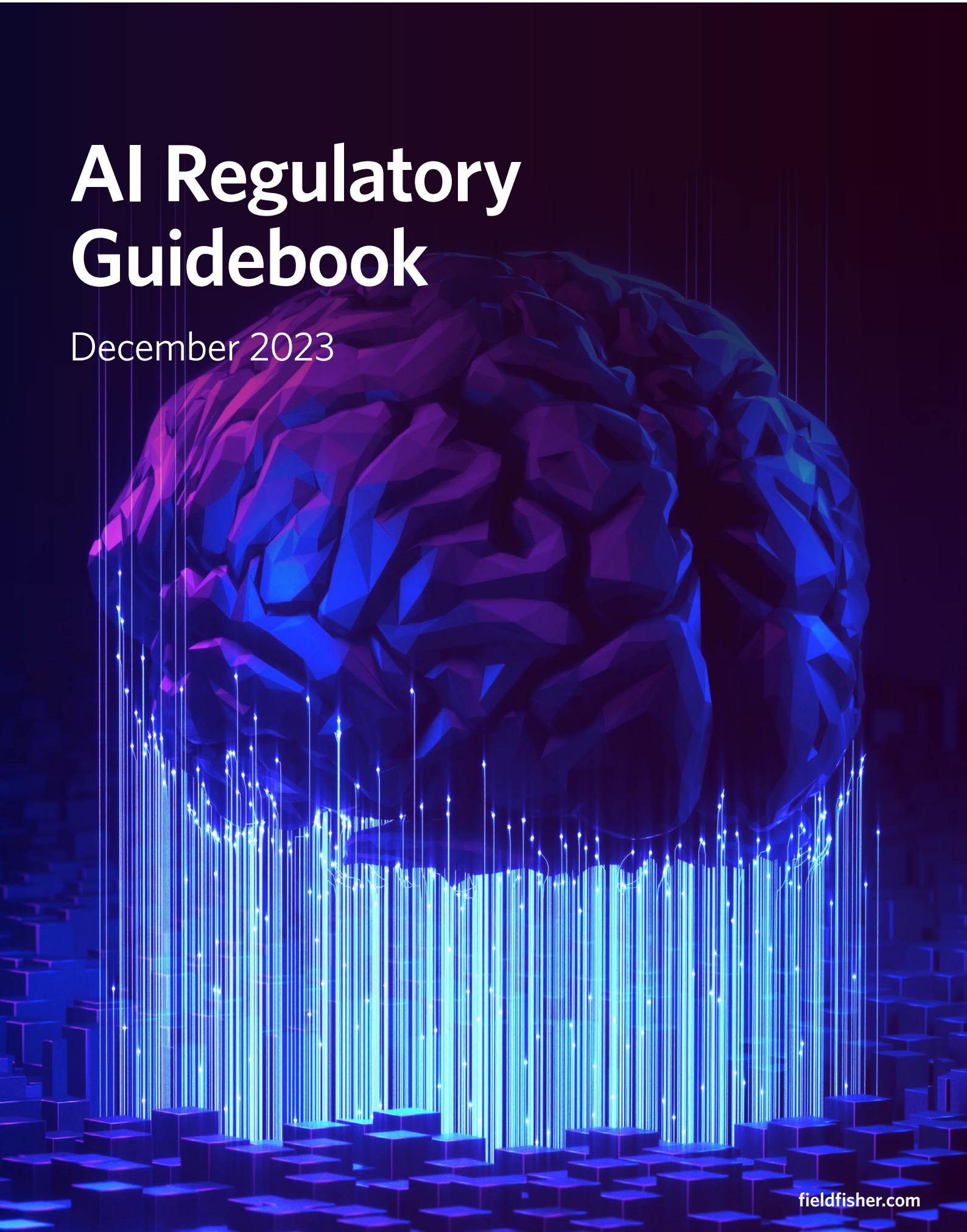
ecomlex

fieldfisher

AI Regulatory Guidebook

December 2023



fieldfisher.com

Acknowledgements

This document was prepared jointly by Fieldfisher's Technology & Data lawyers and the members of the Ecomlex network.

Special thanks to the following contributors:

Ady Van Nieuwenhuizen, Carlos Pérez, Ciara Burke, Clara-Ann Gordon, Francesca Gravili, Gabrielle Slotthagen, Inès Benazzouz, Ivan Rames, Louis Vanderdonckt, Marek Korcz, Dr. Márk Pécsvárady, Martin Gynnerstedt, Martin Von Willebrand, Michael Hopp, Michał Pietrzyk, Monica Oliveira Costa, Oliver Süme, Olivier Proust, Paul Barton, Philip Reinisch, Rasmus Møller Erlandsen, Sonja Laamanen, Sonia Gracia, Ståle L. Hagen, Dr Tamas Gödölle, Tim van Canneyt.

Introduction

Artificial intelligence has become a major area of focus for organisations around the world. While organisations are coming to grips with the complex legal, compliance and ethical issues deriving from AI, legislators around the world are beginning to adopt laws that will regulate the development, distribution and use of AI systems. In the EU, the much-anticipated Artificial Intelligence Act is currently undergoing the legislative process and is expected to be adopted in the course of 2024.

In this guidebook, we provide an overview of the current positions of the national data protection authorities in the EU member states, Norway, Switzerland and the United Kingdom with respect to how personal data may be processed in the context of AI systems. Based on the guidelines and positions that have been adopted by the data protection authorities, we provide a general understanding of how regulators are addressing specific topics such as "*On what legal basis may personal data be used to train AI models?*", "*Who is the competent regulator for enforcing AI laws?*" and "*Have the data protection authorities issued any sanctions regarding AI models?*"

This guidebook is provided for information purposes only and should not be construed as giving legal advice. AI is a fast-developing area of the law and this guidebook will need to be updated periodically.

Paul Barton
Partner, Fieldfisher
+44 330 460 7093
paul.barton@fieldfisher.com

Hazel Grant
Partner, Fieldfisher
+44 330 460 7056
hazel.grant@fieldfisher.com

Olivier Proust
Partner, Fieldfisher
+32 2 742 70 15
olivier.proust@fieldfisher.com

Contents

Austria

Philipp Reinisch

Partner, Fieldfisher

+43 1 928 163 40 18
philipp.reinisch@fieldfisher.com

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

It is not yet decided, if any new supervisory authorities will be established by law. Therefore, the competent authorities will monitor compliance with the requirements of the AI Act considering the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence ("**AI Act**") and amending certain Union acts as well as with further upcoming laws and regulation.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Not so far.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

The Federal Ministry for Climate Protection, Environment, Energy, Mobility, Innovation and Technology has published the future strategy related to AI as follows: *Artificial Intelligence Mission Austria 2030 - AIM AT 2030*. The AIM AT 2030 contains clear goals and measures, which are divided into general fields of action and a selection of initial relevant application fields on the following pages:

https://www.bmk.gv.at/dam/jcr:93f327ac-b69c-4ac7-a9aa-30eee51cc221/AIM_AT_2030_UA.pdf

The Committee for Research, Innovation and Digitisation of the National Council has likewise taken a stand with regard to the rapid development on AI:

https://www.parlament.gv.at/aktuelles/pk/jahr_2023/pk0740
(only available in German)

The Ministry of Digitisation has also stated that, as a first step, it is planned to establish an office in Resort, which will take care of the preparations and national implementation. When the AI Act is implemented, this office will become a separate authority:

https://futurezone.at/netzpolitik/ki-behoerde-tursky-florian-digitalisierung-kuenstliche-intelligenz/402442857
(only available in German)

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

In Austria an Austrian AI Act is already in the law-making process. Any further information as well as responsibilities of authorities are not yet known, as the documents available to the Parliament are not yet publicly accessible. It is therefore not yet possible to specify whether an existing authority will be responsible for the control and enforcement of the AI Act or whether a new one will be created.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

When dealing with artificial intelligence, it is particularly important that safety for people and the protection of fundamental and human rights must always be the focus, while at the same time enabling innovation and thus economic growth is made possible. This includes in particular:

- safeguarding the **competitiveness** of Austria as a location for technology and business
- **ensuring standards** under international law, especially in the area of human rights and international humanitarian law
- that discrimination or systematic disadvantages are excluded in the technical implementation and that **personal rights and data protection** are respected.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

The processing of personal data in connection with the use of AI requires compliance with the data processing principles of the GDPR, which also applies indirectly in Austria. Thus, among other things, according to the:

- **Principle of data minimisation**
- **Principle of purpose limitation**
- **Accountability**

Not to be disregarded. This also includes the regulations under Art 13 and 14 GDPR in connection with the direct collection and third-party collection of data.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

The same provisions as in Germany apply. Accordingly, data subjects must be informed whether automated decision-making and profile analysis are involved. If this is the case, the data subjects must also be provided with information on the logic and scope used and the intended effects of the data processing.

6.3. Data subject rights

In particular, the data protection authority enforces the following rights:

- **Right to secrecy** of personal data
- **Right of access**: to know who processes data, where they come from, what they are used for and to whom they are transmitted.
- **Right to rectification of inaccurate data**
- **Right to erasure** of data processed in an inadmissible manner.

The fundamental right to data protection has direct third-party effect; it obliges the state and private parties. Violations can be asserted by means of a complaint to the data protection authority.

6.4. Automated decision making (Art. 22 GDPR)

Art 22 GDPR clarifies that the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. The only exceptions to this prohibition are,

- where the profiling is necessary for the conclusion or performance of a contract between the data subject and the controller;
- if the processing is permitted under local law; or
- when it is based on the explicit consent of the data subject.

Art 22 (3) GDPR states that the controller is obliged to protect the rights of the data subject, which include in particular:

- **Safeguards** to challenge a decision and/or human intervention;
- **Right to explanation** about the evaluation criteria, so that the data subject is able to challenge the decision and have all the information;
- **General right to information** and **right to access**.

If a human makes a decision based on a recommendation that was automated by an AI system, Art 22 GDPR would not apply. Therefore, the processing of data for profiling under (i) and (ii) does not fall under the definition of Art 22 GDPR. In these cases, profiling and automated decision making are only subject to the general rules for data processing (Art 5 and Art 6 GDPR).

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

Art 25 (2) GDPR states that:

- appropriate measures must be taken to ensure that, by default, only personal data whose **processing is necessary** for the respective specific processing purpose is processed and
- the controller must ensure that the software used by the controller to fulfil the **purpose of the processing implements** the requirements under the GDPR.

Therefore, if the technical tool processes more data than necessary to fulfil the purpose, the controller would realise, on the one hand, a violation of the data minimisation principle and a violation of the requirement of data protection-friendly default settings (quantitative restriction of data processing under Art 25).

By processing only **pseudonymised data**, the controller would comply with the principle of data minimisation.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

According to Art 35(1) GDPR, a data protection impact assessment shall be carried out where a form of processing, in particular where new technologies are used, is likely to result in a high risk to the rights and freedoms of natural persons by virtue of the nature, scope, context and purposes of the processing. The use of AI constitutes such a new technology.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

Not specified.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

Not specified.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

Since AI systems assume only mathematical weightings and biases in their perceptions, but lack social skills and cannot draw logical conclusions, this poses a risk of discriminatory and manipulative decision-making.

- **Safeguards** must be put in place so that the conclusions are verifiable by a natural person.
- The **consent requirement** under the GDPR is limited, so that in Austria children from the **age of 14 years** can give their consent to data processing.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

Not at the current time.

Belgium

Tim Van Canneyt

Partner, Fieldfisher

+32 2 742 70 36
tim.vancanneyt@fieldfisher.com

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

In Belgium, it is not yet certain whether this supervisory authority will be newly created or attached to an existing institution. In relation to the impeding AI Act, the Belgian DPA indicates in its 2022 Annual Report that it is "*preparing for its regulatory role in this multifaceted and changing regulatory framework*".

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Not so far.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

Not so far.

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Not currently.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

So far, no Belgian authority has issued meaningful statements regarding the development and use of artificial intelligence.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

Nothing mentioned yet.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

N/A

6.3. Data subject rights

So far, the Belgian DPA has not commented on this point.

6.4. Automated decision making (Art. 22 GDPR)

So far, the Belgian DPA has not commented on this point.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

So far, the Belgian DPA has not commented on this point.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

According to Art 35(1) GDPR, a data protection impact assessment shall be carried out where a form of processing, in particular where new technologies are used, is likely to result in a high risk to the rights and freedoms of natural persons by virtue of the nature, scope, context and purposes of the processing. The use of AI constitutes such a new technology.

The Belgian DPA has not commented on this, however.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

So far, the Belgian DPA has not commented on this point.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

So far, the Belgian DPA has not commented on this point.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

So far, the Belgian DPA has not commented on this point.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

So far, the Belgian DPA has not commented on this point.

Czech Republic

Ivan Rames

Partner, Havel & Partners

+420 255 000 949
ivan.rames@havelpartners.cz

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

It has not yet been determined which Czech authority will be responsible for enforcing the AI law in the Czech Republic, or whether a new authority will be created for this purpose.

The Czech Republic (Ministry of Trade and Industry) was one of the first countries to adapt a National Strategy for AI in 2019 and the National Strategy for AI is currently being updated to reflect the latest developments in AI. It is likely to also address the issue of enforcement of the AI Act. As of now, open discussions of the National Strategy for AI are complete and release of the updated National Strategy is expected in early 2024. The National Strategy for AI is currently only available in Czech language, however its key implications are highlighted in the AI Summary Report (available from **https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/AI-Summary-Report.pdf**).

