The new EU AI Act and data protection: What deployers of AI systems need to bear in mind

THE GERMAN DATA PROTECTION AUTHORITIES HAVE PUBLISHED INITIAL GUIDANCE ON THE USE OF ARTIFICIAL INTELLIGENCE

Executive Summary

- The EU AI Act, which is expected to come into force in June 2024, is the first comprehensive legal framework regulating the development and use of artificial intelligence systems in the EU.
- The AI Act does not replace any existing data protection regulations. These regulations will still have to be applied and observed comprehensively in the future.
- In order to provide legal guidance in connection with the new AI Act, the German data protection authorities have published guidelines on “Artificial Intelligence and Data Protection”.

1. Introduction

The regulation of artificial intelligence systems and their application in the EU in the form of horizontal product safety provisions is imminent. This is the first legislative project in the world to have such a broad scope, covering almost every sector of the economy. The regulation laying down harmonised rules on artificial intelligence (AI Act) is anticipated to come into force in June 2024 and will apply gradually in several stages over a period of two years. Certain regulations shall apply as early as six months after the AI Act comes into force, in particular the bans on certain applications of artificial intelligence.

The AI Act does not change the current data protection regime in the EU and, in particular, does not supersede or

supplement the EU General Data Protection Regulation (GDPR). In several instances, the AI Act makes reference to existing data protection regulations. It goes without saying that data protection will play a central role in the implementation and use of AI systems in practice. The use of artificial intelligence comes with considerable data protection risks, e.g., with regard to deepfakes, bias and false identities (fake IDs).

2. Data protection guidance note by the authorities

In view of the imminent entry into force of the AI Act and the increasing use of AI applications, the Conference of Independent Data Protection Authorities in Germany published an initial guidance note on "Artificial intelligence and data protection" on 6 May 2024.[1] This guidance note has legal weight, as the German data protection authorities will use these guidelines as a basis for their understanding and interpretation of the legal provisions and for the prosecution of possible data protection violations.

The guidance note is primarily aimed at deployers of AI systems in the private and public sectors (and only indirectly at the developers of such systems). The guidance note addresses specific data protection risks that may be associated with the use of AI. In addition to providing information on possible data protection violations that can result from the unlawful use of AI, the publication also provides practical examples of measures deployers can take to minimise and avoid such risks.

We have summarised some key aspects of the guidance note below:

2.1 Legal basis for data processing

The processing of personal data requires a legal basis under data protection law (this also applies to the processing of personal data by AI applications). Depending on the specific case, various legal bases may come into consideration, depending on, e.g., whether the application is being used in HR or the healthcare system or if data is to be processed in connection with a consumer contract.

When selecting AI applications, whether and to what extent the application have been trained in compliance with data protection regulations may be relevant for the necessary legal basis for processing. The use of personal data for the training of AI systems is only permitted if the data subject has consented to the processing of their data for that specific purpose or the data has otherwise been lawfully collected in accordance with the Article 6 GDPR (in particular with regard to a contractual basis). Deployers who use AI under their own responsibility must ensure that errors in the training of an AI application do not have an impact on the data processing for which they are responsible.

2.2 Transparency obligations

The use of AI applications triggers various information and transparency obligations for data controllers. If controllers have not developed an AI application themselves, they must ensure that the developer or provider provides them with sufficient information to enable them to implement the transparency requirements of Article 12 et seq. GDPR. The developer or provider must provide AI deployers with appropriate documentation. If the AI application is used as part of a cloud solution, for example, the provider of the cloud solution is generally obliged as a processor to support the controller as far as necessary to ensure that the controller can fulfil its obligations with regard to the rights of data subjects.

2.3 Rights of data subjects

Data controllers must ensure that data subjects can exercise their data subject rights, in particular the rights to rectification in accordance with Article 16 GDPR and

[1] Guidance issued by the Conference of Independent Federal and State Data Protection Authorities on 6 May 2024, available at: https://content.mlex.com/Attachments/2024-05-06_K3DN3E452H0TH6YG%f20240506_DSK_Orientierungshilfe_KI_und_Datenschutz_web.pdf.

erasure in accordance with Article 17 GDPR. In this respect, organisational and technical procedures must be designed so that data subjects can exercise their rights effectively. It must be possible to exercise the right to rectification in an AI application, for example by correcting data or through retraining/fine tuning.

2.4 Data protection impact assessment

In the case of particularly high-risk data processing, the GDPR requires the controller to carry out a data protection impact assessment (DPIA) in accordance with Article 35 GDPR. Before processing personal data, a preliminary assessment must therefore be carried out to determine whether the risk requires a DPIA with regard to the type, scope, purpose and circumstances of the processing.

In this context, the guidance refers to the list of processing activities published by the Data Protection Conference for which a DPIA must be carried out (also referred to as a "black list" or "must list"). If the controller is not also the provider of the AI system, it must rely on information from the provider (e.g., on how the system works) in order to carry out a DPIA. When selecting and purchasing an AI application, care must be taken to ensure that this information is (or can be) provided by the provider.

