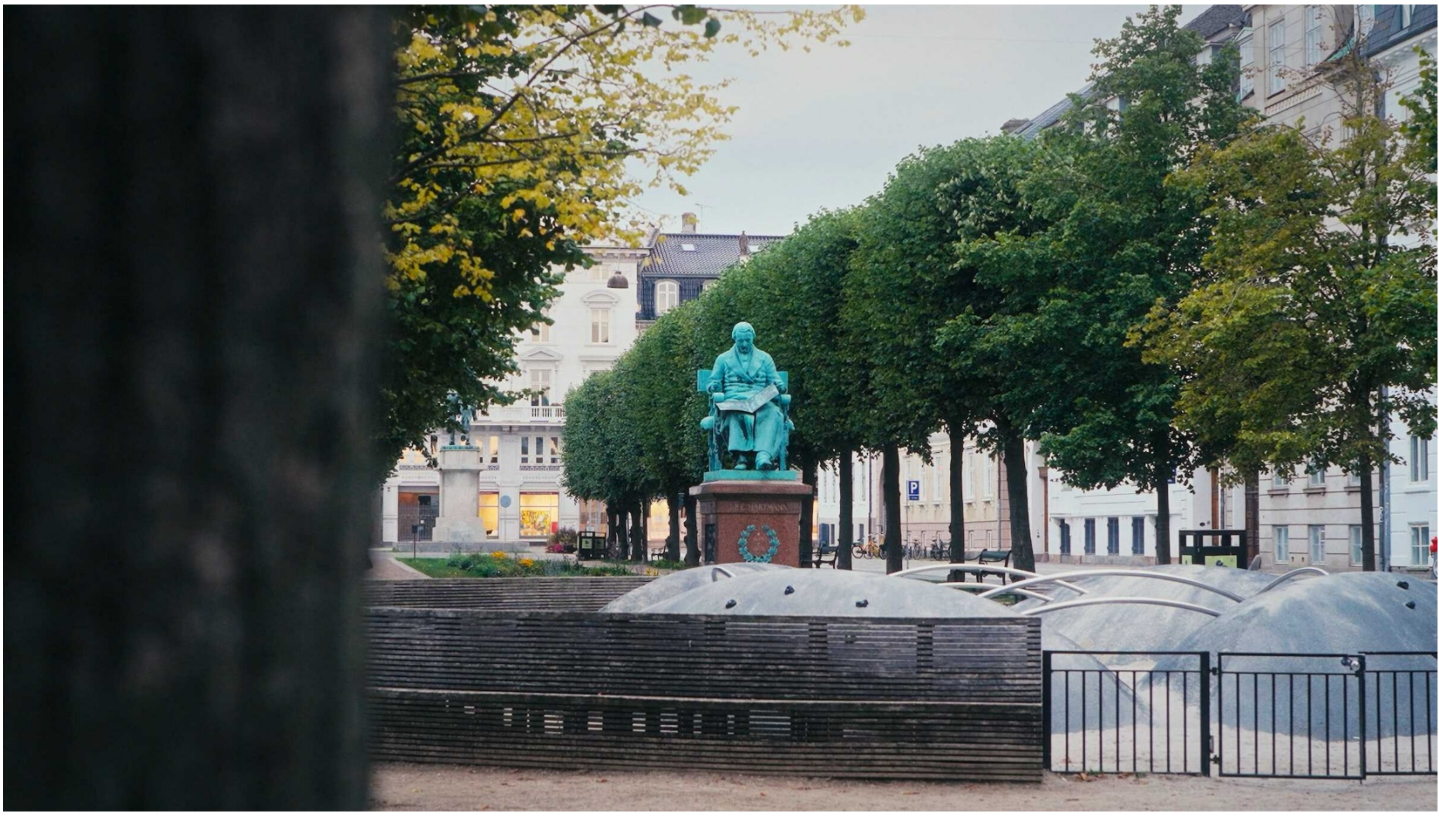
Moalem Weitemeyer

Moalem Weitemeyer
Advokatpartnerselskab
Amaliegade 3
DK-1256 Copenhagen

Tel. +45 7070 1505
moalemweitemeyer.com

CVR 3162 7885



THE POLITICAL AGREEMENT ON THE EU ARTIFICIAL INTELLIGENCE ACT ("THE AI ACT") AND NEW IMPORTANT JUDGMENTS FROM THE CJEU ON GDPR FINES AND DAMAGES ACTIONS

19 December 2023

Introduction

In this newsletter, we reflect on important novel AI regulation[1] and GDPR[2] case-law emanating from the EU.

