GLOBAL LEGAL INSIGHTS

AI, Machine Learning & Big Data 2024

Sixth Edition

Contributing Editor:

Charles Kerrigan

CMS Cameron McKenna Nabarro Olswang LLP

glg Global Legal Group

CONTENTS

Germany

Moritz Mehner, Martin Böttger & Christoph Krück
SKW Schwarz

Trends

In 2024, it is expected that artificial intelligence (AI) and Big Data will continue to develop rapidly. Significant progress has already been made in recent years in areas such as natural language processing, machine vision and machine learning (ML).

Specifically, the language models field, where human-like texts are generated from extensive language data, was profoundly influenced by ChatGPT's proliferation in 2023. It is expected to remain a highly competitive field in the 2024 AI market. ChatGPT not only led to significant technological progress, but also propelled AI into a mainstream topic for the first time. The diverse fields of application are increasingly coming into focus, with the result that one in three large companies in Germany has now integrated AI into their daily business processes. And the trend is still rising. Although ChatGPT has a leading position in the field of AI language models, a significant change in the market situation with considerably more competition between the various AI models is expected in 2024.

In December 2023, for example, Google launched the AI "Gemini", which is already delivering impressive results. This year, however, particular attention should be paid to the use of open-source models. With the release of its AI Llama as an open-source model, Meta has taken a significant step that could have a fundamental impact on the development of AI technology. This enables small development studios and start-ups to build on a big player's platform and develop powerful AIs themselves. A prime example of the potential of open-source AI is the French start-up Mistral, which developed an AI model based on Llama in just nine months that even surpasses ChatGPT in some areas. This example shows that the AI landscape is in a state of upheaval. In Germany alone, there are over 500 AI start-ups. It is therefore to be expected that these AI start-ups will play an important role in further shaping the market and helping Germany and the EU become established as AI locations.

In addition, the use of Big Data analysis will continue to be a growing trend in 2024. With advancing AI models and ML algorithms, it is possible for the first time to utilise the enormous amount of data available in a meaningful way. It is therefore not surprising that an increasing number of companies are leveraging the advantages of Big Data and ML.

However, with such rapidly developing technology, concerns about the potential risks and ethical implications are also increasing. In particular, there is a risk of biased decisions being automated or AI being used to create fake news and propaganda. At the same time, open-source models, for example, offer the possibility of transparent development, which means that high security standards can be guaranteed. Nevertheless, it remains essential that a legal framework is created to contain the risks without jeopardising the great opportunities offered by technology. The German government is focusing on a balance

between innovation and safety, with the aim of promoting trustworthy AI "Made in Europe". An initial framework has already been created with the EU AI Act, which points the way forward in terms of both innovation and the regulation of risks. Nevertheless, this is only the first step. Further regulations remain essential in order to keep pace with the constant development of the technology.

Ownership/protection

Big Data

In principle, the German legal system does not know a legal ownership of data itself. In the final report of their conference in 2017, the German Minister of Justice of all 16 German states explicitly denied such an ownership right or the economical need of such a right to data itself; the current legal provisions are considered effective to meet the industries' interests and requirements.

The German legal system offers a multilayered framework of legal provisions under which data, access to data or the integrity of data may be protected:

Intellectual property rights

In principle, whether or not data may be protected under German copyright law solely depends on the content of the respective data. For the protection of data, regardless of its content as a copyrighted work, the mandatorily required act of intellectual creation by a natural person within the meaning of the German Copyright Act (*UrhG*) is regularly absent due to its characteristic being the result or intermediate state of a machine process. Insofar as the content of the corresponding data constitutes a copyrighted work within the meaning of the UrhG, the content itself will be fully protected accordingly.

As a result of the implementation of the European Directive RL 96/9/EC, database works are protected under copyright under Section 4 UrhG, as well as the database creator under Sections 87a *et seq*. UrhG with a right of protection *sui generis*. The creation of a database work also requires a personal intellectual creation which manifests in the systematic or methodical arrangement of the data as the database. The decisive factor in the creation is the conception of the selection and linking of the data. A systematic/methodical arrangement of data that is decisively determined or specified by an algorithm or other software will regularly fail to be an intellectual creation by a natural person. In principle, the arrangement can be executed by a "machine", without precluding the possibility of a personal intellectual creation.