In addition, at the government level, the Czech Republic has established a dedicated AI Committee and an AI Observatory Platform and Forum, which focus on monitoring the legal and ethical implications of AI.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Currently, we are not aware of any sanctions imposed by the Czech authorities in this respect.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

Apart from the National Strategy for AI (which only broadly highlights the key issues), we are not aware of any published guidelines or position papers regarding the key issues of the AI yet.

Currently, the National Strategy for AI is to be updated and may include additional guidelines and position papers (its release is expected in early 2024).

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

We are not aware of any such legislative initiatives other than those listed in response to question 1 and those to be adapted on the EU scale.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

As of now, the current focus is the update of the National Strategy for AI which would also provide guidelines for key areas of focus. Any additional regulation progress was halted and is likely only to occur after the introduction and effect of the AI Act.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

Exclusively in relation to AI, the relevant Czech authority has not published any position in this regard. The Czech legislation on data protection does not differ substantially from the GDPR in this respect.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

Exclusively in relation to AI, the Czech DPA has not published any position in this regard. The Czech legislation on data protection does not differ substantially from the GDPR in this respect.

6.3. Data subject rights

Exclusively in relation to AI, the Czech DPA has not published any position in this regard. The Czech legislation on data protection does not differ substantially from the GDPR in this respect.

6.4. Automated decision making (Art. 22 GDPR)

Exclusively in relation to AI, the Czech DPA has not published any position in this regard. The Czech legislation on data protection does not differ substantially from the GDPR in this respect.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

Exclusively in relation to AI, the Czech DPA has not published any position in this regard. The Czech legislation on data protection does not differ substantially from the GDPR in this respect.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

Exclusively in relation to AI, the Czech DPA has not published any position in this regard. The Czech legislation on data protection does not differ substantially from the GDPR in this respect.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

Exclusively in relation to AI, the Czech DPA has not published any position in this regard. The Czech legislation on data protection does not differ substantially from the GDPR in this respect.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

Exclusively in relation to AI, the Czech DPA has not published any position in this regard. The Czech legislation on data protection does not differ substantially from the GDPR in this respect.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

Exclusively in relation to AI, the Czech DPA has not published any position in this regard. The Czech legislation on data protection does not differ substantially from the GDPR in this respect.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

As of now, there are no specific additional regulations for special categories of AI-tools.

Denmark

Michael Hopp
Partner, Plesner

+45 33 12 00 14
mho@plesner.com

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

It is not yet decided, but a lot points to The Danish Data Protection Agency ("**DDPA**"). It has, however, also been mentioned that the Danish Financial Supervisory Authority will be the competent authority specifically in regards to the financial sector.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Not so far.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

The DDPA has issued guidance on 5 October 2023 regarding the use of AI in the public sector and a mapping of AI in the public sector.

Further, the DDPA has - on the basis of a specific inquiry from a public authority - made a public statement on 5 July 2022 regarding the AI tool Asta. Asta is a tool that aims to provide machine analysis of the risk of a newly unemployed unemployment benefit recipient's process with the job centre being prolonged.

The DDPA stated that consent could not be used as a legal basis, as the consent cannot be seen as freely given. The DDPA pointed to 6.1.e. and 9.2.g as the legal basis for such a processing of personal data, provided that said provisions can rely on national laws that provide the foundation for the application of art. 6.1.e and 9.2.g.

The Danish Business Authority and The Agency for Digital Government have published joint guidelines regarding private companies and public authorities' safe use of AI.

The Financial Supervisory Authority has published guidelines on data ethics in the financial sector when using AI.

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Not currently.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

The previous focus has been guidance regarding the legal basis for the processing of personal data in relation to the AI-solution. Furthermore, the DDPA has highlighted that the data subjects have a right to be provided with information when their personal data is being collected in relation to an AI-solution.

The DDPA stated - when issuing its guidance on use of AI - that "*The Danish Data Protection Agency will continue to focus on the use of artificial intelligence. In the shorter term, the supervisory authority will, among other things, prepare a template for carrying out impact assessments that authorities can use in their development work. In the slightly longer term, the Danish Data Protection Agency will look at more guidance on how organisations can handle the risks that may be associated with the use of AI, such as bias and lack of transparency.*"

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

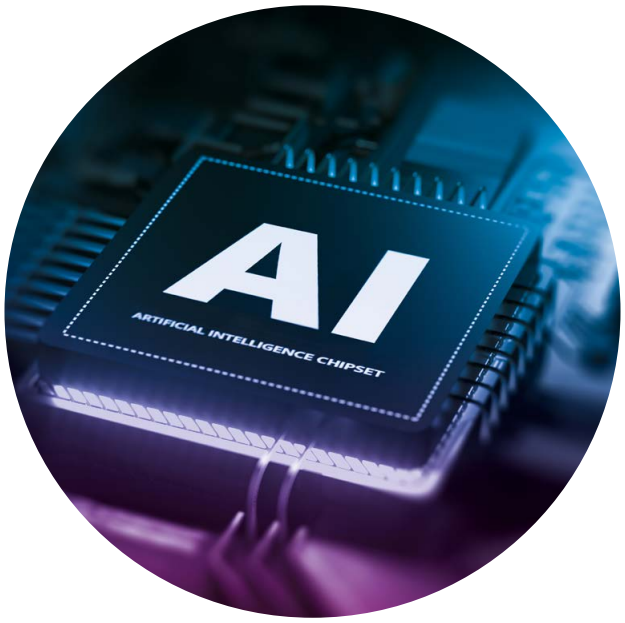
in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

The developers should initially conduct an overall assessment of the entire lifecycle of the upcoming AI-solution to ensure that the necessary legal basis has been identified. According to the DDPA this will for public authorities most likely be GDPR art. 6.1.e. The DDPA has stated that public authorities can process special categories of personal data cf. art. 9, when the processing is necessary for the exercise of public authority.

The developer of an AI-solution can collect personal data for specific, explicit and legitimate purposes only (the principle of purpose limitation).

It is important to be aware that the purpose of the processing is not necessarily the same throughout the whole lifecycle of the AI-solution. The purpose will most likely change. If the purpose changes from the "*development phase*" to the "*use phase*", then the further processing will have to be based on a different (new) legal basis.

The developer shall assess whether the processing of personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (the principle of data minimisation).



6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

The DDPA has explicitly stated that there is an obligation to inform the data subjects about the processing of personal data, when an AI-solution collects personal data about individuals. The requirements for what information must be provided depend on whether the personal data is collected directly from the data subject or from others.

6.3. Data subject rights

See above about the right to be informed (GDPR article 13 and 14).

Nothing further specified by the DDPA.

6.4. Automated decision making (Art. 22 GDPR)

The DDPA has stated that the data subject has a right not to be subject to automated decision making. Therefore, it is prohibited to develop and use an AI-solution that makes automated decisions. However, public authorities may use automated decision making if national law grants a precise authorisation to do so.

Further, the DDPA has stated that the risk of "*automation bias*" is especially relevant when developing an AI-solution for decision support.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

Not specified by the DDPA.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

The DDPA has stated that a DPIA is particularly relevant if you want to process personal data using new technology.

It is the opinion of the DDPA that developing and using AI-systems constitutes "*new technology*" and therefore requires a DPIA.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

Not specified by the DDPA.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

Not specified by the DDPA.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

The DDPA has stated that the requirements for the clarity of the legal basis for the processing of personal data in relation to AI-solutions depends on how intrusive the processing is for the affected individuals. The more personal data that is being processed about vulnerable individuals such as children, the clearer the legal basis should be.

Please note that the DDPA would like to brand itself as the guardian for the processing of personal data about children among the European agencies. One could therefore expect the DDPA to take a further stance on processing of personal data about children.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

Not specified by the DDPA.

Finland

Martin Von Willebrand

Partner, HH Partners

+358 9 177 613
martin.vonwillebrand@hhpartners.fi

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

It has not yet been decided which authority (or authorities) will be responsible for the enforcement of the AI Act in Finland.

On 27 May 2021, the Finnish Government published its statement concerning the commission's proposal on the AI Act and estimated in this statement that the supervisory authority would be the Finnish Safety and Chemicals Agency (Tukes) with regard to market surveillance of products that contain safety components that utilise AI. According to the estimation of the Finnish Government, the Finnish Transport and Communications Agency (Traficom) would act as a supervisory authority with regard to the transport sector. In addition, the Finnish Government envisaged in its letter that the Finnish Data Protection Authority (the Office of the Data Protection Ombudsman) might act as the supervisory authority with regard to AI and the processing of personal data.

In addition, the Finnish Data Protection Authority (the Office of the Data Protection Ombudsman) has stated in its Annual Report 2022, that the Office of the Data Protection Ombudsman should be named as the responsible supervisory authority with regard to AI and processing of personal data. According to the Annual Report, one of the special focus areas of the Office of the Data Protection Ombudsman in 2023 will be AI, automated decision-making, and profiling.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Yes, please see the below.

The Finnish Deputy Data Protection Ombudsman, Statutory reprimand, the National Police Board (decision no. 3394/171/21): The Finnish Deputy Data Protection Ombudsman issued a statutory reprimand to the National Police Board for the failure to comply with data protection legislation (Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security) when processing special categories of personal data during a facial recognition technology trial. The trial was related to the police's experiment of identifying possible victims of child sexual abuse with the US-based Clearview AI service. In addition, the police had also tested Arachnid service for face recognition. The Finnish Deputy Data Protection Ombudsman stated, among other things, that:

- The police did not sufficiently take into account the requirements of processing special categories of personal data, as facial images were considered as biometric data, and thus as a special category of data;
- The police did not acquire information on how the personal data was processed in the service (e.g. data retention periods and transfers to third parties) during the trial before starting to use the service.

The Finnish Deputy Data Protection Ombudsman, Warning, Terveyshyötyarvio (decision no. 6482/186/2020): A healthcare service provider had used software called Terveyshyötyarvio that, based on patients' health data, evaluated which patients were in need of further examination by a healthcare professional. The Deputy Data Protection Ombudsman stated that the decision-making was to be considered automated decision-making with regard to those patients the software identified were not in need of further investigation, and thus, the controller was obliged to comply with Article 22 of the GDPR. The decision-making was not considered to be automated decision-making with regard to the patients who were selected for further examination since a health care professional provided the further examination, and thus, the final decision was made by a human.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

The Finnish Data Protection Authority (the Office of the Data Protection Ombudsman) has published on its website a guidance on automated decision-making and profiling (available in English: **https://tietosuoja.fi/en/automated-decision-making-and-profiling**).

The Ministry of Economic Affairs and Employment of Finland has published the AI Strategy in 2017. The AI Strategy contains action recommendations both for private sector companies and public sector operators (unfortunately only available in Finnish): **https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80849/TEMrap_41_2017_Suomen_teko%C3%A4lyaika.pdf**)

The Finnish Digital and Population Data Services Agency has published a guidebook on how to develop safe AI systems (Turvallisen tekoälykehittäminen opas, unfortunately available only in Finnish: **https://dvv.fi/documents/16079645/110183105/Turvallisen+tekoa%CC%88lykehitta%CC%88misen+opas.pdf/db481eab-1b27-f0d6-b97f-c60741b3bc84/Turvallisen+tekoa%CC%88lykehitta%CC%88misen+opas.pdf?t=1686317697273**).

The Ministry of Finance has published an Ethical Guidelines for AI in Public Administration on its website (available in English: **https://vm.fi/en/ethical-guidelines-for-ai-in-public-administration**).

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

The Finnish Government is preparing legislation related to automated decision-making in public administration (HE 145/2022 Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi). According to Article 22(1) of the GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, which produces legal effects concerning him or her. However, Article 22(2)(b) states that Article 22(1) shall not apply if the decision is authorised by a Member State Law to which the controller is subject. The aim of the new legislation is to enable authorities to practice automated individual decision-making by creating the legal basis with regard to Article 22(2)(b) of the GDPR. According to the government proposal, the authority practicing automated decision-making shall inform the person who is the object of the decision that the decision has been made by using a system that utilises automated decision-making. According to the proposal, utilising machine learning as a part of the authorities' automated decision-making should be prohibited. Automated decision-making shall be practiced by rule-based automation and authorities shall document these rules. In addition, appropriate remedies should be available when decisions are made by automated decision-making systems.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

According to the authorities' guidance, the following should be taken into account while developing and using AI systems:

- protecting fundamental rights and human rights
- ensuring data protection and data security
- ethical aspects and long-term impacts on society
- risk of discrimination
- transparency with regard to developing the AI systems as well as the functioning of the AI systems
- data minimisation principle when using AI tools for processing of personal data

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

So far, the Finnish Data Protection Authority has not commented on this point in relation to AI.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

So far, the Finnish Data Protection Authority has not commented on this point in relation to AI.

6.3. Data subject rights

So far, the Finnish Data Protection Authority has not commented on this point in relation to AI.

6.4. Automated decision making (Art. 22 GDPR)

The Office of the Data Protection Ombudsman has published guidance on automated decision-making and profiling on its website (available in English: **https://tietosuoja.fi/en/automated-decision-making-and-profiling**). According to Article 22(2) of the GDPR, automated decision-making is permitted if the decision: (a) is necessary for entering into, or performing a contract between the data subject and a data controller (b) is authorised by Union, or a Member State Law to which the controller is subject, or (c) is based on the data subject's explicit consent. Please see below some highlights of the guidance on automated decision-making.