[1] The Commission's "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" (COM(2021) 206 final 2021/0106 (COD).

[2] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

On 9 December 2023, the European Parliament ("the EP") and the European Council ("the Council") reached the much-awaited political agreement on the AI Act[3] following the proposal prepared by the EU Commission ("the Commission") in April 2021.

As a regulation, the AI Act will become directly applicable in each Member State following its formal adoption by the EU legislature.

While the final legislative text has not yet been adopted and made public, we will address some of the expected main features of the AI Act based on the Commission's draft proposal for the AI Act and the press releases from the EP and the Commission.

No political agreement has yet been reached with regard to the Commission's AI Liability Directive proposal[4], which was prepared on 28 September 2022 with the intent of complementing the AI Act in the future insofar as the directive shall provide a new legal basis for claims for damages in the EU caused by AI systems. However, the political intention appears unaltered as concerns the eventual adoption of the directive.

For this reason, we will also touch on the main features of the AI Liability Directive as per the Commission's proposal along with the expected timeline for its formal adoption.

Third, the EU Court of Justice ("the CJEU") has recently passed some highly important judgments shedding further light on the imposition and calculation of fines on "undertakings" breaching the GDPR as well as the basis for damages actions resulting from GDPR infringements.

Aside from providing important clarity with respect to the legal state of play under the GDPR, these judgments could very well mirror the legal state of play that would similarly apply under the AI Act and AI Liability Directive once eventually applicable.

Therefore, we will also expand on these judgments and their potential implications for the future state of play under the impending AI regulation.

[3] Reference is made to the press release of Commission of 9 December 2023, "*Commission welcomes political agreement on Artificial Intelligence Act*",* and the press release of the EP of 9 December 2023, "*Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI*".

[4] The Commission's "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)" (COM(2022) 496 final 2022/0303 (COD)

The AI Act

The AI Act provides harmonised rules for the placing on the market, the putting into service and the use of AI systems in the EU.

As a main feature, the AI Act is founded on a risk-based approach.

It lays down prohibitions of certain AI practices, imposes specific requirements for high-risk AI systems and obligations for operators of such systems, while introducing transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio, or video content.

The main scope of the AI Act extends to i) "*providers*"[5] placing AI systems on the market or putting into service AI systems in the EU, irrespective of whether those providers are established within the EU or in a third country; ii) "*users*"[6] of AI systems located within the EU and iii) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the EU.

The obligated Parties under the AI Act

The AI Act imposes varying obligations on different economic operators depending on their position in the AI system value chain. The most extensive obligations are however imposed on the providers of high-risk AI systems.

Providers of high-risk AI systems which consider or have reason to consider that a high-risk AI system which they have placed on the market or put into service is not in conformity with the AI Act shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it or to recall it, as appropriate.

Notwithstanding, the AI Act also imposes significant obligations on other relevant parties, such as the users of high-risk AI systems as well as importers, distributors, authorised representatives of providers of high-risk AI systems, and certain product manufacturers[7].

[5] The AI Act defines the concept "*provider*" as *"[..] a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge [..]"*.

[6] The AI Act defines the concept "*user*" as *"[..] any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity [..]"*.

[7] Where a high-risk AI system related to products covered by the applicable annex to the AI Act, is placed on the market or put into service together with the product manufactured in accordance with the annex regulation and under the name of the product manufacturer, the manufacturer of the product shall take the responsibility of the compliance of the AI system with the AI Act and, as far as the AI system is concerned, have the same obligations imposed by the AI Act on the provider.

As concerns the *users* of high-risk AI systems, they shall in particular ensure that the input data used is relevant in view of the intended purpose of the high-risk AI system to the extent that the user exercises control over the input data. The *users* shall also monitor the operation of the high-risk AI system on the basis of the instructions of use. Moreover, when the users have reasons to consider that the particular use may result in the AI system "*presenting a risk*" within the meaning ascribed to it under the AI Act, they shall inform the provider or distributor and suspend the use of the AI system concerned.