A similar case-by-case consideration is also necessary in the case of the *sui generis* property right of the database creator under Section 87a *et seq*. UrhG. This is primarily a right for the protection of investment. The creator of a database who makes a substantial investment in the creation or maintenance of the database is granted the exclusive right to reproduce, distribute and publicly display the database in its entirety or a substantial part thereof, pursuant to Section 87b UrhG. A personal act of intellectual creation is thus not required. Consequently, it is not the individual case of intellectual creation by a natural person that needs evaluation, but rather the existence of a substantial investment. As a rule, one can also assume with regard to Section 87a *et seq*. UrhG in the case of machine-generated data that this usually represents a standardised by-product of the actual operation of the machine or software rather than a specific investment for the creation of a database.

In addition to this specific copyright content of data, it regularly may also contain names, company designations, trademarks, logos and likenesses of personalities and be of commercial value. Therefore, the requirements and prerequisites of trademark law, name law (Section 12

of the German Civil Code (*BGB*) is also regularly applicable to aliases and pseudonyms) and personal rights must always be observed when (commercially) exploiting data. However, this regularly does not play a role in the possibility to protect data, but rather plays a considerable role in the commercial exploitation by the respective party exploiting the data.

Lastly, ownership rights of course exist regarding the physical storage device/facility that empowers the owner respectively. However, this only relates to the physical items and facilities and not the data contained therein.

Legal access and/or integrity protection

The central provisions in the German Criminal Code (*StGB*) are Sections 202a, 202b, 202c and 202d StGB (data access protection), as well as Section 303a StGB (data integrity protection) regarding the protection of databases. According to the legal general opinion, these are considered protective laws within the meaning of Section 823 (2) BGB and can therefore also give rise to claims under civil law against third parties.

Section 202a StGB makes it a criminal offence to obtain unauthorised access for oneself or another to data that has been specially secured against unauthorised access, by bypassing the access security. Section 202a StGB thus requires special security against unauthorised access – technical and organisational measures to protect data thus play an important role as elementary prerequisites for its legal protection (this is also the case in the German Business Secret Act (*GeschGehG*)). This usually excludes a large number of the relevant cases where a person from within a company, who regularly handles the relevant data, "leaks" the data or passes it on "under the table" to third parties or provides them with access.

Section 303a StGB protects the integrity of data against deletion, rendering unusable, suppression and modification – not only in the stored state, but also during transmission of the data. Interference is only punishable if it is unlawful. This is already the case if there is unlawful interference with another's right, such as a right of disposal or possession.

The GeschGehG, introduced in 2019, may also grant protective rights to certain data. The GeschGehG mainly protects business secrets against unauthorised access, use and/or disclosure. Data may be considered a business secret, if (as per the mandatory requirements) the information contained in the data is not publicly known and thereby has an economic value, is protected in its secrecy by appropriate technical and organisational measures and a legitimate interest in keeping it secret is shown. To fulfil these requirements and enable respective protection under the GeschGehG, entities are usually required to have a cohesive policy in place to appropriately protect business secrets from an operational as well as legal perspective.

Next to this legal framework provided under German laws, a key legal instrument in successfully protecting and simultaneously exploiting data is the correct use of contractual agreements. While such contractual relationships regularly only have a legal effect between the contracting parties, they should cover the complete value chain of the data to be exploited and make sure to meet the legal requirements to grant the protection as outlined above.

Reliable data business therefore depends on the overall effective legal framework and internal compliance policy.

Lastly, EU regulation also introduced an allowance for text and data mining in Section 44b UrhG. Text and data mining is understood as the automated analysis of single or multiple digital or digitised works to extract information, particularly about patterns, trends and correlations. Reproductions of lawfully accessible works for such text and data mining are permitted. An owner may reserve his rights to exclude his copyrighted works from such lawful text and data mining (i.e., with a digital watermark); such a reservation needs to be machine-readable.

AI

AI applications are, by their nature, regularly protected as software under Section 69a *et. seq*. UrhG. Preparatory design work leading up to the development will also be protected; however, ideas and principles will not be. Protection under a software patent may be considered, in case the software is firmly connected to a specific technical or mechanical feature or process.

On the other hand, as with machine-generated databanks above, any works that are generated by an AI application will regularly lack the necessary act of intellectual creation by a human being to be considered a copyright-protected work under the UrhG – often regardless of the human effort giving direction for the AI application through prompting. There are, however, situations imaginable in which a human being creates copyright-protected work with the help of an AI application. It will come down to the individual case and the assessment of whether the respective process can still be considered an act of intellectual creation under the control by a human being (but only) with the help of an AI application, or if the human actions are not detrimental enough for the final outcome. As a general rule, the results – meaning generated works – of AI applications will not be protected under copyright law in Germany. Therefore, there is also no comparable ownership right to these generated works. Contractual exploitation remains possible.