According to the guidance, the controller must pay particular attention to the transparency of processing activities in the case of automated decision-making. "*The individuals subject to automated decision-making must be informed of:*

- *the existence of automated decision-making, including profiling,*
- *meaningful information about the logic involved in the processing and*
- *the significance and envisaged consequences for the data subject.*"

"*The controller should, in clear and plain language, inform the data subject of the principles of automated-decision making and the weighting of factors in the decisions. The information provided should be meaningful to the data subject. An exhaustive and complicated description of the decision-making algorithm is not necessarily an appropriate way of informing data subjects on the logic employed.*"

With regard to the processing of children's personal data, the guidelines set out the following: "*Taking the special status of children into account, the GDPR does not explicitly provide for automated decision-making and profiling with regards to children. However, it is stated in the recitals that children should not be subjected to decisions that are based solely on automated processing and have legal effects or correspondingly significant effects. Subjecting children to automated decision-making and profiling can be justified, however, such as in order to safeguard the well-being of the child. In such cases, ensure that the appropriate protection measures are taken.*"

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

So far, the Finnish Data Protection Authority has not commented on this point in relation to AI.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

So far, the Finnish Data Protection Authority has not commented on this point in any greater detail in relation to AI.

However, with regard to impact assessments the following has been set out in the guidance of the Office of the Data Protection Ombudsman on automated decision-making and profiling:

"*Carry out a data protection impact assessment particularly when:*

- *performing a systematic and extensive evaluation of the personal aspects of individuals*
- *the evaluation is based on automated processing such as profiling and*
- *the evaluation will lead to decisions with legal effects concerning natural persons or that affect them in a correspondingly significant manner.*"

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

So far, the Finnish Data Protection Authority has not commented on this point.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

So far, the Finnish Data Protection Authority has not commented on this point in relation to AI.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors
- risk of discrimination (so-called bias)

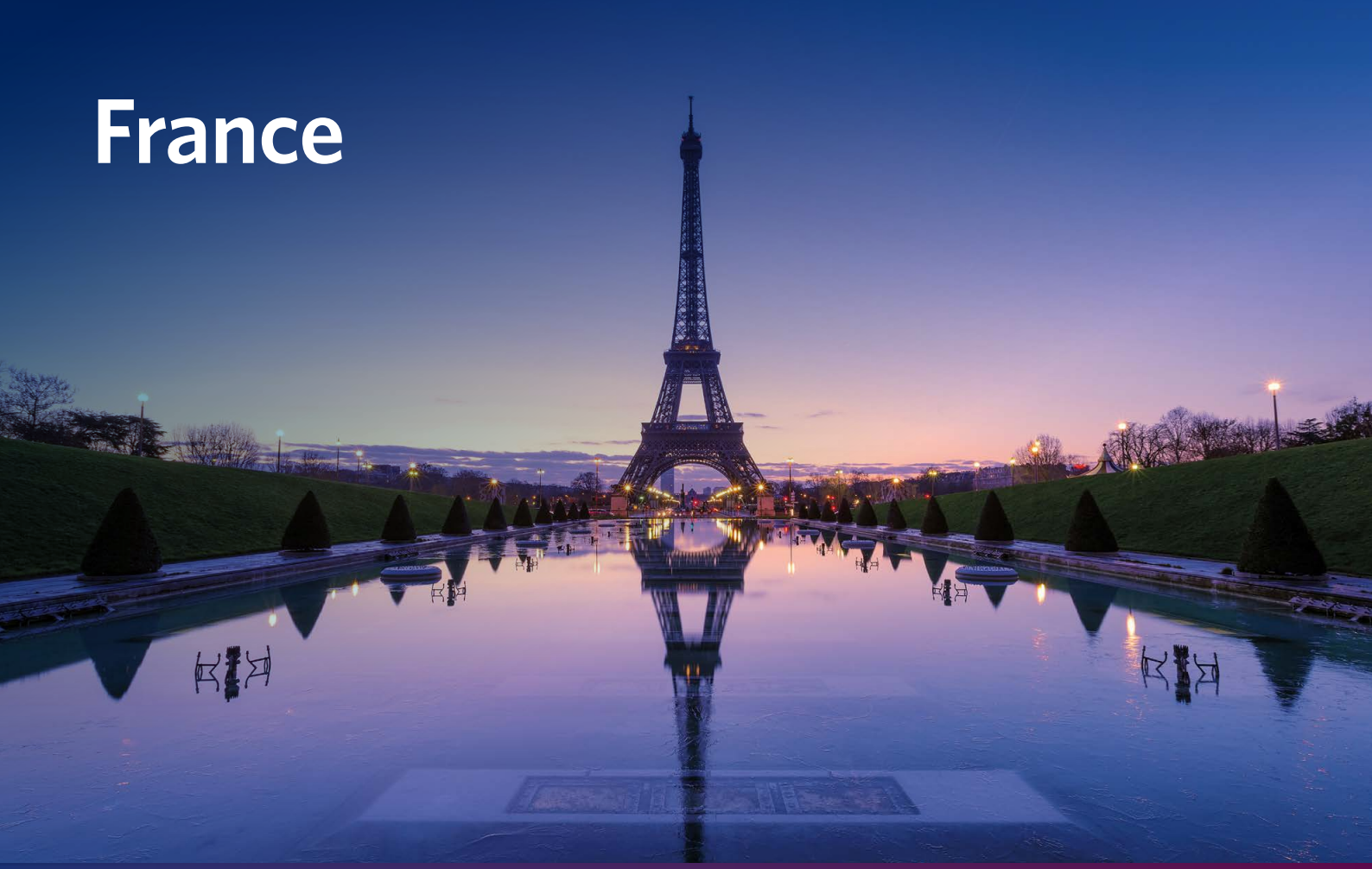
The Office of the Data Protection Ombudsman has published guidance on automated decision-making and profiling on its website. With regard to the processing of children's personal data, the guidelines set out the following:

"*Taking the special status of children into accoun, the GDPR does not explicitly provide for automated decision-making and profiling with regards to children. However, it is stated in the recitals that children should not be subjected to decisions that are based solely on automated processing and have legal effects or correspondingly significant effects. Subjecting children to automated decision-making and profiling can be justified, however, such as in order to safeguard the well-being of the child. In such cases, ensure that the appropriate protection measures are taken.*"

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

So far, no.

France



Olivier Proust
Partner, Fieldfisher
+32 2742 7015
olivier.proust@fieldfisher.com

Christopher Mesnooh
Partner, Fieldfisher
+33 1 70 37 81 14
christopher.mesnooh@fieldfisher.com

Marguerite Brac de la Perrière
Partner, Fieldfisher
+33 1 89 53 20 49
marguerite.bracdelaperriere@fieldfisher.com

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

This has not yet been decided under national law but it is likely that the French Data Protection Authority (CNIL) will become the competent authority to enforce the AI Act.

On 30 August 2022, the State Council ("**Conseil d'Etat**") published a report at the request of the French Government in which among other things, it encourages the CNIL's powers to be strengthened and its role to evolve so that it becomes the national supervisory authority responsible for regulating AI systems under the future AI regulation. The State Council highlights the importance for the future authority to act as a coordinating authority with other institutions and authorities.

To this end, the study specifies that it will be necessary to increase the CNIL's capabilities. An immediate, massive and determined investment in its resources (especially human resources) is therefore recommended to ensure the credibility of the public authorities in the development of AI systems.

On 23 January 2023, the CNIL announced the creation of a new department composed of five people (both jurists and engineers) who are fully dedicated to AI. The main missions of the Artificial Intelligence Department will be to:

- facilitate the CNIL's understanding of how AI systems work, but also for professionals and private individuals;
- consolidate the CNIL's expertise in the knowledge and prevention of privacy risks associated with the implementation of these systems;
- prepare for the implementation of the European regulation on AI (currently under discussion at European level); and
- develop relations with players in the ecosystem.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Yes. In its press release of 16 May 2023, the CNIL says that it will focus its enforcement actions on AI in three areas:

- augmented cameras used by private and public entities;
- the use of AI to combat fraud (e.g. in the field of social security);
- generative AI. Specifically, the CNIL has received several complaints against OpenAI and has launched an investigation.

As part of its enforcement actions, the CNIL will be attentive to whether users of AI systems have:

- carried out a DPIA;
- informed the data subjects; and
- implemented measures to enable individuals to exercise their rights.

On 20 October 2022, the CNIL imposed a EUR 20 million fine on CLEARVIEW AI (facial recognition software) for collecting and using personal data in France without a legal basis.

CLEARVIEW AI did not follow the CNIL's formal notice to cease the processing activities and to facilitate the exercise of individuals' rights.

Therefore, considering the "*very serious*" risks to the fundamental rights of the data subjects impacted by the processing activities carried out by CLEARVIEW AI, the Authority fined the company EUR 20 million along with an injunction of EUR 100.000 per day to cease the processing activities and to delete the data. Regardless of that, the company still did not comply with the CNIL's instructions, resulting in the enforcement of the injunction on 17 April 2023 with an additional EUR 5.2 million penalty.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

Yes. The CNIL has published a dedicated dossier on AI on its website which is available (in French only) at: **https://www.cnil.fr/fr/intelligence-artificielle-ia**

On 11 October 2023, the CNIL issued practical guidelines on the interplay between GDPR and use of AI, specifically for the development phase of an AI system. These guidelines are still open to public consultation and will likely be updated/improved. The guidelines are accessible (in French and English) at: **https://www.cnil.fr/fr/les-fiches-pratiques-ia**

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Not currently.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

The CNIL has announced that the regulation of AI is a key focus of its strategy and is structured around four objectives:

- understand how AI systems work and their impact on individuals;
- enabling and supervising the development of AI that respects personal data;
- unite and support innovative players in the AI ecosystem in France and Europe;
- audit and control AI systems and protect individuals.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

As with any processing activity, an AI system using personal data can only be implemented if it complies with one of the six legal grounds in the GDPR: consent, compliance with a legal obligation, performance of a contract, performance of a task in the public interest, safeguarding vital interests and pursuit of a legitimate interest. In practical terms, the legal basis is what gives an organisation the right to process personal data. The choice of this legal basis is therefore an essential first step in ensuring compliance. Depending on the legal basis chosen, the organisation's obligations and the rights of individuals may vary.

In its Guidelines published on 11 October 2023, the CNIL addresses the interplay between GDPR and use of AI, specifically data minimisation, purpose limitation, limited retention and secondary use of personal data in the AI system development phase.

In addition, in a decision dated 20 October 2022, the CNIL imposed a **EUR 20 million** fine on CLEARVIEW AI (facial recognition software) for collecting and using personal data in France without a legal basis.

In particular, the investigations revealed two breaches of the GDPR, namely:

- processing operations carried out without a legal basis (the CNIL considered that CLEARVIEW AI could not rely on legitimate interest nor on the individuals' consent); and
- failure to take into account the rights of individuals such as the right of access (the company restricted the right of access to twice a year and by responding to certain requests only after an excessive number of requests by the same person).

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

While the main principles of the GDPR and the Data Protection Act apply in the case of AI systems, the information to be given to individuals may vary:

- when the data has not been collected directly by the manager implementing the AI system and it is difficult to get back to the data subjects. This problem is not specific to AI processing, but is frequently encountered in the latter, particularly in the use of learning databases;
- for the exercise of certain rights (notably Article 22 of the GDPR), it is essential to provide precise explanations to the data subjects on the reasons that led to the decision in question. The complexity and opacity of some AI systems can make the provision of these elements complicated.

6.3. Data subject rights

When an AI system involves the processing of personal data, it is necessary to ensure that the principles for the exercise of rights by individuals provided for by the GDPR are complied with: access (Article 15), rectification (Article 16), erasure (Article 17), limitation (Article 18), portability (Article 20) and objection (Article 21). These rights constitute essential protection for individuals, enabling them not to suffer the consequences of an automated system without having the opportunity to understand and, if necessary, to object to data processing that concerns them. In practice, these rights apply throughout the lifecycle of the AI system, and therefore cover personal data:

- contained in the databases used for learning;
- processed during the production phase (which may include the outputs produced by the system).

Data controllers must therefore be aware from the system design stage that they must include appropriate mechanisms and procedures for responding to requests that may be received. Exceptions to the exercise of certain rights may be invoked in the case of AI processing implemented for scientific research purposes.

6.4. Automated decision making (Art. 22 GDPR)

AI systems are often part of processing operations that may involve automated decision-making mechanisms.

The data controller must therefore provide for the possibility of human intervention to enable the data subject to re-examine his or her situation, express his or her point of view, obtain an explanation of the decision taken, and contest the decision. In the case of decision-making assistance, guarantees are also necessary, particularly in terms of information.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

Controllers must be aware from the design stage of the system that they must include appropriate mechanisms and procedures for responding to requests that may be received.

Learned AI models may also contain personal data:

- by construction, as is the case for certain specific algorithms which may contain fractions of training data (e.g. SVM or certain clustering algorithms);
- by accident, as described in the section "*Protecting yourself against the risks of AI models*".

In the first case, the data controller is able to (re)identify the data subject, so that the exercise of the individual's rights can be realised.

In the second case, the rights of the persons concerned may be difficult or even impossible to exercise and satisfy.