In addition, any distributor, importer, user or other third-party shall be considered a "*provider*" for the purposes of the AI Act and shall be subject to the obligations incumbent on providers under AI Act in certain specific circumstances, including where such parties *"[..] modify the intended purpose of a high-risk AI system already placed on the market or put into service [..]"* or *"[..] they make a substantial modification to the high-risk AI system [..]"*.

Prohibited AI Practices

The following AI practices shall be outright prohibited due to their considered potential threat to the fundamental rights and safety of the EU citizens:

- biometric categorisation systems that use sensitive characteristics (e.g. political, religious, philosophical beliefs, sexual orientation, race);
- untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases;
- emotion recognition in the workplace and educational institutions;
- social scoring based on social behaviour or personal characteristics;
- AI systems that manipulate human behaviour to circumvent their free will as well as AI systems used to exploit the vulnerabilities of people (due to their age, disability, social or economic situation).

High-Risk AI Systems

AI systems identified in the AI Act, with applicable annexes, as "high-risk" will be required to comply with strict requirements, including establishing risk-mitigation systems, high quality of data sets, logging of activity, detailed documentation, clear user information, human oversight, and a high level of robustness, accuracy, and cybersecurity.

Examples of such high-risk AI systems include certain critical infrastructures for instance in the fields of water, gas, and electricity; medical devices; systems to determine access to educational institutions or for recruiting people; or certain systems used in the fields of law enforcement, border control, administration of justice and democratic processes.

Moreover, AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts is also considered a high-risk AI system.

The Commission shall also be empowered to update the list of high-risk AI systems covered by the AI Act subject to these systems meeting certain conditions set out in the act.

Importantly, the fact that an AI system is classified as high risk under the AI Act does not imply that the use of that system is necessarily lawful under other acts of EU law or under national law compatible with EU law, such as the protection of personal data under the GDPR.

Any such use should continue to occur solely in accordance with the applicable requirements resulting from the Charter[8] and from the applicable acts of secondary EU law and national law.

Minimal Risk AI Systems

The vast majority of AI systems are deemed to fall into the – implicit - category of minimal risk. Minimal risk applications such as AI-enabled recommender systems or spam filters will not be subject to any obligations under the AI Act as these systems present only minimal or no risk for EU citizens' rights or safety.

General-purpose AI Systems

General-purpose AI ("GPAI") systems, and the GPAI models they are based on, will have to adhere to certain transparency requirements under the AI Act. These include drawing up technical documentation, complying with EU copyright law and disseminating detailed summaries about the content used for training.

For high-impact GPAI models with systemic risk, more stringent obligations apply.

If these models meet certain criteria, they will have to conduct model evaluations, assess, and mitigate systemic risks, conduct adversarial testing, report to the Commission on serious incidents, ensure cybersecurity and report on their energy efficiency.

Public Enforcement of Infringements of the AI Act

In terms of governance, the AI Act will be enforced through a governance system at Member States level consisting of national competent market surveillance authorities, which shall

[8] The Charter of Fundamental rights of the European Union.

supervise the implementation of the AI Act at national level. In addition, the creation of a new European AI Office within the Commission shall ensure coordination at the European level.

Next, the AI Act proscribes that an obligated "*company*" is subject to potentially very significant fines for infringements of the AI Act.

Fines would range from EUR 35 million or 7% of the global annual turnover (whichever is higher) for violations of banned AI applications, EUR 15 million or 3% for violations of other obligations related to high-risk AI systems and EUR 7.5 million or 1.5% for supplying incorrect information.

More proportionate caps are foreseen for administrative fines for SMEs and start-ups in case of infringements of the AI Act.

It will be interesting to see if the term "company" will be amended to the broader term "undertaking" as applicable under the EU competition law area[9] and the GDPR once the formal AI Act text is adopted by the EU legislature.

Expected Timeline for Adoption and Entry into Force of the AI Act

The political agreement on the AI Act is now subject to formal approval by the EP and the Council. It will enter into force 20 days after publication in the OJE.