While the result of AI applications will regularly not be protected under German copyright laws, the training of the AI application with existing copyright-protected works may very well constitute an infringement of the respective author's copyright. Also, Section 44b UrhG for text and data mining may apply, depending on the individual case – see above.

The upcoming European AI Act primarily governs compliance of AI applications themselves, without significantly affecting the ownership regime regarding AI applications and/or their outcomes.

Antitrust/competition laws

AI & Big Data in competition law

German competition law may come into play if scraping technology is used for the respective learning processes. Scraping can, under specific circumstances, constitute a so-called "targeted obstruction" of a competitor pursuant to Section 4 no. 4 of the German Act against Unfair Commercial Practices (*UWG*). However, a breach of terms and conditions of a website does not suffice alone according to the case law of the German Federal Court of Justice (*BGH*). A "targeted obstruction" additionally requires that security measures are being circumvented against the will of the creator, respectively, the provider of the content or database (e.g., through automatic circumvention of a "Captcha-Tool"). Thus, whether security measures are circumvented will have to be assessed based on the specific scraping technology. In case of a breach of the UWG, the creator of the protected material has the right to a cease-and-desist claim and claims for damages.

AI & Big Data in antitrust law

Antitrust law in Germany is governed by the German Competition Act (*GWB*). Establishing a market dominance under Section 18 GWB cannot simply be based on market shares or "data power" in case of Big Data or digital platforms. As part of recent reforms, additional factors for the assessment were included in Section 18 GWB, *inter alia*, direct and indirect network effects, access to competition-relevant data and the principle that the assumption of a market shall not be invalidated by the fact that a good or service is provided free of charge (i.e., in case the service is "only" paid with personal data).

Section 19 GWB prohibits the abuse of a dominant position. The "essential facilities doctrine" forms one group of cases in the context of the so-called refusal of business. This concerns cases in which companies control access to information, services or infrastructure and thereby prevent access for other competitors in order to improve their own market position.

It is being discussed whether the mass amounts of data held by large Internet companies should be classified as such an "essential facility". However, the European Court of Justice requires "exceptional circumstances" as a prerequisite for access, and other arguments speak against this; in the case of personal data, data protection law itself can be a barrier, since personal data cannot be transferred to competitors in general without the consent of the data subject.

Board of directors/governance

General

In connection with the handling of Big Data and AI, managing directors and members of a management board (in the following referred to as "directors") must take appropriate measures to ensure that the public law regulations applicable to their company are observed. Since the EU AI Regulation will come into force shortly, most likely before summer 2024, directors now have the obligation to review whether and what type of AI their company uses and to what extent an update of corporate governance and compliance systems is required.

Besides the AI Regulation, directors will have to comply with and closely observe the development of, *inter alia*, the following legal areas:

- The Data Act (Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data).
- The Data Governance Act (Regulation (EU) 2022/868 on European data governance).
- The AI Act (Proposal of an EU directive on non-contractual civil liability rules to AI).
- The GDPR (EU data protection regulation (EU) 2016/679).
- The GeschGehG for the protection of trade secrets.
- Sector-specific laws such as Section 75c of the German Fifth Social Code (*SGB V*) (hospital sector), German Federal Office for Information Security Act (*BSIG*) (for providers of critical infrastructure) and at a European level DORA (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations) (a regulation on resilience against cyber risks for financial companies).

General director duties

Due to the quick and rather unforeseeable technical development, the new area of "responsible AI", as outlined in the AI Regulation, will become increasingly important, particularly for a company director. Directors across all business sectors and industries will have to comply with the "AI Regulation".

For the handling of the legal requirements set out under the AI Regulation and the other aforementioned legal provisions, the directors' personal due diligence obligations as a manager are governed by applicable corporate laws and internal corporate governance rules. The admissible ratio between entrepreneurial risks and opportunities of a company also applies to the handling of Big Data and AI, and the technical and legal risks discernible in these areas.

As a rule, directors have to act with the care of a prudent and diligent businessman (*cf.*, for example, Section 43 of the German Limited Liability Companies Act (*GmbHG*) and Section 93 of the German Stock Corporation Act (*AktG*)). This means the directors have to act

diligently themselves and monitor the behaviour of the company's employees. In addition, directors also have a general compliance duty. This means that suitable organisational measures must be taken to avoid liability and control risk in the event of a potential risk.