The data controller must not collect or retain additional information to identify the data subject for the sole purpose of complying with the GDPR (Article 11). Consequently, in some cases, identifying individuals may prove complex. If the controller demonstrates that it is unable to do so, it will then be able to waive rights without prejudice to individuals providing additional information, which could enable them to be re-identified in the processing. This will be the case, for example, when a person believes that an AI system treats him or her in a particular way.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

The evaluation of AI systems is a key issue and at the heart of the European Commission's draft regulation. From a data protection point of view, it is essential in order to:

- Validate the approach tested during the system design and development phase (known as the "*learning phase*"). The aim is to verify, as scientifically and honestly as possible, that the system functions in accordance with the designers' expectations and, if necessary, is suitable for deployment in the production phase.
- Minimise the risks of system drift that can be observed over time. For example, because it is aimed at people with profiles different from those of the people whose data form the learning base, or because the system is regularly re-trained, this can lead to a deterioration in performance which is potentially harmful to the people concerned.
- Ensure that the system, once deployed in production, meets the operational needs for which it was designed. The performance obtained during the training phase must be distinguished from that of the system once in production, since the quality of the former does not prejudge that of the latter.

In its Guidelines dated 11 October 2023, the CNIL addresses how providers should conduct a DPIA (related risks to consider, measure to mitigate those risks).

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

In its Guidelines published on 11 October 2023, the CNIL addresses the allocation of roles under data protection rules when developing an AI system, more specifically:

When the provider creates the data base for training the AI system from data it selected for its own behalf, it acts as a data controller;

When the provider develops an AI system for the benefit of a client in the course of a service, it acts as a processor.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

Not specified.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

The use of AI systems can also entail risks of discrimination. There are many reasons for this, and they may stem from:

- the data used for learning, for example because they are non-representative, or because, although they are indeed representative of the "*real world*", they nevertheless reflect a discriminatory character (for example, the reproduction of wage gaps between women and men); or
- the algorithm itself is flawed in its design. This dimension, also very present in the European Commission's draft regulation, requires specific consideration by data controllers.

The CNIL gave its support to the French Defender of Rights for the publication of a report on "*Algorithms: how to prevent automated discrimination*". In particular, the report calls for a collective awareness and urges the public authorities and stakeholders concerned to take tangible, practical measures to prevent discrimination being reproduced and amplified by these technologies.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

No.

Germany

Felix Wittern
Partner, Fieldfisher
+49 40 87 88 69 8 114
felix.wittern@fieldfisher.com

Oliver Süme
Partner, Fieldfisher
+49 40 87 88 69 8 217
oliver.sueme@fieldfisher.com

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

The **competent authorities will monitor compliance with the requirements of the AI Act**. In Germany, it is not yet certain whether this supervisory authority will be newly created or attached to an existing institution (e.g., the Federal Office for Information Security "BSI"; the Federal Cartel Office or the Federal Network Agency).

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Not so far.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

The German authorities have published the following (so far):

- ***Hambach Declaration on Artificial Intelligence***, published by the German Data Protection Conference ("DSK") in 2019 (only available in German),
- **Questionnaire from the state data protection commissioners to OpenAI** about data protection regarding ChatGPT (April 2023, answer pending).
- The "DSK" has set up a "Taskforce AI" which will work on the relevant issues regarding AI and the GDPR.

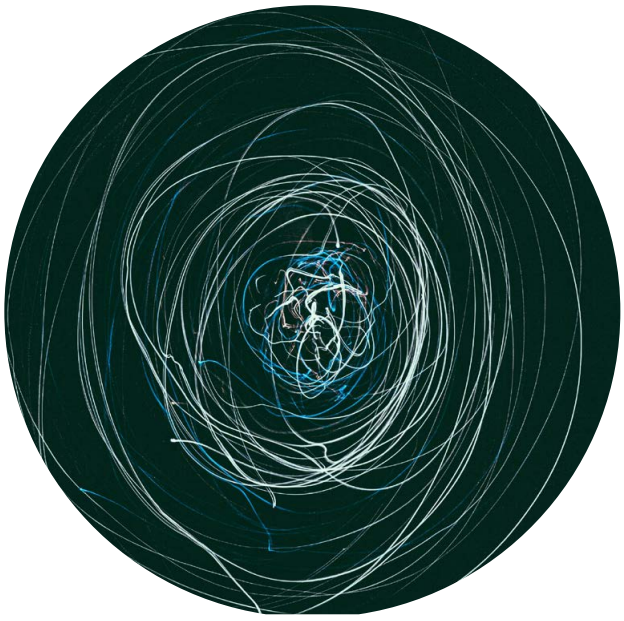
4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Not as of now.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

At the moment, the German authorities seem to focus in particular on

- **Transparency** about the (technical) details of the data processing and the technology/logic behind the AI tool as well as the use of AI,
- **Risk of discrimination**, especially in the context of automated decision making (including profiling),
- Regarding **Training Data** (if it is personal data): Source of the data and legal basis for processing the data for the purpose of training the AI model.
- Regarding **Input Data**: What happens to the Input Data? Is the data used to train the AI model?



6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

- **Changes of purpose are strictly limited by Art. 6 (4) GDPR**. Also for AI systems, extended processing purposes must be compatible with the original purpose of collection.
- Regarding **data minimisation** (especially with regard to training data): depending on the AI-tool, often completely anonymised data may be sufficient (as Training Data and as Input Data).
- **Ensuring the accuracy of the data used for training purposes is important**.
- With regard to training and training data, **discrimination tendencies are to be recognised and prevented at an early stage** of the development process.
- **Accountability, Art. 5 (2) GDPR**: the controller is responsible for the use of the AI tool.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

Regarding transparency obligations, the authorities emphasise:

- The provider of AI tools **must inform the user about the details of the data processing** (in particular logic involved, technology behind the software, data processing procedures, creation of the output).
- For provider and user: **Decisions based on AI systems must be transparent, comprehensible and explainable** (with regard to the result / the outcome as well as the technical process behind).

6.3. Data subject rights

Authorities seem to place particular emphasis on

- **Right to erasure ("right to be forgotten"), Art. 17 GDPR** (especially after using the AI model).

6.4. Automated decision making (Art. 22 GDPR)

The guaranty of human dignity (Art. 1 (1) Basic Law for the Federal Republic of Germany, "GG"; Art. 1 of the European Charter for the Protection of Human Rights and Fundamental Freedoms) requires that **the individual may not be made an object through the use of AI**, therefore:

- Fully automated decision making including profiling by AI systems is **only permitted to a limited extent**. Decisions with legal effect or similar significant impairment may **not be left solely to the machine**, according to Art. 22 GDPR.
- Data subjects also have the right to human intervention on the part of the controller (intervenability), to express his or her point of view and to contest a decision when AI systems are used.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

- The **algorithm underlying the AI system must be technically developed and designed** in such a way that **any risks are identified and minimised**, ideally eliminated, in advance, especially those associated with the use of AI.
- It must be ensured that the **Input Data of one user does not appear as Output Data** for another user.
- **Differentiation** should be made **between non-personal and personal data**. The **risk of re-identification** must be addressed.
- Personal data should always be **pseudonymised or anonymised, if possible,** before using the data for the purpose of training the AI.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

- In principle, a **DPIA must always be carried out**.
- If no DPIA is carried out, detailed reasons must be given as to why no DPIA was carried out.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

So far, the authorities have not commented on this point in any greater detail.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

So far, the authorities have not commented on this point in any greater detail.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

- **Safeguards for children and minors**: Specified age limits and corresponding verification system are necessary. In some cases, consent is also required.
- **Risk of discrimination (so-called bias)**: Any kind of discrimination must be prevented and discrimination tendencies (including hidden discrimination) detected, both while developing (training) the AI tool) and during the use of the AI-tool (risk monitoring by the developer/provider).

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

Not as of now.

Hungary

Tamás Gödölle

Partner, Bogsch & Partners

+361 318 1945
tamas.godolle@bogsch.hu

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

The National Media and Infocommunications Authority (NMHH) is responsible to prepare the AI Act. It has not yet been decided which regulatory authority will be responsible for the enforcement of the AI Act. Should the AI related activity involve personal data management, the acting authority is going to be the Hungarian Data Protection Agency (NAIH).

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

The Hungarian Data Protection Agency (NAIH) has already decided in a case, which involved AI. Budapest Bank Zrt. has implemented a software using AI solutions to analyse the recorded audio of customer service calls. The speech signal recognition and evaluation system analysed the speaker's emotional state, keywords and other characteristics, on the basis of which it established a sequence for recalling customers. The decision to recall is then taken by the bank's employees. The bank claims that it operated the application to prevent complaints and customer churn. However, it also used the data to rate the performance of its customer service staff. It did so without properly informing the data subjects.

The NAIH also assessed that the voice analysis software was operating with a rather low efficiency: the emotion was not detectable in 91.96% of the cases, so the system was not suitable for the intended purpose.

In its first decision on the unlawful use of AI, the data protection authority imposed a record fine of 250 million HUF.

The NAIH identified the following data protection shortcomings in the solution used to analyse conversations with case handlers:

- violation of fundamental principles ("*legality, fairness and transparency*" and "*purpose limitation*", Article 5(1)(a) and (b) GDPR),
- problems with processing compatible with the legal basis and the original purpose (Article 6),
- transparency and information failures (Articles 12 and 13),
- the exercise of data subjects' rights (in particular the right to object, Article 21),
- failure to apply appropriate technical and organisational measures (Article 24(1)),
- breach of the principles of data protection by design and by default (Article 25).

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

The Hungarian Government has decided to create a comprehensive Artificial Intelligence Strategy within the framework of the so-called Digital Welfare Program, setting targets up to 2030 and outlining a plan of action until 2025.

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Currently no national legislative initiatives are presented other than the national Artificial Intelligence Strategy where the development of anonymisation technologies is supported. It would help AI learning with personal data with ensuring the legal provisions. The GDPR and the national data protection laws shall be used for the AI.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

In the National AI Strategy: developing machine perception, machine learning-based intelligent manufacturing, logistics, IoT solutions development, developing language technology, developing anonymisation technologies, developing the mathematical foundations of AI

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

The national authority hasn't yet reported on the subject matter. That means the GDPR and the National Data Protection Act shall be applicable.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

The national authority hasn't reported position paper yet in the subject matter. That means the GDPR and the National Data Protection Act shall be applicable.

6.3. Data subject rights

As per the GDPR, no special provisions exist.

6.4. Automated decision making (Art. 22 GDPR)

Authorities have not yet commented in relation with AI.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

Authorities have not yet commented in relation with AI.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

As per GDPR, no further guidance or legislation has been issued related to AI.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

Authorities have not yet commented in relation with AI.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

Authorities have not yet commented in relation with AI.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

› Safeguards for children and minors: as per the provisions of the GDPR, no specific provisions exist.

› Risk of discrimination (so-called bias): Discrimination is generally prohibited in Hungary, a separate Act is enforced in this regard, which must be applied in the private and public sector. Accordingly, the general prohibition of discrimination must also be observed during AI-related developments

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

Not yet.

Ireland

Ciara Burke

Partner, Fieldfisher

+353 1 828 0976
ciara.burke@fieldfisher.com

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

It has not yet been decided which regulatory authority will become the competent authority under the EU's AI Act. In 2021, the Irish Government launched the National AI Strategy and appointed an AI ambassador. Further, the Minister of State for Trade Promotion, Digital and Company Regulation is currently seeking expressions of interest from suitably qualified individuals to serve as voluntary members of an Artificial Intelligence (AI) Advisory Council. Of note, in the most recent progress report, as part of the National AI Strategy, consideration is being given to an appropriate mechanism for ensuring a coordinated approach by Irish regulators to Digital, including AI, as part of Ireland's National Digital Strategy.

There has also recently been reports that the DPC has sent several of its staff on an Artificial Intelligence diploma course.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Nothing specific to nor focusing on AI yet.

Google's European Bard launch however, was delayed due to concerns raised by the DPC. The DPC was quoted as saying that they had not received sufficient information about the product before launch, including not having had sight of a DPIA or other supporting documentation. It subsequently sought further information from Google and raised several data protection questions about the product (**https://www.independent.ie/business/technology/googles-european-bard-launch-halted-by-irish-data-regulator-over-privacy-concerns/a623534495.html**).

With regards to the regulation of AI tools such as chatbots, the DPC has also warned against rushing into prohibitions of such tools and has instead said that governing bodies must figure out how to regulate such technology instead.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

In 2021, the Irish Government launched the National AI Strategy which is founded on three core principles: (1) adopting a human-centric approach to the application of AI; (2) staying open and adaptable to new innovations; (3) ensuring good governance to build trust and confidence for innovation to flourish. A key component of the National AI Strategy is to ensure an agile and appropriate governance and regulatory environment for AI, with a focus on the three key areas: (1) legal framework; (2) ethics; and (3) standards and certification.

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Other than GDPR (and national data protection legislation) considerations, nothing specific to data protection and AI. However, whilst not specifically focusing on GDPR and AI, in 2021, the Irish Government launched the National AI Strategy. See above.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

See above re the National Strategy for AI.

The DPC has also been reported as saying that they are trying to understand more about the technology and about where the training data is sourced (**https://nationaltechnology.co.uk/Irish_Data_Protection_Chief_Generative_AI.php**).

Further, a Deputy Commissioner from the DPC was recently quoted as saying in the context of AI products that when it comes to personal data, GDPR is king at the moment.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

So far, the DPC has not commented on this point in any great detail in the context of AI.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

So far, the DPC has not commented on this point in any great detail in the context of AI.

6.3. Data subject rights

So far, the DPC has not commented on this point in any great detail in the context of AI.