The AI Act will then become generally applicable two years after its entry into force, except for some specific provisions:

The regulation in the AI Act on the prohibited AI practices shall apply already after six months whereas the rules on General Purpose AI shall apply after 12 months.

The proposed AI Liability Directive

The proposed AI Liability Directive complements the Artificial Intelligence Act by introducing a new EU-law based regime applicable to non-contractual fault-based civil law claims brought before national courts for damages caused by an AI system.

It covers national liability claims mainly based on the fault of any person with a view of compensating any type of damage and any type of victim.

[9] Reference is made to Articles 101 and 102 as well as 107 TFEU and the EU Foreign Subsidies Regulation.

Traditionally, Member States' different non-contractual fault-based liability regimes often require the victim or the consumer to establish a wrongful act or omission as well as an incurred loss in order to be compensated.

However, such national law regimes may likely disadvantage victims or consumers severely if applied similarly to harm caused by AI-enabled products and services given the specific characteristics of AI systems, which include their complexity, autonomy, and opacity (the so-called "black box" effect).

In practice, these special features related to AI systems would likely make it difficult or prohibitively expensive for victims or consumers to identify the liable person, let alone to meet all the requirements for a successful liability claim to the requisite evidential extent.

In order to mitigate this issue, the proposed AI Liability Directive intends to ease the burden of proof in a very targeted and proportionate manner through the use of disclosure and rebuttable presumptions. It establishes for those seeking compensation for damage a possibility to obtain information on the high-risk AI systems to be recorded/documented pursuant to the AI Act.

With respect to damage caused by AI systems, the proposed AI Liability Directive aims to provide an effective basis for claiming compensation in connection with the fault consisting in the lack of compliance with a duty of care under applicable EU law or national law.

Therefore, a targeted rebuttable presumption of causality has been laid down in the proposed AI Liability Directive.

The fault of the defendant must be proven by the claimant according to the applicable EU law or national rules. Such fault can be established, for example, for non-compliance with a duty of care pursuant to the AI Act or pursuant to other rules set at EU level.

In addition, the proposed AI Liability Directive provides that the defendant shall have the right to rebut the causality presumption proscribed by the directive.

Next, whereas for high-risk AI systems, the AI Act provides for specific documentation, information, and logging requirements, the proposed AI Liability Directive provides such obligated parties with a further incentive to comply with aforesaid requirements as the draft directive provides that these economic operators risk being met by a disclosure court order under a damages case.

More specifically, the proposed AI Liability Directive suggests that national courts shall be able to, in the course of civil proceedings, order the disclosure or preservation of relevant evidence related to the damage caused by high-risk AI systems from persons who are already under an obligation to document or record information pursuant to the AI Act.

This disclosure obligation may also extend to third parties which are under an obligation to document or record such evidence pursuant to the AI Act, but are not a party to the damages proceedings.

At this stage, no political agreement has been reached with respect to the AI Liability Directive.

Given the directive would complement the AI Act in many important respects it would have to be assumed that the directive will however eventually be adopted by the EU legislature, following which it would likely also be subject to a 2-year deadline for implementation into national law meaning that it will, anyhow, not enter into force at the same time as the AI Act.

This may appear somewhat unfortunate given the intertwined and complementary objectives of the AI Act and the AI Liability Directive.

The new judgments from the CJEU on parental GDPR liability with respect to fines for infringement of the GDPR and private GDPR enforcement in the form of damages claims for GDPR infringements

In its landmark judgment of 5 December 2023 in case C-807/21, *Deutsche Wohnen SE*, the CJEU (Grand Chamber) has now first of all confirmed that the competent data protection authorities may only impose a fine for a GDPR infringement to the extent it is proven that the responsible controller has intentionally or negligently committed the infringement.

No strict liability standard applies when it comes to the legal basis for fining GDPR infringements.

According to the CJEU, the controller has committed the infringement intentionally or negligently when the controller *"[..] could not be unaware of the infringing nature of its conduct, whether or not it is aware that it is infringing the provisions of the GDPR [..]"*.

Second, the CJEU also ruled on how the concept of "undertaking" is to be construed for the purposes of the calculation of fines imposed on the basis of Article 83 of the GDPR.