Accordingly, measures taken by the management are generally at the director's reasonable discretion. A central aspect in this context is the so-called business judgment rule, which is codified in the AktG, but is correspondingly also applicable to other types of companies. According to this rule, the manager is acting diligently if, when making an entrepreneurial decision, he or she could reasonably assume to be acting for the company's benefit on the basis of appropriate information.

In this context, for the area of AI, it is critical that the director in his or her organisation ensures that the limited capabilities of AI are realistically assessed, the scope of application is clearly defined, intellectual property and privacy laws are complied with, and the results delivered by AI are subject to critical and constant human monitoring and review. In the current state of the art, the director cannot readily rely on the results provided by any AI systems, as those results are fundamentally based on statistical considerations rather than on a thorough assessment of the individual circumstances.

AI compliance systems

Legal regulations and developments

With the Data Act, the AI Regulation and other statutes coming into force shortly, the director must generally set up a compliance system – or review and modify an existing one – that enables the company to avoid and control legal and business risks.

The directors (themselves and through suitable employees) must identify and take measures to prevent IT and digital risks, e.g., by installing defensive devices, restricted access rights and access controls, shut-down mechanisms and by applying the need-to-know principle or taking other adequate special precautions. Such devices or mechanisms must be incorporated into a legal set of rules (so-called (IT) compliance guidelines) that must be brought to the workforce's attention and represent a binding work instruction.

In the area of Responsible AI, the AI Regulations safety, conduct, documentation and transparency obligations, risk-management requirements and sanction options for the authorities must be observed. In the area of the Data Act, the information rights of customers (users) and corresponding organisational and technical obligations of manufacturers and service providers must be complied with.

Companies must be aware that responsibility for a violation of AI, Big Data or other IT compliance legislation can fall on the company itself as well as the responsible managers and – with appropriate delegation – compliance officers. Attention must be paid to this within the framework of the rules of procedure, employment contracts and instructions to executives entrusted with corresponding tasks. Directors' and Officers' (D&O) insurance policies should also be checked to ensure that they include the relevant activities and persons involved.

In the following, we provide a brief overview of the regulatory responsibility and liability of the company, managing director and compliance officer in the event of a breach of the general legal compliance obligation, in particular in relation to AI systems.

Regulatory liability in general

Violations of the legal requirements set out in particular legal statutes such as the Data Act or the AI Regulation may directly constitute an administrative offence (*cf.*, e.g., Art. 40 Data

Act which, however, leaves the definition of details of fines to the Member States or *cf*., e.g., Art. 71 paras 3 and 4 AI Regulation, which already sets out a corridor for fines up to EUR 30 million or 6% of the company's global turnover in the previous year).

In addition, even if there is no specific breach of regulations, under German law, the mere failure to take appropriate supervisory measures or the complete lack of a suitable compliance system, including for AI systems, can constitute an administrative offence which is punishable by a fine of up to EUR 1 million (Section 130 German Act on Offences (*OwiG*)).

Personal liability

Even though further details of the fines applying under the Data Act and the AI Regulation have yet to be defined by the Member States, in principle it should be assumed that such fines may be imposed on the persons involved and on the company itself.

Since in terms of fines the European regulations are still in flux, we hereinafter focus on the existing German status law.

Under already existing German administrative offence laws, a liability for fines generally applies to the "business owner", i.e., the directors, managing directors and other persons specified by the company (Section 130 OwiG). However, a fine can also be imposed on the company for which the compliance officer works (so-called "association fine", Section 30 OwiG). Finally, the compliance officer of a company can also be held directly liable for an offence, even if he or she works as a (managerial) employee.

Delegation to compliance officers

Under existing German law, a "delegation" of legal responsibility (and thus partial exoneration of the manager under administrative offences law) is possible under the following conditions (*cf*., Section 9 (2) sentence 1 no. 2 OwiG):

The delegation is given to persons who are expressly designated by a business owner to perform the owner's tasks on their own responsibility.

The delegation can be affected vertically, i.e., by involving designated employees at subordinate levels (e.g., CSO, CCO). However, at the same time, the necessary know-how and processes for effective monitoring of employees must also be ensured horizontally (i.e., on a senior-management level), namely by adequate company (and group) by-laws for the directors/management and advisory/supervisory board.