6.4. Automated decision making (Art. 22 GDPR)

So far, the DPC has not commented on this point in any great detail in the context of AI.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

So far, the DPC has not commented on this point in any greater detail in the context of AI.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

So far, the DPC has not commented on this point in any great detail in the context of AI. The DPC has however published guidance on DPIAs which includes a list of processing operations for which a DPIA is mandatory. Processing operations of note and which have been included on this list include:

(1) "*use of profiling or algorithmic means or special category data as an element to determine access to services or that results in legal or similarly significant effects*";

(2) "*Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals, particularly where the data sets are combined from different sources where processing was / is carried out for different purposes of by different controllers*".

Guidance: **https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf**

It is also worth noting that the European launch of Google's Bard AI tool was delayed, with the DPC stating that it did not receive sufficient information nor had sight of a DPIA or supporting documentation.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

So far, the DPC has not commented on this point in any great detail in the context of AI.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

So far, the DPC has not commented on this point in any great detail in the context of AI.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

In October 2022, the Department of Enterprise, Trade and Employment, in cooperation with the Department of Children, Equality, Disability, Integration and Youth, convened a National Youth Assembly on AI to gather the views of young people. Recommendations from this assembly are to be considered as part of the National AI Strategy.

Further the DPC's Fundamentals for a Child-Oriented Approach to Data Processing currently suggest that organisations may consider AI tools to "know" their audience, possibly for age verification purposes (to be determined on a case by case basis and grounded on a risk based approach). Despite the DPC stating that it was considering the addition of further guidance addressing the use of AI for identifying child users in response to the public consultation, such guidance was not included in the final published Fundamentals. The Fundamentals further mention artificial intelligence without human involvement / a human element in the context of profiling and triggering requirements in that regard.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

Not yet.

Italy

Diego Rigatti
Partner, Fieldfisher

+39 041 2905711
diego.rigatti@fieldfisher.com

Francesca Gravili
Partner, Fieldfisher

+39 02 806731
francesca.gravili@fieldfisher.com

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

This has not yet been decided under national law but it is likely that the Italian Data Protection Authority ("**Garante**") will become the competent authority to enforce the AI Act.

In a recent interview, Guido Scorza, a member of the Italian Data Protection Authority stated: "It is a fact that, currently, in Europe, ensuring compliance with the provisions enacted on the basis of Article 16 TFEU is the task of the national Data Protection Authorities, also through the European Data Protection Board [EDPB], which ensures their coordination, and, to the extent of its competence vis-à-vis the European Institutions, of the European Data Protection Supervisor [EDPS].

In this respect, therefore, in spite of the ambiguity currently present in the proposed Regulation (see Article 59), **it seems difficult to assume that national DPAs may not be identified as national supervisory authorities also with regard to artificial intelligence**.

The Garante has established an ad hoc department for Artificial Intelligence. These initiatives were deliberated on 27 May 2021 by the Authority.

In February 2023, the Garante launched a call for professional consultants in the field of artificial intelligence.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Yes, please find the list of the relevant Garante decisions:

› **Injunction Order against Clearview AI** - 10 February 2022. Focuses on the unlawful processing of personal data carried out by the owner with reference to the way in which the AI was fed, through web scraping.

› **Order of 2 February 2023 against Replika**: AI-powered chatbot equipped with a text and voice interface generating a "*virtual friend.*" Users can configure as a friend, partner or mentor; noting that those tests had reportedly pointed to factual risks to minors and, generally speaking, emotionally vulnerable individuals.

EN Version: **https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9852214#english**

› **Order of 11 April 2023 against Open AI - ChatGPT ("ChatGPT Order")** The Italian SA highlights that no information is provided to users and data subjects whose data are collected by Open AI; more importantly, there appears to be no legal basis underpinning the massive collection and processing of personal data in order to 'train' the algorithms on which the platform relies. As confirmed by the tests carried out so far, the information made available by ChatGPT does not always match factual circumstances, so that inaccurate personal data are processed. Finally, the Italian SA emphasises in its order the lack of an age verification mechanism exposes children to receiving responses that are absolutely inappropriate to their age and awareness, even though OpenAI's terms state the service is for users over 13 years old.

EN version: **https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702#english**

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

Yes. The Italian authorities have published the following (so far):

› **Garante**: the project "*The Words of AI*" - A series of videos on the main issues related to artificial intelligence and their relationship with data protection. h**ttps://www.youtube.com/GARAntedatipersonaliGP** (Italian);

› the **Agency for Digital Italy - *Agenzia per l'Italia Digitale* (Italian government agency)**: a white paper "AI from justice to transport, from cultural heritage to health and education: the book outlines challenges and recommendations for a sustainable and responsible use of Artificial Intelligence in Public Administration" **https://ia.italia.it/assets/librobianco.pdf**;

› the **Italian Government**: the Artificial Intelligence Strategic Programme 2022-2024 (November 2021) **https://assets.innovazione.gov.it/1637937177-programma-strategico-iaweb-2.pdf**;

› the **Ministry of Economic Development**: Italian Strategy for Artificial Intelligence (June 2020) **https://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf**.

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Not currently.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

The **Garante** focuses in particular on (for reference **ChatGPT Order**):

(a) transparency about the (technical) details of the data processing and the technology/logic behind the AI tool as well as the use of AI (i.e. Easy-to-find and easy-to-read privacy policy);

(b) availability of an easy way to object and to exercise the right of erasure and rectification;

(c) identification of the correct legal basis for processing data (not performance of a contract, but legitimate interest);

(d) effective age verification process in place.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

As per France.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

Please, refer to answer n.5, letter a).

6.3. Data subject rights

Please, refer to answer n.5, letter b).

6.4. Automated decision making (Art. 22 GDPR)

N/A.

6.5. Data Protection by Design and Data Protection by Default

Especially technical and organisational measures, Art. 24 and 25 GDPR

For the time being, there are no specific indications by the Garante.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

As per Germany.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

For the time being, there are no specific indications by the Garante.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

In the injunction Order against Clearview AI - 10 February 2022, the Garante confirms the respect of the requirements of Chapter V GDPR.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

The Garante required the "*deployment of age verification tools(...), whereby users aged under 13 should be prevented from accessing the service along with users aged under 18 in the absence of an express indication of consent by the person exercising parental authority over the latter*" (for reference **ChatGPT Order**).

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

No.

Netherlands

Ady Van Nieuwenhuizen

Partner, Fieldfisher

+31 20 225 220
ady.vannieuwenhuizen@fieldfisher.com

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

This is not yet decided, it is likely however that it will be one or more regulators that are already active within the digital domain:

(1) In the Netherlands, seven regulators in total are active within the digital domain. The Authority Consumers and Market (ACM), the Financial Markets Authority (AFM), the Data Protection Authority (DPA) and the Dutch Media Authority (Commissariaat voor de Media (CvdM)). In addition, the College for the Human Rights (CHRM), De Nederlandsche Bank (DNB) and the State Inspectorate for Digital Infrastructure (RDI). These regulators regularly have to deal with supervision of algorithms and more complex algorithmic systems also known as AI.

https://open.overheid.nl/documenten/a0e22cc8-45e9-4bf2-9d24-05099c142ea9/file

(2) Dutch Data Protection Authority (Autoriteit Persoonsgegevens) will be involved because of the overlap between GDPR and AI enforcement. In addition to that they recently published information regarding AI and algorithms:

"Overseeing the proper use of algorithms involving personal data is part of the work of the DPA. The DPA only monitors compliance with data protection laws. However, the development and deployment of algorithms can also have consequences for other areas of law, such as (among others) consumer law, competition law and anti-discrimination. For this reason, the DPA will also cooperate with other national regulators in the area of algorithms and AI. For example, the DPA has consulted experts from various departments, from other regulators and academics."

https://autoriteitpersoonsgegevens.nl/uploads/imported/toezicht_op_ai_en_algoritmes.pdf

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

The DPA imposed administrative fines of a total of €2,750,000 for violation of Articles 5, 6 and 8 of the Protection of Personal Data Act (the predecessor to the GDPR). This is because for years, the Dutch Tax Authority Belastingdienst has processed the (dual) nationality of applicants for child care benefits in an unlawful, discriminatory and therefore improper manner. **Part of the fine was imposed for the use of a self-learning risk classification model.**

https://www.autoriteitpersoonsgegevens.nl/documenten/boete-belastingdienst-kinderopvangtoeslag

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

1. Strategic action plan for artifical intelligence published by the Dutch Government:

https://ai-watch.ec.europa.eu/countries/netherlands/netherlands-ai-strategy-report_en

2. In 2020 a handbook for GDPR and AI has been created by the government:

https://www.datavoorgezondheid.nl/documenten/publicaties/2020/01/27/handreiking-avg-en-ai

3. The DPA has published a guideline on automated decision making and profiling:

https://www.autoriteitpersoonsgegevens.nl/documenten/guidelines-geautomatiseerde-besluitvorming-en-profilering

4. The DPA started a landing page on their website regarding AI and algorithms:

https://autoriteitpersoonsgegevens.nl/themas/algoritmes-ai

They also published a report on this topic:

https://autoriteitpersoonsgegevens.nl/actueel/primeur-eerste-rapportage-algoritmerisicos-nederland

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Regarding regulation, the Dutch Government advocates an ethical, trustworthy and responsible use of AI with respect for human rights and consumer protection, and based on a well-developed legal framework. Policy actions relate to various research activities on ethical, legal and transparency aspects, and responsible use of AI. The Netherlands AI coalition has for instance developed the concept of ELSA labs (ELSA refers to Ethical, Legal and Societal Aspects) to enhance synergies between research, education and organisations on human-centric AI. The Dutch Government also highlights its active participation into High Level Experts Groups and European Directives on these issues. Several reforms to the legislation are ongoing to support the protection of public values and encourage the use of AI in a trustworthy environment: **https://ai-watch.ec.europa.eu/countries/netherlands/netherlands-ai-strategy-report_en#regulation**

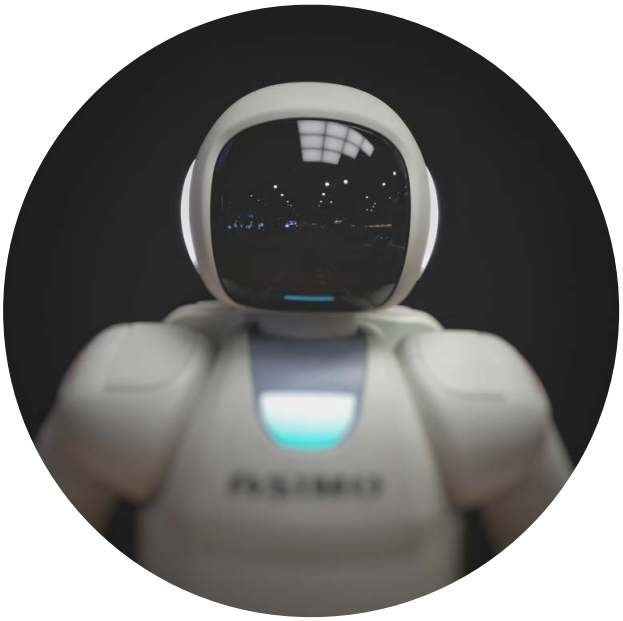
5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

For the regulators we know the focus is on AI and algorithms based on the published materials to date.

According to the Strategic Action Plan published by the House of Representatives the following have been highlighted as the current focus of national regulators when it comes to regulating AI:

- High-quality research and innovation,
- A workforce with the right knowledge and skills to develop and work with AI,
- Access to sufficient high-quality data and high-quality and intelligent digital connectivity; and
- Opportunities in solving social challenges.

Strengthening the foundations is necessary to take advantage of the opportunities of AI and address the risks. In doing so, the government is committed to protecting the fundamental rights of citizens and providing appropriate ethical and legal frameworks. (**https://open.overheid.nl/documenten/ronl-e14cdcee-690c-4995-9870-fa4141319d6f/pdf**)



6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

The Dutch DPA comments on these topics, specifically AI and algorithms, on their website. However, this is a very high level overview that does not deviate from the general GDPR rules.

https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/algoritmes-ai-en-de-avg/regels-bij-gebruik-van-ai-algoritmes

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

General

Processors must be transparent towards data subjects.
There is also the obligation to draw up a processing register (Art. 30 AVG).

Specific

When algorithms are used, information must be provided about the underlying logic and the expected consequences of that processing for the data subject.

A mandatory algorithm register applies to public authorities.

https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/algoritmes-ai-en-de-avg/regels-bij-gebruik-van-ai-algoritmes

6.3. Data subject rights

No specific guidance.

6.4. Automated decision making (Art. 22 GDPR)

No specific guidance.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

When developing (algorithmic) systems, you must consider the principles of privacy by design and privacy by default. This means that you must develop, set up and deploy privacy-friendly systems. Settings for the user must be privacy protected by default. (**https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/algoritmes-ai-gebruiken**)

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

Are you using algorithmic systems in a project and will personal data be processed in the process? If so, it is mandatory to conduct a data protection impact assessment (DPIA). With a DPIA, you identify the privacy risks of data processing in advance. You can then take measures to reduce the risks. (**https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/algoritmes-ai-gebruiken**)

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

So far, the authorities have not commented on this point in any greater detail.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

Third countries are all countries outside the European Union (EU), except those that are part of the EEA. These are Norway, Liechtenstein and Iceland. These 3 countries have the same level of personal data protection as the EU. The main rule is that you may only transfer personal data to third countries that have an adequate level of protection. Does a third country not have an adequate level of protection? Then transfer is only allowed under one of the legal provisions in Chapter V of the General Data Protection Regulation (GDPR). It is possible to transfer personal data to a third country in 3 cases. Namely on the basis of: an adequacy decision; appropriate safeguards, such as a model contract, code of conduct, certification or "binding corporate rules" (BCR); specific exceptions. (**https://www.autoriteitpersoonsgegevens.nl/themas/internationaal/doorgifte-binnen-en-buiten-de-eer/doorgifte-persoonsgegevens-buiten-de-eer**)

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

If you want to process children's data gathered online or use children's personal data for marketing purposes or to create personality or user profiles, you may only do this for children under 16 with the consent of their parents or guardians.

