Oppenhoff AI Taskforce

We integrate AI systems into your business processes in a legally compliant manner.

AI systems are increasingly penetrating business processes, offering countless opportunities to increase efficiency and opening up innovative paths for sustainable growth.

This transformation does not only offer opportunities, it also raises many legal questions, for example:

- What obligations arise from the AI Act for manufacturers or users of AI applications?
- Does my AI application comply with the data protection requirements?
- What are my liability risks in the event of damage?
- Do I have to contact the works council before implementing an AI system?

Manufacturers and users of AI systems must take precautions to ensure that AI systems can be developed, trained, placed on the market, deployed and used in a legally compliant manner. The legal risks must be allocated appropriately in contracts for AI systems.

AI projects of all kinds, starting with the purchase of standard AI applications, should therefore be supported by legal experts from an early stage. This is because a non-compliant use of AI technologies can lead to considerable fines, liability risks and reputational damage.

Your AI projects: Legally compliant right from the start

The interdisciplinary Oppenhoff AI Taskforce ensures that you comply with the requirements of the EU's AI Act, as well as the many other legal requirements for AI, and can use AI systems in a legally compliant manner from the outset.

Our advisory services include

- Conducting industry-specific **AI training courses**
- Drafting and implementing an **AI company policy**, as well as introducing and negotiating shop agreements
- Developing an **AI strategy and designing contracts for AI projects**, from the purchase of AI applications to complex agile development projects
- Advising on the **data protection-compliant use of AI** in your company, in particular with regard to the processing of employee and customer data

Together, we build a bridge between technology and law – enabling your AI projects to be sustainably successful!

Oppenhoff

or scan for further information

Oppenhoff AI Taskforce

The development and use of AI raises many different legal issues
and is not limited to the EU's AI Act.

Have you thought of everything?

AI Act

Are you aware of the schedule of obligations?

The AI Act came into force on 1 August 2024. However, its provisions are applicable in stages:

- The regulations on prohibited AI practices and the obligation for companies to ensure the AI literacy of their employees have already been in force since 2 February 2025.

- Sanctions and regulations on general purpose AI models are applicable from 2 August 2025.

- Most of the requirements for high-risk AI systems will apply from 2 August 2026 and all requirements from 2 August 2027.

The aim is to make Europe a pioneer for trustworthy, safe and innovative AI. The AI Act imposes numerous obligations on providers and deployers of AI systems, depending on the risk associated with their use. The higher the risk, the stricter and more extensive the obligations. In the case of highrisk AI systems, all companies that use them are subject to strict monitoring obligations. Certain AI applications are prohibited, e.g. biometric systems, emotion recognition systems and social scoring. Consumers have the right to lodge complaints and receive informative explanations.

Violations could result in fines of up to 40 million euros or 7 percent of global turnover.

Data protection

Do your AI applications comply with the applicable data protection laws?

By their very nature, AI projects raise numerous data protection issues. This is because the development and use of AI requires the availability of large amounts of data and the processing of personal data can be relevant in all phases of the AI's development, including training and use. Furthermore, the concept of personal data is interpreted broadly. Data protection authorities are of the opinion that personal data is also processed in AI models.

Overriding legitimate interests of the providers and deployers of the AI systems often justify the respective data processing, e.g. if this is done for research and statistical purposes. Any data transfers to third countries must be justified separately.

In addition, providers and deployers of AI must fulfil the transparency and information obligations under data protection law and observe the principle of data minimisation.

Software

Do you own all the rights?

AI systems consist of software and databases and utilise data. Open source software (OSS) is often used. Against this background, companies that develop AI systems must ensure that they own all rights to the object of their development, as this is the only way they can amortise their investments and prohibit the unlawful use of their systems by third parties.

If companies use AI systems when developing software, this raises the question of who owns the rights to software codes generated by AI.

Liability under civil law

Are you aware of the special liability provisions for AI?

If damage occurs during the use of AI systems, various liability issues arise. A draft AI liability directive submitted by the European Commission has since been withdrawn, although there are still plans to issue such a liability directive. This aims to harmonise the liability regulations under civil law and will possibly contain simplified rules of representation and proof for the enforcement of claims in the injured party's favour.

Oppenhoff

Cybersecurity

Are your measures in line with EU requirements?

EU cybersecurity regulations such as the NIS 2 Directive define the legal framework throughout the EU to achieve a uniformly high level of cybersecurity. In addition, different national regulations apply under German law. Companies must implement reporting obligations for security incidents, risk management measures to combat cyberattacks and cybersecurity training for their company management, among other things.

Germany was supposed to transpose the new obligations into national law by 17 October 2024 with the NIS 2 Implementation Act [NIS-2-Umsetzungsgesetz]. This is now not expected to happen until some time in 2025. Companies now only have a narrow window of opportunity to implement the measures. AI technology can support these compliance processes - provided it is used in a legally compliant manner.