2.5 Privacy by design; privacy by default

The right to privacy and the protection of personal data must be guaranteed throughout the life cycle of the AI system. In this respect, it is not only the principles of data minimisation that apply to the processing of personal data. AI systems must also consider data protection-compliant design in terms of the principles of "privacy by design" and "privacy by default" (Article 25 GDPR). These requirements must be taken into account while the AI system is still in the design phase. For example, in the case of accounts that are to be used by employees, it must be possible to configure the settings for using inputs for AI training and for the input history when an account is set up in such a way that no data is processed for training purposes and no input history is saved after the end of the session. In principle, output data belonging to an account may not be published automatically.

2.6 Data security

In addition to the technical and organisational measures required under data protection law (see in particular Articles 25 and 32 GDPR), AI applications must also comply with the requirements that generally apply to IT systems (e.g. in terms of reliability, usability, security (confidentiality, integrity, availability and resilience)). If attackers succeed in gaining unauthorised access to AI applications, this may result in a breach of data protection, for example if previous activities, personal information and trade secrets are accessed. Suitable protective measures therefore need to be implemented.

2.7 Checking results for accuracy and discrimination

The output of AI applications with reference to individuals must be subjected to critical scrutiny. As a rule, texts generated using AI applications do not make any claim to be accurate. Results or the application of results referencing individual persons may contain incorrect information that could result in unauthorised processing, and must therefore be checked before the data is processed any further.

Results from AI applications that have a discriminatory effect can also lead to unauthorised processing. Data processing may be unlawful and therefore prohibited if, for example, it (structurally) leads to a violation of the General Equal Treatment Act (AGG). Data controllers must therefore check whether the further use of the output generated by an AI application is legally permissible.

3. Outlook

As long as the principles and measures addressed in the data protection guidance note are observed, it is possible to align the use of AI applications with data protection requirements in practice. This will help to strengthen user confidence in AI systems and promote their responsible use, as well as minimising legal risks, particularly in relation to data protection.

The data protection authorities will play a central role in monitoring and regulating the use of artificial intelligence, particularly with regard to data protection and the rights of data subjects. The AI Act already stipulates that the data protection authorities are to act as competent market surveillance authorities for certain sectors. Due to their existing responsibilities under the GDPR, many years of expertise in the protection of digital fundamental rights and the established, cooperative supervisory and coordination mechanisms, the German data protection authorities are actively calling for their scope of responsibility to be expanded to cover the provisions of the AI Act. The data protection authorities in Germany are proposing that they be tasked with market surveillance of AI systems in accordance with the AI Act at the national level.[2] This would make compliance with data protection provisions and their monitoring an overriding core element of future AI regulation.

Dr Jörg Kahler
Lawyer
Berlin
Tel +49 30 2039070
joerg.kahler@gsk.de

Dr Martin Hossenfelder
Lawyer
Berlin
Tel +49 30 2039070
martin.hossenfelder@gsk.de

[2] Resolution of the Conference of Independent Federal and State Data Protection Authorities on 3 May 2024, available (in German) at: https://www.datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf.

GSK
STOCKMANN

Disclaimer
This client briefing exclusively contains general information which is not suitable to be used in the specific circumstances of a certain situation. It is not the purpose of the client briefing to serve as the basis of a commercial or other decision of whatever nature. The client briefing does not qualify as advice or a binding offer to provide advice or information and it is not suitable as a substitute for personal advice. Any decision taken on the basis of the content of this client briefing or of parts thereof is at the exclusive risk of the user.

GSK Stockmann as well as the partners and employees mentioned in this client briefing do not give any guarantee nor do GSK Stockmann or any of its partners or employees assume any liability for whatever reason regarding the content of this client briefing. For that reason, we recommend you to request personal advice.

www.gsk.de

GSK Stockmann
Rechtsanwälte Steuerberater Partnerschaftsgesellschaft mbB

BERLIN
Mohrenstrasse 42
10117 Berlin
T +49 30 203907 - 0
F +49 30 203907 - 44
berlin@gsk.de

HEIDELBERG
Mittermaierstrasse 31
69115 Heidelberg
T +49 6221 4566 - 0
F +49 6221 4566 - 44
heidelberg@gsk.de

FRANKFURT/M.
Bockenheimer Landstr. 24
60323 Frankfurt am Main
T +49 69 710003 - 0
F +49 69 710003 - 144
frankfurt@gsk.de

MUNICH
Karl-Scharnagl-Ring 8
80539 Munich
T +49 89 288174 - 0
F +49 89 288174 - 44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBOURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L - 1855 Luxembourg
T +352 271802 - 00
F +352 271802 - 11
luxembourg@gsk-lux.com

LONDON
GSK Stockmann International
Rechtsanwaltsgesellschaft mbH,
London branch
Queens House, 8-9 Queen Street
London EC4N 1SP
United Kingdom
T +44 20 4512687-0
london@gsk-uk.com

Registered office: Munich
Munich Local Court
HRB 281930
Managing directors:
Dr Mark Butt, Andreas Dimmling

YOUR PERSPECTIVE.
GSK.DE | GSK-LUX.COM