(**https://autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd**)

Guidance on non-discrimination Artificial Intelligence (AI) **https://www.rijksoverheid.nl/documenten/apporten/2022/12/05/handreiking-non-discriminatie-artificial-intelligence-ai**

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

Not specifically for generative AI.

However, a handbook has been created by the government: **https://www.datavoorgezondheid.nl/documenten/publicaties/2020/01/27/handreiking-avg-en-ai**

The research report provides insights into the changes resulting from application of AI, the risks and possible approaches for Telecom Agency to maintain societal trust in telecom infrastructure. **https://www.rdi.nl/onderwerpen/kunstmatige-intelligentie/documenten/rapporten/2020/06/30/dialogic-gebruik-van-en-toezicht-op-ai-toepassingen-in-telecominfrastructuren**

Norway

Ståle L Hagen

Partner, Selmer

+47 934 90 842
s.hagen@selmer.no

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

This is not yet decided. The government has been requested to establish an algorithm authority, but a final decision has not yet been made. As for the use of artificial intelligence in connection to personal data, the Norwegian Data Protection Authority (the "**NDPA**") is the responsible authority.

It appears to be probable that the NDPA will also be responsible for the enforcement of the AI Act, if no new authority for the surveillance of algorithms used for artificial intelligence is established.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Nothing neither specific to nor focusing on AI yet.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

Yes, the following have been published:

1. ***The National Strategy for Artificial Intelligence***, Ministry of Local Government and Regional Development (2020), available here: **https://www.regjeringen.no/en/dokumenter/nasjonal-strategi-for-kunstig-intelligens/id2685594/?ch=1**

An important part of the strategy for AI, was the creation of a regulatory privacy sandbox initiative, supervised by the NDPA. Norwegian enterprises working with AI and privacy may apply for their projects to be included in the sandbox project. If they are elected, the NDPA will provide them with free guidance on regulatory requirements during a testing period.

2. The NDPA's framework for the regulatory sandbox, available here: **https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/framework-for-the-regulatory-sandbox/**

The regulatory sandbox will provide free guidance to selected private and public organisations of different types and sizes and from different sectors.

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Nothing neither specific to nor focusing on AI yet.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

Due to the lack of legislative initiatives regarding AI (yet), not much has been said. However, the NDPA have expressed that the objective for the regulatory sandbox is to promote development and implementation of "ethical and responsible artificial intelligence from a privacy perspective."

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

Norway has implemented the GDPR through the Norwegian Data Protection Act, and the legal grounds for processing of personal data are the same as per the GDPR. What has been set out to apply in Spain, can also be applied in Norway.

The government has addressed that the development of AI will create new and complex issues related to privacy, but it has not made any specific regulations on the processing of personal data in AI that deviates from the general rules of the GDPR and the Data Protection Act. NDPA has stated that use of AI does not deviate from what otherwise applies to processing of personal data.

https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/algoritmes-ai-en-de-avg/regels-bij-gebruik-van-ai-algoritmes

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

Norway has implemented the GDPR through the Norwegian Data Protection Act, and what has been set out to apply in Spain, can also be applied in Norway.

In addition, the NDPA has published a guideline on how to succeed with transparency while AI is used in connection with the processing of personal data. The guideline does not provide much beyond what is already outlined in GDPR Articles 13 and 14.

The transparency requirements in the application phase depend on whether an AI model is used for decision-support or to produce automated decisions. The NDPA recommends that the processor discloses the information necessary for automated decisions, even when the AI model is used for decision support. This is particularly important where meaningful information about the AI system's underlying logic can help the data subject to better uphold their rights.

6.3. Data subject rights

Norway has implemented the GDPR through the Norwegian Data Protection Act, and what has been set out to apply in Spain, can also be applied in Norway.

In addition, the NDPA wrote a report on data protection and AI in January 2018, where the data subjects rights were addressed. However, the NDPA only assessed the requirements of the GDPR. There are no special national requirements for data subjects' rights beyond those outlined in the GDPR chapter III.

6.4. Automated decision making (Art. 22 GDPR)

Norway has implemented the GDPR through the Norwegian Data Protection Act, and what has been set out to apply in Spain, can also be applied in Norway.

The NDPA has not made any AI specific comments regarding this topic.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

Norway has implemented the GDPR through the Norwegian Data Protection Act, and what has been set out to apply in Spain, can also be applied in Norway.

The NDPA has not made any AI specific comments regarding this topic.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

Norway has implemented the GDPR through the Norwegian Data Protection Act, and what has been set out to apply in Spain, can also be applied in Norway.

The NDPA emphasised the importance of conducting a DPIA in accordance with art. 35 GDPR in the 2018 report on AI and data protection (only available in Norwegian).

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

Norway has implemented the GDPR through the Norwegian Data Protection Act, and what has been set out to apply in Spain, can also be applied in Norway.

The NDPA has not made any AI specific comments regarding this topic.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

Norway has implemented the GDPR through the Norwegian Data Protection Act, and what has been set out to apply in Spain, can also be applied in Norway.

The NDPA has not made any AI specific comments regarding this topic.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

Norway has implemented the GDPR through the Norwegian Data Protection Act, and what has been set out to apply in Spain, can also be applied in Norway.

The NDPA has not made any AI specific comments regarding this topic.

Guidance on non-discrimination Artificial Intelligence (AI)

https://www.rijksoverheid.nl/documenten/apporten/2022/12/05/handreiking-non-discriminatie-artificial-intelligence-ai

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

Nothing neither specific to nor focusing on AI yet.

Poland

Marek Korcz

Partner, Laszczuk

+48 22 351 00 67
marek.korcz@laszczuk.pl

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

There is no official candidate for an authority primarily responsible for the enforcement of the AI Act. It could be potentially the President of the Data Protection Office or the President of the Competition and Consumer Protection Office.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

To our best knowledge so far, no. However, currently there is a pending case in which Personal Data Protection Office investigates Open AI and potential mishandling of data of one of its users and lack of transparency. (**https://uodo.gov.pl/en/553/1567**).

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

The Council of Ministers, by resolution of 28 December 2020, established a general "*Policy for the development of artificial intelligence in Poland from 2020*" ("**AI Policy**"). The Policy is of a general character and describes opportunities related to AI for Polish business, academics, public bodies and society. It also sets forth goals for the state that should be aimed for so Poland can benefit from AI.

https://www.gov.pl/attachment/fc404068-7a75-4404-8167-a66fb73c067f

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

There are no legislative initiatives which may result in separate Polish regulation - it seems that the Polish government is rather awaiting EU regulations in this respect.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

At the moment there has not been any communication from the Polish DPA about regulating AI separately from the EU. The Polish government has published the "*Policy for the development of artificial intelligence in Poland from 2020*" that seem to focus in particular on:

- the effective protection of fundamental rights and the development of secure, trustworthy, and ethically sound artificial intelligence systems,
- providing opportunities for the development of artificial intelligence solutions, in particular the possibility for SMEs to develop artificial intelligence,
- creating a favourable environment for investment in the development of such solutions, as well as for the widespread use of AI systems for the benefit of society.

As mentioned above the Policy is of a general character and describes opportunities related to AI for Polish business, academics, public bodies and society as well as sets forth goals for the state that should be aimed for so Poland can benefit from AI.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

So far, the Polish DPA has not commented on this point in the context of AI.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

So far, the Polish DPA has not commented on this point in the context of AI.

6.3. Data subject rights

So far, the Polish DPA has not commented on this point in the context of AI.

6.4. Automated decision making (Art. 22 GDPR)

So far, the Polish DPA has not commented on this point in the context of AI.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

So far, the Polish DPA has not commented on this point in the context of AI.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

The President of the Personal Data Protection Office included in the lists of processes requiring a personal data protection impact assessment a creditworthiness assessment, using artificial intelligence algorithms.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

So far, the Polish DPA has not commented on this point in the context of AI.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

So far, the Polish DPA has not commented on this point in the context of AI.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

None.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

None.

Portugal

Mónica Oliveira Costa

Partner, Coelho Ribeiro e Associados

+351 21 383 90 60
monica.costa@cralaw.com

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

In Portugal it is not yet certain whether this supervisory authority will be newly created or attached to an existing institution.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Not so far. Nevertheless, in December of 2019 the Portuguese DPA did not authorise the use of AI in CCTV systems by two Municipalities because such use must be well based with a careful analysis of the risks to people's rights and a careful evaluation of the measures planned to mitigate them, which, under the opinion of the Portuguese DPA, was not made.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

In 2019 the National Strategy for AI was published - AI Portugal 2030 available at **https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBAAAAB%2bLCAAAAAAABACzMDQxAQC3h%2byrBAAAAA%3d%3d** and in 2022 it published the Guide to Ethical, Transparent and responsible AI in Public Administration available at **https://bo.tic.gov.pt/api/assets/etic/95bcaf56-87ba-446b-9f0b-ab06e1549aa0/**.

The Portuguese Competition Authority has also published two policies addressing the use of monitoring and pricing algorithms available at **https://www.concorrencia.pt/sites/default/files/processos/epr/Digital%20Ecosystems%2C%20Big%20Data%20and%20Algorithms%20-%20Issues%20Paper.pdf** and **https://www.concorrencia.pt/sites/default/files/documentos/estudosrelatorios/Defence%20of%20Competition%20in%20the%20Digital%20Sector%20in%20Portugal.pdf**.

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Not currently, except the following:

a) Portuguese charter on human rights in the digital age (Law 27/2021 of May, 17) which foresees the following:

1 - The use of artificial intelligence must be guided by respect for fundamental rights, ensuring a fair balance between the principles of explainability, security, transparency and accountability, taking into account the circumstances of each specific case and establishing procedures to avoid any prejudice or discrimination.

2 - Decisions with a significant impact on the sphere of recipients that are taken using algorithms must be communicated to the interested parties and be subject to appeal and audit, under the terms provided for by law.

3 - The principles of beneficence, non-maleficence, respect for human autonomy and justice, as well as the principles and values enshrined in Article 2 of the Treaty on European Union, namely non-discrimination and tolerance, shall apply to the creation and use of robots.

b) Portuguese Labour Code that foresees the following:

1. The right to equality in access to employment and at work applies equally in the case of decision-making based on algorithms or other artificial intelligence systems.

2. The employer shall provide information to its employees on the parameters, criteria, rules and instructions on which algorithms or other artificial intelligence systems that affect decision-making on employment access and retention, as well as working conditions, including profiling and job monitoring, are based (the works council as well as the union delegate also have the right to this information).

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

Based on the National Strategy for AI and the Guide above referred, the focus is to promote research and innovation in this specific area, in favour of its development and application in fields such as public administration, education, training and business and ensure it is ethical, transparent and responsible.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

For the time being, there is no specific position in the context of AI by the Portuguese DPA on this aspect . Thus, these principles shall apply to AI whenever personal data is processed.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

For the time being, there is no specific position in the context of AI by the Portuguese DPA on this aspect. Thus, transparency shall apply to AI whenever personal data is processed.

6.3. Data subject rights

For the time being, there is no specific position in the context of AI by the Portuguese DPA on this aspect. Thus, data subject rights shall apply to AI whenever personal data is processed.

6.4. Automated decision making (Art. 22 GDPR)

For the time being, there is no specific position in the context of AI by the Portuguese DPA on this aspect. Thus, Article 22 GDPR on automated decision making shall apply to AI whenever personal data is processed.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

For the time being, there is no specific position in the context of AI by the Portuguese DPA on this aspect. Thus, data protection by design and by default shall apply to AI whenever personal data is processed.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

For the time being, there is no specific position in the context of AI by the Portuguese DPA on this aspect. Thus, Article 35 GDPR and the Regulation 1/2018 of the Portuguese DPA that approved the list of the data processings for which a DPIA is mandatory shall apply to AI whenever personal data is processed.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

For the time being, there is no specific position in the context of AI by the Portuguese DPA on this aspect.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

For the time being, there is no specific position in the context of AI by the Portuguese DPA on this aspect. Thus, Chapter V of the GDPR and particularly transfers of data outside the EU shall apply to AI whenever personal data is transferred.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

For the time being, there is no specific position in the context of AI by the Portuguese DPA on this aspect.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

For the time being, no. The Portuguese DPA has stated that it will act in line with the other EU DPAs and the EDPB

Slovakia

Ivan Rames

Partner, Havel & Partners

+420 255 000 949
ivan.rames@havelpartners.cz

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

It has not yet been determined which Slovak authority will take responsibility for enforcing the AI law in Slovakia.

Nevertheless, on the basis of the Preliminary Opinion of the Slovak Republic on the AI Act (2021), the Office for Personal Data Protection of the Slovak Republic ("**Authority**") is applying for this position. The Authority itself has not published any relevant statement or opinion on this matter.