Data Act

Are you aware of the data provision requirements?

The data access and data sharing requirements set out in the Data Act are intended to increase the availability of data and break down the multitude of data silos. Among other things, data generated by networked products and connected services are to be accessible by default.

This also applies to data generated by AI implemented in devices. Large parts of the regulation will apply from 12 September 2025, and companies will have to prepare themselves for this and adapt their internal processes and products accordingly.

Intellectual property

Are your AI creations sufficiently protected?

The use of AI can lead to new challenges in the area of intellectual property, especially when it comes to the creation of works, patents, designs or brands by AI systems. Companies should protect their rights and make clear agreements on intellectual property with regard to AI developments.

This can also prevent disputes with employee inventors. At the same time, companies should clearly define which data is used for training and in the deployment of their AI systems.

World of work

Do you have employees and the works council on board?

The introduction of AI technologies is causing significant changes in the world of work. Recruiting and HR management are being supported by AI and work processes are being reorganised by AI. The demands on employees are increasing. The use of AI technology in the company requires the consent of the works council.

A timely dialogue with employees and negotiations with the works council should be initiated at an early stage in order to achieve a high level of acceptance of AI in everyday working life. At the same time, individual training concepts should be implemented to provide employees and other users with the AI literacy required under the AI Act.

Oppenhoff

Cartels

Does your AI operate within the framework of competition law?

Cartel authorities around the world are making sure that the use of AI does not lead to restrictions on competition.

AI developers and users are obliged to continuously check the functions of the programmes for any effects that might violate antitrust law. AI applications may not be misused for price or market agreements between competitors. Increased market transparency created by AI applications or the "signalling" of future market behaviour can also be problematic under competition law.

Public law / regulatory

Are there processes to minimise liability risks under public law?

AI applications can be used to fulfil obligations under public law, such as reporting and supervisory duties. However, it should be noted that the fulfilment of these duties is primarily the responsibility of the management. It also remains responsible if the AI makes mistakes.

Developers, users and deployers of AI must also be careful when it comes to foreign trade law: both software and hardware components as well as technical data that serve as the basis for AI can be relevant under export control law and therefore restricted in their handling. In addition, the sale of a German deployer or developer of AI can fall under investment screening.

Insurances

Are you using AI in compliance with regulations?

There are various innovative AI-based business models in the insurance industry. Examples include chatbots in sales and customer service, fraud prevention applications and automated underwriting, claims settlement and audit processes.

Supervisory compliance must also be taken into account if existing regulatory requirements are to be fulfilled. Insurers and intermediaries must ensure careful AI governance. Insurance companies must also adhere to the limits of permissible insurance-related activities when integrating and financing AI systems.

Company acquisitions & VC investments

Are you aware of all "bought-in" consequential risks?

Companies are increasingly trying to drive their own AI transformation through external growth. Technology start-ups and SMEs are therefore at the centre of the resurgent transaction environment. However, as the AI regulation will also apply in part to mere deployers of AI who use AI in their company, the "bought-in" consequential risks will have to be analysed in practically every M&A deal in future.

From a start-up and investor perspective, funding programmes such as the announced EU package of measures to support European start-ups and SMEs also need to be taken into consideration when developing trustworthy AI.

Oppenhoff

Oppenhoff AI Taskforce

Team

IT Law and Data Protection

Dr. Marc Hilber
Partner • Attorney
marc.hilber@oppenhoff.eu

Dr. Jürgen Hartung
Partner • Attorney
juergen.hartung@oppenhoff.eu

Valentino Halim
Junior Partner • Attorney
valentino.halim@oppenhoff.eu

Dr. Axel Grätz
Associate • Attorney
axel.graetz@oppenhoff.eu

Employment Law

Kathrin Vossen
Partner • Attorney
kathrin.vossen@oppenhoff.eu

Intellectual Property Law

Georg Lecheler
Partner • Attorney
georg.lecheler@oppenhoff.eu

Antitrust Law

Dr. Daniel Dohrn
Partner • Attorney
daniel.dohrn@oppenhoff.eu

Public Law

Mareike Heesing
Junior Partner • Attorney
mareike.heesing@oppenhoff.eu

Tax Law

Marc Krischer
Partner • Certified Tax Adviser •
Certified Public Accountant (in own
practice)
marc.krischer@oppenhoff.eu

Corporate Insurance & M&A

Anna-Catharina von Girsewald
Partner • Attorney
anna.vongirsewald@oppenhoff.eu

Oppenhoff & Partner Rechtsanwälte Steuerberater mbB
info@oppenhoff.eu · www.oppenhoff.eu

Oppenhoff