybersecurity risk assessment which, for AI systems, shall additionally examine risks and vulnerabilities specific to AI systems.

Table 6.4 Concise overview of the essential cybersecurity requirements imposed by the Cyber Resilience Act

Security requirements	Vulnerability handling requirements
• Design, development and production of products with digital elements in a way that ensures an appropriate level of cybersecurity based on the risks. • Absence of known exploitable vulnerabilities. • Secure by default configuration. • Security updates addressing vulnerabilities and corresponding user controls and settings. • Protection from unauthorised access by appropriate control mechanisms. • Protection of the confidentiality of the processed data. • Protection of the integrity of the processed data. • Data minimisation. • Protection of the availability of essential and basic functions, also after an incident. • Minimisation of the negative impact on the availability of services provided by other devices or networks. • Reduction of the impact of incidents through design, development and production measures. • Provision of security related information to the user. • User controls enabling the secure and permanent removal of all data and settings and, where applicable, their secure portability to other products or systems.	• Identification and documentation of vulnerabilities and components contained in products. • Addressing and remediating vulnerabilities without delay. • Application of effective and regular tests and reviews of the productâĂŹs security. • Sharing and public disclosure of information on fixed vulnerabilities. • Implementation and enforcement of a policy on coordinated vulnerability disclosure. • Measures facilitating the sharing of information about potential vulnerabilities in products and third-party components contained therein. • Mechanisms for the secure distribution of updates. • Requirements on the dissemination of security updates.

The Cyber Resilience Act entered into force on 10 December 2024 but is not yet applicable[26] and, for this reason, no guidance has been issued by the European Commission at the time of writing. The Commission will have the

[25] For the precise formulation of these requirements, see articles 6, 13 and Annex I of Regulation (EU) 2024/2847.

[26] The Act will apply from 11 December 2027, except for manufacturers' reporting obligations concerning actively exploited vulnerabilities and severe incidents having an impact on products' security to Computer Security Incident Responses Teams designated as coordinator

opportunity to provide guidance to manufacturers subject to the simultaneous application of the Cyber Resilience Act and other Union legislation. In that regard, guidance on the interplay between this Act and the Artificial Intelligence Act could be useful also for manufacturers of edge AI systems.

---

at national level and the European Union Agency for Cybersecurity through the future single reporting platform.