Currently, in relation to AI-related strategies, the Ministry of Investments, Regional Development and Informatisation of the Slovak Republic ("**MIRRI**") has prepared action plans and strategies involving the development and anchoring of AI in Slovakia. Based on the interest of this Ministry, a Permanent Commission on Ethics and Regulation of Artificial Intelligence has been established for the purpose of assessing legal, ethical and other issues related to the development and use of technologies with AI elements.

In this context, the Slovak Centre for Artificial Intelligence Research - slovak.AI was also established as an independent platform for discussions.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Currently, we are not aware of any sanctions imposed by the authorities in this respect.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

We are not aware of any published guidelines or position paper regarding key issues of the AI yet.

Currently, as we outlined above, MIRRI has published a paper on the Digital Transformation Strategy of Slovakia (only in Slovak), in which it discusses the allocation of financial resources for the development of AI and its inclusion in public administration systems, etc. However, it is only a strategic document without any binding force.

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

We are not aware of any such legislative initiatives other than the potential initiatives of the entities listed in response to question 1.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

No relevant authorities have clearly commented on this issue. Attitudes on this topic may also be changing in the light of the recent parliamentary elections in Slovakia.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

Exclusively in relation to AI, the Authority has not published any position in this regard. The Slovak legislation on data protection does not differ substantially from the GDPR in this respect.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

Exclusively in relation to AI, the Authority has not published any position in this regard. The Slovak legislation on data protection does not differ substantially from the GDPR in this respect.

6.3. Data subject rights

Exclusively in relation to AI, the Authority has not published any position in this regard. The Slovak legislation on data protection does not differ substantially from the GDPR in this respect.

6.4. Automated decision making (Art. 22 GDPR)

Exclusively in relation to AI, the Authority has not published any position in this regard. The Slovak legislation on data protection does not differ substantially from the GDPR in this respect.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

Exclusively in relation to AI, the Authority has not published any position in this regard. The Slovak legislation on data protection does not differ substantially from the GDPR in this respect.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

Exclusively in relation to AI, the Authority has not published any position in this regard. The Slovak legislation on data protection does not differ substantially from the GDPR in this respect.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

Exclusively in relation to AI, the Authority has not published any position in this regard. The Slovak legislation on data protection does not differ substantially from the GDPR in this respect.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

Exclusively in relation to AI, the Authority has not published any position in this regard. The Slovak legislation on data protection does not differ substantially from the GDPR in this respect.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

Exclusively in relation to AI, the Authority has not published any position in this regard. The Slovak legislation on data protection does not differ substantially from the GDPR in this respect.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

No.

Spain

Carlos Pérez
Partner, Fieldfisher
+34 93 415 00 88
carlos.perez@fieldfisher.es

Sonia Gracia
Senior Lawyer, Fieldfisher
+34 93 415 00 88
sonia.gracia@fieldfisher.es

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

The Spanish Agency for the Supervision of Artificial Intelligence (AESIA - Agencia Española para la Supervisión de la Inteligencia Artificial). The creation of this authority was approved in 2021, and its offices are placed at La Coruña. The statutes of the agency were recently passed in September 2023, which means that it will start its operations in a 3 month period.

In addition, the Spanish Government has approved a National Strategy on Artificial Intelligence, which can be found at **https://portal.mineco.gob.es/es-es/digitalizacionIA/Paginas/ENIA.aspx**

According to AESIA's statutes, AESIA will most likely assume competence over the implementation of the AI Act.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Not so far.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

Since the AESIA is not operational yet, the only regulatory authority that has published papers and guidelines regarding the use and development of AI elements is the Spanish data protection authority:

(i) Guidelines to ensure GDPR compliance for AI solutions, products and services (see at **https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-una-guia-para-adaptar-al-rgpd-los-productos-y** and **https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf**);

(ii) Guidelines to audit AI products and services under GDPR (**https://www.aepd.es/sites/default/files/2021-01/requisitos-auditorias-tratamientos-incluyan-ia.pdf**); and

(iii) Guidelines addressing governments and public administrations with recommendations for the use and implementation of new technologies, including AI (**https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-guia-nuevas-tecnologias-aapp**).

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Yes, particularly in one field. Legislation on Gender Equality and Non-Discrimination includes a specific reference to artificial intelligence. Article 23 of the Spanish Law (Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación), says as follows:

1. In the context of the National Artificial Intelligence Strategy, the Digital Rights Bill and European initiatives on Artificial Intelligence, public administrations shall encourage the implementation of mechanisms so that the algorithms involved in decision-making used in public administrations take into account criteria of minimisation of bias, transparency and accountability, whenever technically feasible. These mechanisms will include their design and training data, and address their potential discriminatory impact. To this end, impact assessments will be promoted to identify potential discriminatory bias.

2. Public administrations, within the scope of their competences in the field of algorithms involved in decision-making processes, shall prioritise transparency in the design and implementation and the interpretability of the decisions taken by them.

3. Public administrations and companies shall promote the use of Artificial Intelligence that is ethical, reliable and respectful of fundamental rights, especially following the recommendations of the European Union in this regard.

4. A quality seal for algorithms shall be promoted.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

Since AESIA will not be operational for at least the next 3 months, no reference can be made to this regulator, although there are several papers and documents published by the Spanish Government promoting and encouraging the use and development of AI systems. The Spanish data protection Authority focuses on (i) quality and security; (ii) GDPR compliance to ensure high ethical standards and avoid biases; (iii) transparency and risk management approach (completed by audit and certification) and (iv) accountability and ultimate responsibility of the promotor of the AI initiative.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

Changes of purpose are strictly limited by Art. 6 (4) GDPR. Also for AI systems, extended processing purposes must be compatible with the original purpose of collection. The Spanish DPA also assesses that the life cycle of data in an AI system is an essential part, and the legal basis applicable to each stage should be evaluated, as the legal basis may vary.

In addition, the Spanish DPA remarks in its guidelines that *"the lapse of an existing valid legal basis, such as the withdrawal of consent, does not have a retroactive effect in relation to the results obtained in a processing operation already carried out. For example, where personal data have been used to train an AI component, the extinction of the legal basis does not invalidate the exploitation of the model, although the controller has to heed requests for the exercise of data protection rights".*

Data subjects subject to automated decision-making or profiling must be informed about *"the meaningful information on the logic applied" and "the significance and intended consequences",* such as the details of the data used for decision making, the relative importance of each data in the decision quality of the training data and the type of patterns used, profiling performed and its implications or the existence or not of qualified human supervision.

To support compliance with the obligation to inform, the Spanish DPA has published the Guide for Compliance with the Duty to Inform (see **https://www.aepd.es/sites/default/files/2019-11/guia-modelo-clausula-informativa.pdf**), as well as a specific note on the duty to inform and other measures of proactive responsibility in apps for mobile devices (**https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf**).

The Spanish DPA in its guidelines on AI systems and GDPR also points out the importance of creating governance models when different data controllers intervene in the data lifecycle that allow sufficient traceability to be generated to identify the data controller at each stage when a data right is exercised.

Data accuracy:

- When training data, metrics, cleaning and traceability techniques have to be employed to ensure the fidelity and integrity of the dataset.
- Data controllers should properly differentiate soft (subjective) data from hard (objective) data. Hard data are not free from biases, but controllers should take special care to assess the accuracy issues that may arise from giving greater prominence to soft data as a source of information.

The Spanish DPA also pays attention to the need of carrying out algorithmic impact assessments aimed at examining and determining the possible existence of biases in the algorithms that support the AI system.

Regarding data minimisation (when establishing the extent of the data categories to be used in the AI tool): the use of proxy variables needs to be justified. It is important that data minimisation not only takes place during the analysis phase, but also throughout the entire data processing.

Accountability: clear identification of the functions in relation to the audited processing, risk analysis for rights and freedoms, study of the necessity and proportionality of the processing and the different risk management measures, privacy measures by default and by design, security measures, incident management, etc.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

Regarding AI-based processing, transparency can be considered a critical aspect:

- Data subjects must be able to access all information on the processing of their data by AI, in an easy, understandable, concise manner and in simple and clear language.
- Data subjects must be informed about the impact that the use of AI may have, as well as the actual efficiency, capabilities and limitations of AI tools.
- Creation of false expectations among data subjects must be avoided.
- Transparency is also linked to information about the context and status of the processing, such as the existence of third parties and/or the physical/virtual location of the AI solution.
- Transparency should be understood as a principle around which the processing carried out orbits dynamically and which affects each and every element and participants involved in the solution.
- It is mandatory not to rely solely on the representations of providers, but to establish mechanisms based on reliable third parties to determine the necessary levels of quality and reliability.
- The use of AI tools does not imply an obligation to have a DPO, but it can be very useful for entities using AI-tools in order to comply with this principle.

The Spanish DPA remarks the need to explain the logic applied to automated decision-making or profiling. It pays particular attention to the need to explain to the data subject what logic is followed and the intended consequences, in compliance with Article 13(2)(f) of the GDPR. This means providing the data subject with information that makes them aware of the type of processing that is being carried out on their data and provides them with certainty and confidence about the results.

6.3. Data subject rights

Generalities on the exercise of rights:

As mentioned previously, in case where personal data are distributed among a network of controllers, an effective information governance model has to be included to address correctly each exercise of rights.

Regarding specific exercise of rights:

- Right of access: to be exercised by the person responsible for each stage of the lifecycle of the AI solution involving personal data.
- Right of rectification: The responsible person has the obligation to attend to the right of rectification of the data of the interested parties, especially those generated by the inferences and profiles elaborated by the AI solution.
- Right to erasure: When the training stage of the AI system is completed, controllers shall implement their removal, unless the need to maintain such data is justified for the purpose of system refining or evaluation.
- Right to data portability: Controller has to assess and document whether its processing is obliged to provide data portability of data subjects.

6.4. Automated decision making (Art. 22 GDPR)

The GDPR guarantees the right not to be subject to automated decisions when there is no human intervention, or it has legal effects, or it affects the data subject in a similar and meaningful way.

Exceptions exist when the data processing:

- Are based on explicit consent and safeguards are established to protect the rights and freedoms of data subjects.
- Are necessary for the conclusion or performance of a contract, do not relate to special categories of data, and in addition, safeguards are in place to protect the rights and freedoms.
- Is based on EU or Spanish law and does not concern special categories of data.

› It is based on Spanish or EU law and is necessary to protect an essential public interest.

If these requirements are not fulfilled, human supervision of the algorithm in AI-based processing and automated decisions must be ensured, action procedures must be established, and incidents or challenges to automated decisions received from data subjects must be documented, in order to be able to detect situations where human intervention is necessary because the processing may not be working.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

If the distribution of the AI solution involves personal data of data subjects, it will be necessary to demonstrate that privacy measures have been implemented by default and by design (especially data minimisation).

Privacy Impact Assessments (PIAs) must also be adopted to identify privacy requirements and adopt the necessary measures.

Privacy by default and by design measures must follow the principles of minimisation and anonymisation, independence, transparency, accuracy and proactive accountability.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

› DPIAs must be carried out when levels of risk associated with the processing are high.

› DPIAs must be carried out before the actual processing of personal data takes place, i.e. before the processing starts. Therefore, validation has to be carried out prior to the design/selection and implementation of the AI solution before the design/selection and implementation of the AI solution for a given processing operation and thus, in this way, it is possible to identify which privacy requirements to incorporate and to be able to apply privacy requirements to be incorporated and effectively implement privacy measures by design and by default.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

› The data controller is the one in charge of the decision to select a **diligent technological solution** and cannot hide behind a lack of information or technical knowledge to evade his or her responsibility to audit and decide on the adequacy of the system.

› It is **not acceptable to shift responsibility** to the AI's system itself.

› From a data protection point of view, the processing users using AI could be classified as follows:

- Entities employing such AI on data subjects' data (employees, customers or others);
- Natural persons who purchase a product or a service that includes an AI component for the purpose of processing their own personal data.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

So far, the Spanish DPA has only ruled on international data transfers that take place within the framework of the Common European Space (the European Union states plus Iceland, Norway and Liechtenstein), but not with respect to data transfers outside the European Union.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

› AI tools may have a multiplier effect on ethical shortcomings. For this reason, the GDPR safeguards must be applied in order to minimise these risks.

› In order to determine the level of risk of a data processing tool (and including an AI tool), the following should be taken into account:

- **Risks of discrimination** (algorithmic discrimination): special attention needs to be paid to attributing responsibilities to AI components without supervision and without critical stance (so-called bias)
- **Risks arising from the processing in relation to the social context** and the side-effects that may arise from it.

Furthermore, the Spanish DPA is concerned about the development of AI-based systems whose data set or validation is flawed based on erroneous information that determines the existence of inherent biases in the system because the training data was already biased. Again, it stresses the need to include quality and accurate data from the training phase. Another concern is that related to the interpretation and use of the results generated by the users of the AI based system, in what it calls psychological bias.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

Not for now.