The core task of a compliance officer is regularly the development and maintenance of a compliance structure, as well as an appropriate response to compliance violations, i.e., the compliance officer often has the task of preventing legal violations in and out of the company. Since it is unanimously agreed that compliance is a necessary component of good corporate governance today, the compliance officer can be expressly assigned this task within the meaning of Section 9 (2) sentence 1 no. 2 OwiG.

An effective delegation is dependent on two prerequisites. Firstly, the compliance officer must be given an unambiguous understanding that he or she will be responsible for performing a specific area of responsibility in the future; whether this is actually the case must be clarified on the basis of the overall circumstances, whereby in particular the job advertisement, the employment contract or internal guidelines must be taken into account. Secondly, the compliance officer must be able to carry out his or her duties independently (*cf*., Section 9 (2) sentence 1 no. 2 OwiG).

Accordingly, at least the compliance officer with the corresponding level of authority will be an effective "delegate" in the meaning of Section 9 (2) sentence 1 no. 2 OwiG and is therefore to be regarded as legally responsible within the meaning of Section 130 OwiG.

If the compliance officer is hired and works as an employee, he or she generally falls within the personal scope of limited employee liability, i.e., his or her special task does not lead to an exclusion of the liability privilege. However, it should be noted that according to German case law, the limitation of liability only applies in the area of slightest negligence anyway, i.e., in the case of medium and gross negligence, the compliance officer may also be personally liable as an employee, whereby German case law has so far set a liability limit of no more than one year's salary.

Directors (and compliance officers) will need to be particularly critical of whether insurance policies in place cover the company's Big Data and AI activities. This applies in particular to D&O insurance policies. It is therefore recommended to discuss the director's measures and the company's compliance system with the insurance company when using or distributing Big Data or AI products.

In any event, it is clear and important to note that – still – a complete delegation of business decisions to AI systems is currently not legally permitted.

Selection and monitoring

If the AI responsibility is effectively delegated to the compliance officer, the responsibility of the managing director is reduced to the proper selection (initial), training and monitoring of the compliance officer, if necessary. This means that the managing director must receive regular reports on compliance with the legal requirements and the compliance officer's risk assessment, e.g., on sufficient AI competence in the company's operational environment ("AI literacy"; *cf*., Art. 4b AI Regulation) and on the important delimitation of the special (supervisory) obligations for the use of high-risk AI (*cf*., Art. 29 of AI Regulation).

In particular, responsible compliance officers and business managers must follow the ongoing discussion (and, if necessary, adapt their compliance system to changes) as to the extent to which AI itself can contribute to legally binding declarations and agreements and whether misconduct by AI systems, especially in the area of tortious liability, always requires an attribution to the user or manufacturer or whether the AI itself can also trigger a liability consequence under certain circumstances.

If the director violates his or her supervisory duties, he or she may be subject to personal liability claims for damages incurred by the company, directly or through claims raised by third parties. As indicated above, in the case of administrative offences within the company, a director may be personally responsible – regardless of his or her own fault (and can even be personally fined) – if there is no proper compliance system in place or if, for example, the measures pursuant to Art. 32 GDPR are not sufficiently implemented (*cf*., Section 130 OwiG).

Whether the breach of the general compliance obligation (Section 130 OwiG) of those responsible can also result in tort liability for the persons involved has not yet been clarified by the courts and is still controversially discussed in German legal literature. However, this cannot be ruled out in the case of specific regulatory provisions of the AI Regulation (depending on their respective rationale). It remains to be seen how German or European case law will develop on this issue. In terms of liability for the AI Liability Regulation, which to date is still in draft version, this will need to be considered.

AI and Big Data legal due diligence

The requirements for legal compliance of a company and its representatives in terms of Big Data and AI also need to be reflected in the scope of any due diligence review in possibly AI-related M&A transactions, not only in terms of a target company producing or distributing AI technology, but also in terms of any target that is using Big Data or AI technology.