In this regard, the CJEU clarified that where the addressee of the fine is or forms part of an undertaking, the supervisory authority imposing the fine must take as its basis the concept of an "undertaking" as construed under EU competition law[10].

This implies effectively that where the addressee of the fine forms part of a group of companies, that fine must be calculated on the basis of the group's turnover and not just the turnover of the legal entity constituting the controller.

Consequently, the judgment means that businesses can potentially be subject to very significant fines for wrongful infringements of the GDPR.

The Judgments of 14 December 2023 in case C-340/21, VB, and in case C-456/22, VX, AT v Gemeinde Ummendorf

The CJEU ruled on 14 December 2023 on two different preliminary referrals pertaining to damages actions based on Article 82 (1) for alleged infringements of the GDPR.

In its judgment in case C-456/22, *VX, AT v Gemeinde Ummendorf*, the CJEU held that Article 82(1) of the GDPR implies that there is no "*de minimis* threshold" applicable to the establishment of non-material damage caused by an infringement of the GDPR.

However, the data subject (the claimant) is nonetheless still required to show that the consequences of the infringement which he or she claims to have suffered constitute "damage" which differs from the mere infringement of the provisions of that regulation. Otherwise, no damages can be awarded.

In its judgment in case *C-340/21, VB*, the CJEU inter alia ruled that Article 82(1) of the GDPR must be interpreted to the effect that the fear experienced by a data subject (the claimant) with regard to a possible misuse of his or her personal data by third parties as a result of an infringement of the GDPR is capable, in itself, of constituting "non-material damage" within the meaning of that provision.
However, the national court dealing with the damages action must verify that that fear invoked by the data subject (the claimant) can be regarded as well founded, in the specific circumstances at issue and with regard to the data subject.

The CJEU also ruled that in an action for damages under Article 82 of the GDPR, the controller in question bears the burden of proving that the security measures implemented by it are appropriate pursuant to Article 32 of the GDPR.

[10] That concept covers any entity engaged in an economic activity, irrespective of the legal status of that entity and the way in which it is financed. The concept of an undertaking therefore refers to an economic unit even if, in law, that economic unit consists of several natural or legal persons.

Moalem Weitemeyer's Comments

As appears, the AI Act and the AI Liability Directive will undoubtedly affect most businesses in the EU as well as a very significant number of businesses outside the EU.

Businesses should already now consider preparing for the future application of this new AI legal framework.

This includes establishing and monitoring the relevant compliance mechanisms and routines, conducting the requisite cross-border compliance checks for the entire group, extending the due diligence scope for the purposes of future M&A transactions while taking the AI legal framework into consideration for the purposes of the drafting and negotiation of the transaction documents.

In addition, the AI Act and the AI Liability Directive may also pave the way for new types of AI damages actions, including class actions, for which businesses should also prepare and seek to risk-mitigate to the extent relevant.

Similarly, the new GDPR judgments from the CJEU underpin the parental liability doctrine and financial risks facing businesses in connection with GDPR infringements.

For this reason, it is more important than ever that businesses establish the requisite GDPR compliance mechanisms, scrutinize the GDPR compliance of the target in connection with M&A transactions and prepare a solid evidential line of defense in case of being met by any private or public GDPR enforcement action.

Please feel free to reach out to us, should you have any questions or queries in regard to any of the above.

If you have any questions or require further information regarding any of the above, please do not hesitate to contact us.

Thomas Mygind
Partner
thomas.mygind@moalemweitemeyer.com

Michael Thai Hansen
Senior Associate
Michael.hansen@moalemweitemeyer.com

Henrik Ringgaard Diget
Associate
Henrik.diget@moalemweitemeyer.com

The above does not constitute legal counselling and Moalem Weitemeyer does not warrant the accuracy of the information. With the above text, Moalem Weitemeyer has not assumed responsibility of any kind as a consequence of any reader's use of the above as a basis for decisions or considerations.

This news piece has been produced in the English language only. Are you a client or a prospective client, and should you require a Danish version, please email us at news@moalemweitemeyer.com with a link to the article that you would like to request to receive in Danish, and we will attend to your request without undue delay.