Sweden

Martin Gynnerstedt

Partner, Fylgia

+46 8 442 53 00
martin.gynnerstedt@fylgia.se

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

No such government authority has been decided yet.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

On February 10, 2021, in decision DI-2020-2719, the Swedish Data Protection Authority (IMY) issued administrative fines of 2,500,000 to the Swedish Police Authority for their use of Clearview AI, in breach of ch. 2 s. 12 and ch. 3 s. 2 and 7 of the Crime Data Act (Sw. Brottsdatalag (2018:1177)). The main arguments for this were that this processing was not strictly necessary for its purpose, without appropriate safeguards, and there had been no data protection impact assessment prior to the processing. The decision has been appealed.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

The Swedish government tasked the Swedish Authority for Privacy Protection, Integritetsskyddsmyndigheten, with raising the general level of knowledge about privacy and data protection issues among innovation actors. Part of this resulted in a case-based report on federated machine learning between two healthcare providers, which can be viewed here: h**ttps://www.imy.se/globalassets/dokument/rapporter/slutrapport-om-imys-pilotprojekt-med-regulatorisk-testverksamhet-om-dataskydd-230315.pdf**. For another part of this task, IMY has collaborated with AI Sweden, which is the national centre for applied AI funded by the Swedish government and other public and private entities, to provide support and guidance on data protection and AI. The result of this effort were two reports, which can be found here: **https://www.imy.se/globalassets/dokument/rapporter/slutredovisning-av-imys-innovationsuppdrag.pdf** and **https://www.imy.se/globalassets/dokument/rapporter/delredovisning-av-uppdrag-om-kunskapshojande-insatser-till-innovationssystemet-om-integritets--och-dataskyddsfragor.pdf**.

The Swedish government tasked the Swedish Public Employment Service, the Swedish Companies Registration Office, the Agency for Digital Governance, and the Swedish Tax Agency with promoting the use of AI by the public administration. This effort resulted in a report, that can be found here: **https://www.digg.se/download/18.5b30ce7218475cd9ed39384/1674479294670/Slutrapport%20Uppdrag%20att%20fr%C3%A4mja%20offentlig%20f%C3%B6rvaltnings%20f%C3%B6rm%C3%A5ga%20att%20anv%C3%A4nda%20AI%20I2021-01825.pdf**.

The Swedish Association of Local Authorities and Regions has published guidance and provides support on developing AI in local authorities and regions here: **https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/datadrivenutveckling/artificiellintelligensai/vagledningstodutvecklaaitjanster.68667.html**.

The Swedish Equality Ombudsman has published a report on transparency, training, and data as it relates to discrimination and AI here: **https://www.do.se/download/18.56175f8817b345aa7651be9/1646982570826/rapport-transparens-traning-och-data.pdf**.

The Swedish Medical Products Agency has published guidance on the use of AI in Swedish healthcare here: **https://www.lakemedelsverket.se/4a5f16/globalassets/dokument/medicinteknik/artificiell-intelligens-ai/vagledning-anvandning-av-artificiell-intelligens-i-svensk-sjukvard.pdf**.

These reports generally do not provide concrete guidelines on the application of AI, but rather conclude that further guidance on the topic is necessary.

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Not yet.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

The focus of Integritetsskyddsmyndigheten is on enabling innovation in relation to AI while promoting compliance with the GDPR and other legislation.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

Most of the authorities' guidance states that there is a need for more guidance on the practical application of AI but generally lacks such concrete information.

Integritetsskyddsmyndigheten's guidance so far has been general in nature, and IMY has concluded that continued guidance focused on AI is necessary. The intention of Integritetsskyddsmyndigheten moving forward is to give case-based guidance on privacy concerns that AI give rise to. The report on federated machine learning between two healthcare providers is an example of such guidance. As such, the guidance is specific and not generally applicable for other uses of AI as it relies on Swedish healthcare and secrecy legislation, in addition to the GDPR. Moreover, a range of issues, such as purpose limitation, data minimisation, and data accuracy, were not considered in the project.

However, Integritetsskyddsmyndigheten has commented on some of these matters in a Q&A on its website. IMY recommends mapping out which personal data are necessary in order to train the AI and removing the personal data that is not necessary. Personal data that is no longer required for the purpose of training the AI must be deleted after this purpose is completed unless they are required for another purpose. Pseudonymising personal data is also recommended where possible in order to increase privacy protection. This information can be found here: **https://www.imy.se/verksamhet/dataskydd/innovationsportalen/vanliga-fragor/utmaningar-med-uppgiftsminimering-och-utveckling-av-ai/**.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

No specific guidance.

6.3. Data subject rights

No specific guidance.

6.4. Automated decision making (Art. 22 GDPR)

No specific guidance.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

Integritetsskyddsmyndigheten recommends utilising pseudonymisation where possible. This information can be found here: **https://www.imy.se/verksamhet/dataskydd/innovationsportalen/vanliga-fragor/utmaningar-med-uppgiftsminimering-och-utveckling-av-ai/**.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

No specific guidance.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

No specific guidance.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

No specific guidance.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

Integritetsskyddsmyndigheten states that it is important to ensure that the AI is trained using relevant personal data in order to ensure that the AI model is statistically correct and non-discriminatory. This information can be found here: **https://www.imy.se/verksamhet/dataskydd/innovationsportalen/vanliga-fragor/utmaningar-med-uppgiftsminimering-och-utveckling-av-ai/**.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

Not yet.

Switzerland

Clara-Ann Gordon

Partner, Niederer Kraft Frey

+41 58 800 8426
clara-ann.gordon@nkf.ch

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

The Swiss DPA has not issued any general guidelines on AI.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

The Swiss DPA has not issued any general guidelines on AI.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

The Swiss DPA has not issued any general guidelines on AI.

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

The Swiss DPA has not issued any general guidelines on AI.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

The Swiss DPA has not issued any general guidelines on AI.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

The Swiss DPA has not issued any general guidelines on AI.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

The Swiss DPA has not issued any general guidelines on AI.

6.3. Data subject rights

The Swiss DPA has not issued any general guidelines on AI.

6.4. Automated decision making (Art. 22 GDPR)

The Swiss DPA has not issued any general guidelines on AI.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

The Swiss DPA has not issued any general guidelines on AI.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

The Swiss DPA has not issued any general guidelines on AI.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

The Swiss DPA has not issued any general guidelines on AI.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

The Swiss DPA has not issued any general guidelines on AI.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

The Swiss DPA has not issued any general guidelines on AI.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

The Swiss DPA has not issued any general guidelines on AI.

United Kingdom

Paul Barton
Partner, Fieldfisher

+44 330 460 7093
paul.barton@fieldfisher.com

Nuria Pastor
Director, Fieldfisher

+44 330 460 7066
nuria.pastor@fieldfisher.com

1. Which government authorities will or should be primarily responsible for the enforcement of the AI Act?

The AI Act will not apply in the UK. The UK's approach to AI does not currently envisage a general AI law but instead aims at the creation of sector specific rules for AI. UK users of AI will, therefore, need to consider the laws applicable to their specific sector. In the UK, a variety of existing laws, such as the UK GDPR, Data Protection Act 2018, Human Rights Act 1998 and Equality Act 2010 potentially apply to the use of AI. The UK Department of State for Science, Innovation and Technology (DSIT) released a white paper on AI (**https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper**) asking existing regulators to implement a set of five general AI principles (security, transparency, fairness, accountability and contestability).

Key regulators for AI in the UK will include the Information Commissioner's Office (ICO), the Financial Conduct Authority (FCA), the Competition and Markets Authority (CMA) and the Office of Communications (Ofcom). We may also see the Digital Regulation Cooperation Forum (DRCF), which brings together the ICO, CMA, Ofcom and FCA, take on a leading role in developing guidance on AI for the UK's digital sector.

2. Have there already been cases in which authorities have issued administrative fines, bans or similar regarding specific AI models and what were the main arguments?

Not that we are aware.

3. Have the relevant authorities already published specific guidelines, position papers or such on the key legal issues regarding the development and use of AI?

The UK Department of State for Science, Innovation and Technology (DSIT) released a white paper on AI (https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper) asking existing regulators to implement a set of five general AI principles (security, transparency, fairness, accountability and contestability). Whilst regulators are not required to have regard to these principles, the white paper hints at the introduction of a statutory duty following an initial monitoring period. The UK's data protection regulator, the Information Commissioner's Office (ICO), has already produced detailed guidance (**https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/**) on how the UK's data protection rules are to be interpreted in the context of AI. **https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/** It has also produced explainabilty guidance in conjunction with the Alan Turing Institute: **https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/** The Financial Conduct Authority (FCA), Competition and Markets Authority (CMA) and other UK regulators are also actively working on producing guidance for their sectors.

4. Are there specific national legislative initiatives regarding Data Protection and AI that could affect the development and use of AI-technology in the future?

Please see above regarding the UK's white paper on AI.

5. What is the current focus of national regulators when it comes to regulating AI, especially in terms of development and use?

Whilst the regulatory landscape is still evolving (please see above), the UK's data protection regulator, the Information Commissioner's Office (ICO) has produced guidance on how the UK's data protection rules are to be interpreted in the context of AI (see above). The guidance is broadly structured along data protection's foundational principles, namely lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and security and accountability. The regulators have not yet indicated particular areas of focus/interest. However, we suspect that transparency/explainability and fairness will be key areas of regulatory interest.

One area of apparent focus is use of AI tools in recruitment - the ICO has asked one client to participate in a voluntary audit in respect of its use of AI in the context of recruitment.

6. In detail, what is the authorities' position on the following aspects:

6.1. Principles relating to processing of personal data and lawfulness

in particular legal basis, purpose limitation, changes of purpose, data minimisation, data accuracy and of processing of special categories of personal data

The ICO's guidance on AI and data protection (see above) does not set out specific rules for AI but rather provides guidance on the application of the UK's existing data protection laws to AI. The ICO notes that in many cases, when determining the purpose(s) and lawful bases, it will make sense to separate the research and development phase of AI systems from the deployment phase. This is because these are distinct and separate purposes, with different circumstances and risks. Therefore, it may sometimes be more appropriate to choose different lawful bases for your AI development and deployment.

6.2. Transparency

in particular information of users, Art. 13 and 14 GDPR

The ICO's guidance on AI and data protection (see above) does not set out specific rules for AI but rather provides guidance on the application of the UK's existing data protection laws to AI. The ICO emphasises the need to be able explain the decision making of an AI system to achieve transparency. The ICO also suggests that not telling data subjects about the use of AI (especially given the technology's novel nature) is unlikely to be viewed as transparent behaviour under the UK GDPR. The ICO has produced specific guidance on explainability in conjunction with the Alan Turing Institute (see above).

6.3. Data subject rights

The ICO's guidance on AI and data protection (see above) does not set out specific rules for AI but rather provides guidance on the application of the UK's existing data protection laws to AI. It is noteworthy that the ICO does not make any exceptions for AI (despite recognising several challenges in the context of AI) - data subject rights will need to be facilitated as per existing GDPR guidance.

6.4. Automated decision making (Art. 22 GDPR)

The ICO's guidance on AI and data protection (see above) does not set out specific rules for AI but rather provides guidance on the application of the UK's existing data protection laws to AI. The ICO states that in general, mere human involvement in the AI lifecycle does not necessarily qualify as meaningful human review. In some cases for example, a human may provide input data into an AI system, that will then process it to make predictions or classifications. If those outputs have significant or legal effects, Article 22 will apply because the decision itself is solely automated. The human's involvement in the decision is not meaningful, as they are merely supplying the data that the system uses to make that decision. In most cases, for human review to be meaningful, human involvement should come after the automated decision has taken place and it must relate to the actual outcome.

6.5. Data Protection by Design and Data Protection by Default

especially technical and organisational measures, Art. 24 and 25 GDPR

The ICO's guidance on AI and data protection (see above) does not set out specific rules for AI but rather provides guidance on the application of the UK's existing data protection laws to AI. The ICO emphasises the importance of data protection by design and default but does not provide specific guidance in the context of AI.

6.6. Data protection impact assessment (DPIA), Art. 35 GDPR

The ICO's guidance on AI and data protection (see above) does not set out specific rules for AI but rather provides guidance on the application of the UK's existing data protection laws to AI. The ICO highlights that a DPIA may form an effective starting point for achieving broader AI compliance. The ICO provides an AI and data protection risk toolkit (**https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/**) that could support a DPIA.

6.7. Involved parties: Allocation of roles under data protection law when using AI

use of the AI tool e.g. by a private user or by other services/third parties

The ICO's guidance on AI and data protection (see above) does not set out specific rules for AI but rather provides guidance on the application of the UK's existing data protection laws to AI. No specific guidance is provided on the allocation of roles in the context of AI other than indicating that it is possible that an organisation may be a controller or joint controller in some phases or purposes, and a processor for others. Reference is made to existing guidance and there are some useful examples of the type of decisions that controllers and processors can take in an AI context.

6.8. Transfer of data outside the EU (Chapter V of the GDPR)

The ICO's guidance on AI and data protection (see above) does not set out specific rules for AI but rather provides guidance on the application of the UK's existing data protection laws to AI. No specific guidance is provided on restricted transfers and AI.

6.9. Further data protection-relevant aspects in relation to AI

This could be e.g.

- special safeguarding of children and minors

- risk of discrimination (so-called bias)

Not that we are aware of - these aspects are covered with the guidance in the context of how to apply the GDPR principles.

7. Are there additional regulations for special categories of AI-tools (e.g. generative AI)?

Not that we are aware of.

About Ecomlex

We are an association of leading lawyers with expertise in technology, IT and e-commerce, data protection and privacy. We focus on meeting the needs of businesses throughout Europe.

We act for a wide range of clients in the technology sector and in other sectors where technology is used and compliance with data protection law and regulation is necessary. Our clients include multinational government and intergovernmental bodies, multinational companies and growing businesses which are expanding outside their own territories.

Our clients benefit from our approach because:

- We have specialist knowledge of the relevant law and technology
- We provide a responsive and cost-effective service to our clients.
- Our approach is commercial and pragmatic
- We can provide one invoice for all our work across territories

If you would like to know more about Ecomlex, please visit **www.ecomlex.com/about-ecomlex**