In the course of due diligence, a prospective buyer may have to review and assess, *inter alia*, the following considerations:

- List and describe (i) data management and AI (including generative AI) software and applications produced, distributed or used by the target, (ii) any type of data, (iii) sources and processes used to train the AI, and (iv) persons inside and outside the target's organisation involved in this area.
- List and describe any security processes (access controls, etc.), malfunctions, errors and data security issues involving Big Data or AI products used or distributed by the target.
- Describe compliance systems in place and explain if and to what extent the system is regarded customary in the market and geared towards the use of Data Governance and AI.
- Describe any processes inside the target by which the Data Act, AI Regulation, GDPR and other public regulations are complied with in their relevant applicable versions when working with Big Data and AI software/applications.
- State any regulatory or civil liability risks alleged by third parties or in any other way discernible to the target's management, including from internal documents or reports.
- Is the D&O insurance sufficient for the area of Data Governance or AI-related legal compliance and is the insurer sufficiently (and currently) informed about the company's field of activity and (maybe limited) compliance processes?

Regulations/government intervention

Big Data

There is no regulation of "Big Data" as such. Since GDPR in particular is becoming relevant as a legal framework, it can be helpful to structure a Big Data project into the following phases: (1) data collection; (2) data storage; and (3) data analysis.

Under the GDPR regime, data collection, storage and analysis are subject to regulation only to the extent that personal data is involved. Regarding non-personal data besides contractual commitments, the upcoming regulation on harmonised rules on fair access to and use of data (Data Act), which will become applicable most likely in September 2025 in the EU, could become relevant as well.

In the context of Big Data, the general processing principles resulting in Art. 5 GDPR could become rather relevant, especially the principles of purpose limitation (Art. 5(1) lit. b GDPR), data minimisation (Art. 5(1) lit. c GDPR) and storage limitation (Art. 5(1) lit. e GDPR). Provided that as a legal basis consent should apply (Art. 6(1) lit. a GDPR), the transparency requirement when obtaining consent may pose some challenges. Overall, Art. 22 GDPR, which contains rules for automated decisions and profiling, must also be taken into account.

In the area of Big Data, it is often necessary to observe sector-specific regulations and evaluations. Big Data applications are widely used in the online and advertising sector. One specific method in this area is web tracking, whereby the data obtained is used for profiling (see Art. 4 no. 4 GDPR) and targeting. This allows companies to offer their customers personalised advertising and content based on created user profiles. In the area of banking, finance and insurance, sector-specific regulations such as the Payment Services Directive (PSD2), which also contain some data protection provisions, apply in some cases. In addition, the EU Solvency II Directive and the German Insurance Supervision Act (*VAG*) may become relevant. In this sector, for example, the risk assessment of a possible payment default is carried out using Big Data applications or insurance tariffs are linked to telematics applications. Another area concerns Big Data applications in the workplace. The German Equal Treatment Act (*AGG*) can become relevant here, for example if Big Data applications are utilised in the pre-selection of applicants.

AI

On an EU legislative level there is a new legal framework regarding AI in the pipeline: the Regulation of the European Parliament and of the Council laying down harmonised rules for AI (AI Act). The regulation will most likely enter into force by April 2024. Two years after that date, the majority of the provisions will actually become applicable. However, bans provided for in the AI Act (prohibited AI systems) are expected to take effect just six months after entry into force, while the provisions on general-purpose AI models (GPAI) are expected to take effect after 12 months.

First of all, companies must address the question of whether the AI Act applies to their technologies and businesses' operations, since the scope of the AI Act is rather broad and will capture a broad spectrum of software products. Most of the extensive compliance obligations apply to *providers* of AI systems. Nevertheless, *users* of such systems also have to comply with certain obligations, in particular if they control the data input. The AI Act will also already apply to providers that place AI systems on the EU market or put them into operation in the EU, regardless of whether these providers are established in the EU, as well as to providers and users of AI systems that are established or located in a third country, if the output produced by the AI system qualifies as high risk and is used in the EU.

According to Art. 3(1) AI Act, an AI system is "a machine-based system 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". The definition was based on an OECD version. The EU hopes that this will lead to greater acceptance and coherence at an international level. According to the definition, a key characteristic that distinguishes AI systems from traditional software is that an AI system derives conclusions for the output from the input ("infers, from the input it receives, how to generate outputs"). This is intended to emphasise the ability of AI systems to derive models and/or algorithms from input data. By contrast, the EU wanted to exclude systems that are based on rules that are defined exclusively by natural persons in order to carry out automatic processes from the scope of the AI Act. By definition, the capabilities of AI systems should go beyond basic data processing operations and should rather be understood as learning, reasoning or modelling. In any case, AI systems include GPAI and their respective basic models, which form the basis for generative-AI applications such as ChatGPT.

The AI Act classifies AI according to the risk associated with its use and human interaction. AI systems that pose an unacceptable risk are prohibited. On the other hand, high-risk AI systems are subject to strict compliance requirements, while AI systems with limited risk face less regulation. However, these are subject to specific transparency obligations. Only the general AI principles apply to AI systems with a minimal risk. GPAI is treated as a special category that is not necessarily a high-risk AI system but is subject to stricter requirements in terms of data management, technical documentation instructions for use and the publication of a summary of the content used for training.

Prohibited AI systems are classified as manipulative or exploitative practices, exploitation of a person's vulnerabilities, biometric categorisation systems, social scoring, facial recognition from social media or video recordings, facial image scraping and emotion recognition in the workplace, and real-time remote biometric identification for law enforcement purposes.

High-risk AI systems are such systems that have a significant detrimental impact on the health, safety and fundamental rights of individuals in the EU. This can either be a security component or product falling under Annex 2 of the AI Act that is subject to a conformity

assessment or specific AI systems used for one of the use cases listed in Annex 3 of the AI Regulation (e.g., biometric identification, emotional recognition and categorisation of individuals, general education, personnel management and employment, access to essential private and public services or goods).

The compliance obligations for providers of high-risk AI systems are rather comprehensive: among other things, they must conduct an assessment of fundamental rights' impact and conformity; enrol their system into the public EU database for high-risk AI; establish risk and quality management systems; conduct governance of their data and input (i.a., bias mitigation, representative training data); comply with transparency obligations (e.g., instructions for use, technical documentation); include human oversight; and ensure accuracy, robustness and cybersecurity (e.g., through testing and monitoring).

Member States are required to lay down rules for sanctions in the event of violations of the AI Act, whereby violations of the unauthorised use of AI systems can be punished with fines of up to EUR 35 million or 7% of the total global annual turnover of the sanctioned company in the previous financial year.

Generative AI/foundation models

For AI models that can be used for any purpose, the general risk-based approach of the AI Act does not apply. Under the term GPAI, a further, separate category of AI systems was therefore introduced in the AI Act for which further special regulations apply. In terms of obligations, a distinction is made between GPAI systems and the models on which these systems are based. An example of this is the ChatGPT system, where the model is the GPT model. Providers of GPAI models have more extensive information and documentation obligations than the providers of AI systems. The background to this is that subsequent providers who wish to integrate a model into an AI system should be able to understand the functions and limitations of the models. The transparency requirements include the creation of technical documentation and summaries of the content used for training. For models with a so-called high systemic risk, additional measures are required, such as the obligation to carry out model evaluations which, in addition to the analysis and assessment of systemic risks, also provide for the performance of counter-tests. In the event of a serious incident, a report to the EU Commission is mandatory.

Implementation of AI/Big Data/ML into businesses

The rapid evolution of technology in recent years has propelled the integration of AI, Big Data and ML into various business sectors, including finance, healthcare and retail, among others. By leveraging these tools, companies are now able to analyse vast amounts of data, improve decision-making processes, streamline their operations and gain a competitive edge. However, as businesses embrace these technological advancements, it is crucial for them to comply with legal requirements and implement policies to minimise legal risks associated with data protection.

Possible-use cases

AI algorithms, particularly ML models, can process and analyse large amounts of data from diverse sources. When linked to Big Data, AI models can identify patterns, trends and anomalies that may be difficult or impossible for humans to detect. Possible-use cases encompass customer service with chatbots and virtual assistants, streamlining sales and marketing through data analysis or assisting human resources with recruitment, employee engagement and training. Additionally, AI bolsters fraud detection, cybersecurity and process automation, enabling businesses to focus on more complex tasks.

What companies should be aware of

In addition to legal issues surrounding ownership and protection, antitrust and competition laws, labour and data protection laws also play a role. To enable legally compliant use of new technologies, it is furthermore recommended to introduce company policies. Some key considerations when developing company policies include establishing ethical guidelines, data governance, and training and awareness.

Companies are recommended to create a set of ethical principles that guide the development and deployment of AI and ML systems, ensuring they are transparent, accountable and do not discriminate. Businesses should also implement a data governance framework that outlines the roles and responsibilities of different stakeholders in managing data assets, ensuring data quality and complying with data protection regulations. Finally, it is inevitable for companies to provide regular training and education to employees on data protection laws, ethical AI practices and the responsible use of AI, Big Data and ML.

The implementation of AI, Big Data and ML offers tremendous potential for businesses across various industries. However, it is essential to adopt a responsible approach, comply with legal requirements and implement policies that ensure ethical and transparent use of these technologies.

Discrimination and bias

In Germany, the AGG can become relevant in the employment context, e.g., with robo-recruitment or other AI systems used in the work context. The AGG aims to prevent and eliminate discrimination on the grounds of race or ethnic origin, gender, religion or belief, disability, age or sexual identity (Section 1 AGG). In order to achieve this goal, the persons protected by the law have legal claims against employers and private individuals if they violate the statutory prohibition of discrimination against them. The AGG can be applied, for example, if algorithms make discriminatory decisions during recruitment or in the employment relationship. Discriminatory decisions can be created by the general design, but above all also by the training of an AI.

Therefore, AI systems that come into use in a working context should be trained with data sets that reflect and comply as much as possible with all discriminatory aspects set by the AGG (racial or ethnic origin, gender, religion or belief, disability, age or sexual identity). Burden of proof in case of a challenge by an employee may fall back to the employer (if the employee makes a plausible indication of such discrimination) who uses AI application and ultimately by the developer or the distributor of the AI application.

Conclusion

The question of legal regulation and applicable laws depends in relation to AI and Big Data on the specific technology and the individual case. In fact, AI and Big Data should always be jointly considered when evaluating and using them in a company.

In the EU, on a regulatory level, European-wide harmonised rules are being considered (GDPR, AI Act) which is also preferable to establish a robust and effective legal framework.

As is often the case in the field of technology, the technological development will be faster than the legislation. This also means that early adopters will have to move from a legal perspective in a grey area for some time. For this reason, early consideration of the legal frameworks and installing compliance systems is particularly relevant.

Moritz Mehner
Tel: +49 89 2864 0206 / Email: m.mehner@skwschwarz.de

Moritz Mehner, transferring his many years of private enthusiasm for esport, data economy and new technologies to his professional life, focuses on the legal matters surrounding these sectors. This includes advising on and drafting of both classic and new (SaaS, Cloud, PaaS) software and licensing agreements, issues relating to ownership and copyright, regulatory requirements and commercial exploitation.

His legal work additionally concentrates on designing and implementing solutions to legal problems associated with digitising innovative business models in the fields of data economy, IoT, Blockchain and cloud computing; utilising his experience from working two-and-a-half years on the business side in the data economy before becoming a lawyer in 2018. Finally, Moritz is experienced in matters of data protection, in particular the practical application of the GDPR.

Martin Böttger
Tel: +49 89 2864 0461 / Email: m.boettger@skwschwarz.de

Dr. Martin Böttger advises on domestic and cross-border medium-sized M&A, private equity and venture capital transactions, capital markets law, corporate compliance and general corporate and commercial law issues. He specialises in the software/IT, high-tech, life sciences and sports/sports tech sectors. He regularly works on transactions in regulated industries.

His clients include international corporations, medium-sized companies, institutional and private investors as well as start-ups. Martin has supported several private-equity-financed buy-and-build platforms in their conception and implementation. He also advises software and tech companies in the areas of legal compliance, corporate governance and contract management.

In addition, Martin represents family offices, high-net-worth individuals, foundations as well as athletes, clubs and associations in the areas of financing, corporate law, asset management and sports law.

Christoph Krück
Tel: +49 89 28640268 / Email: c.krueck@skwschwarz.de

Dr. Christoph Krück specialises in IT law and digital business as well as data privacy. One focus is on advising online platforms on issues of internet and platform regulation as well as on youth, consumer and competition law. Furthermore, he advises companies on the drafting and negotiation of terms of use, general terms and conditions, licensing, SaaS, Cloud and other technology and IT contracts.

With regard to data privacy, he advises on the general requirements of the GDPR and is particularly focused on issues relating to the internet, as well as Big Data and platform structures. In addition, he closely monitors the developments concerning regulation of AI, blockchain and algorithms.

SKW Schwarz

Wittelsbacherplatz 1, 80333 Munich, Germany
Tel: +49 89 286400 / URL: www.skwschwarz.de

Global Legal Insights – AI, Machine Learning & Big Data provides analysis, insight and intelligence across 22 jurisdictions, covering:

- Ownership/protection
- Antitrust/competition laws
- Board of directors/governance
- Regulations/government intervention
- Generative AI/foundation models
- AI in the workplace
- Implementation of AI/big data/machine learning into businesses
- Civil liability
- Criminal issues
- Discrimination and bias
- National security and military

---

globallegalinsights.com

glg Global Legal Group