Direktoratet for forvaltning
og økonomistyring

DFØ report 2024:9
August 2024

Governance structure for the EU's Artificial Intelligence Act

Foreword

In its letter of allocation for 2024, the Norwegian Agency for Public and Financial Management (DFØ) was tasked with investigating and providing recommendations for the establishment of a new national governance structure for the enforcement of the EU's Artificial Intelligence Act, in collaboration with the Norwegian Digitalisation Agency (Digdir). DFØ was given primary responsibility for this assignment. Digdir has assisted with the interpretation of the Act and dialogue with other European countries (cf. Chapters 2 and 3, and Appendix 2.)

This has been a demanding project, not least due to the considerable uncertainty about the area of impact and scope of the Act, and the short deadlines. We would especially like to thank the Norwegian Digitalisation Agency (Digdir), represented by Alexandra Kleinitz Schultz and Jens Andersen Osberg for excellent assistance. We would also like to thank all the participants who have made time for interviews and meetings and shared their opinions and views with us.

Head of Section Siri Bjørtuft Ellingsen has been the project coordinator. The work on the project has been carried out by Mats Fremmerlid, Vivi Lassen, Dag Solumsmoen, Eivor Bremer Nebben and Oddbjørg Bakli (project manager). Ingunn Botheim has assisted with quality control.

The Norwegian Agency for Public and Financial Management (DFØ) is responsible for the content, discussions and recommendations.

Oslo, Norway, August 2024

Hilde Nakken
Head of Division

Contents

Summary

The aim of the project has been to assess and recommend an appropriate organisational structure for the enforcement of the EU's Artificial Intelligence Act in Norway. The assessments and recommendations were to be independent, based on the Artificial Intelligence Act and governance policy considerations for the organisation of supervisory tasks.

The regulations are general and allow for different interpretations. The AI Act is closely linked to other EU regulations on product safety and is divided into risk classes. The requirements regarding independence correspond to the requirements in other product safety regulations. The EU's Artificial Intelligence Act has two key elements related to governance structure: follow-up during the product development stage (depending on the risk classification of the product) and post-market monitoring.

The AI Act calls for a governance apparatus consisting of at least one "market surveillance authority", at least one accreditation body ("notifying authority"), and the establishment of at least one regulatory sandbox. The main principle is that responsibility for enforcing the Act shall be distributed among authorities in the various sectors as an extension of the supervisory responsibilities they already have. The Act assumes a two-tier model. One of the designated market surveillance authorities shall act as the national single point of contact vis-à-vis the EU and have a coordination role vis-à-vis the other market surveillance authorities.

The interviews revealed that there are varying levels of knowledge and, in some cases, a high degree of immaturity with regard to AI and the AI Act both within and outside the government administration. Relatively few of the people interviewed have a clear idea about how the governance system should be organised. Most of the stakeholder groups will need a great deal of information, advice and guidance. The lack of expertise, and especially the lack of competencies related to ICT and AI, is perceived as a major challenge.

The report discusses four alternatives for organising the coordinating market surveillance role, including the role as the single point of contact: establishment of a new body, the Norwegian Data Protection Authority (Datatilsynet), the Norwegian Digitalisation Agency (Digdir), and the Norwegian Communications Authority (Nkom).

Our recommendations can be summarised as follows:

- Due to the considerable uncertainty about the scope and impact of the AI Act, the organisation should be re-evaluated once the Act has "taken root" and started to work.
- In addition to uncertainty about the scope, we believe that establishing a new body will be too expensive and time-consuming.
- The national market surveillance function and the role as the single point of contact should be assigned to the Norwegian Communications Authority (Nkom). Nkom will then have overarching responsibility for:

    - contact vis-à-vis the EU and participation in the various EU bodies and processes
    - coordination, guidance and assistance to the other market surveillance authorities
    - advice, guidance and information to AI suppliers, users and the general public

- The Norwegian Communications Authority, the Norwegian Digitalisation Agency and the Norwegian Data Protection Authority should all be tasked with collaborating on information, advice and guidance on artificial intelligence and the AI Act
- The national sandbox should be established and operated as a joint project between the Norwegian Data Protection Authority, the Norwegian Communications Authority and the Norwegian Digitalisation Agency. This will help ensure coordinated, uniform information, advice and guidance on the AI Act and contribute to mutual competence building.
- A "user board" should be created linked to the national sandbox where key players can receive advice, guidance and information and provide input on needs and challenges.
- Norsk akkreditering should be put in charge of accreditation assessments and monitoring of assigned accreditations, while relevant specialist authorities should be responsible for formal designation and notification to the EU.
- The handling of complaints and appeals should initially follow the existing arrangements for the various supervisory authorities that are assigned responsibilities pursuant to the AI Act.
- Costs must be expected linked to the role as the single point of contact, the establishment and operation of a regulatory sandbox, and the increased focus on information, advice and guidance in connection with implementation of the system.

1 Introduction

1.1 Background

In April 2021, the European Commission proposed a Regulation laying down harmonised rules on artificial intelligence – the Artificial Intelligence Act. In December 2023, the Council of the European Union, the European Commission and the European Parliament reached a political agreement. The Artificial Intelligence Act was finally approved on 21 May 2024 and entered into force on 1 August 2024. The Artificial Intelligence Act will affect the use of artificial intelligence within the EU and the EEA, with consequences for both public and private players.

The Artificial Intelligence Act aims to regulate markets for the development and use of artificial intelligence (AI). Information, guidance, market surveillance / supervision and sanctions are the key instruments to ensure compliance with the Act.

An inter-ministerial working group has discussed how the EU's Artificial Intelligence Act can be implemented in Norway. Among other things, the working group recommended investigating how best to structure the national governance system for enforcement of the AI Act. The starting point for the investigation was a two-level model in which one body is responsible for coordination, enforcement and implementation of the AI Act, while sectoral supervisory authorities are given responsibility and delimited supervisory authority within their own areas of responsibility (cf. Section 4.2.3 of the working group's report).

In its letter of allocation for 2024, the Norwegian Agency for Public and Financial Management (DFØ) was put in charge of investigating and making recommendations for the establishment of a new national governance structure for the enforcement of the EU's Artificial Intelligence Act. In its letter of allocation, the Norwegian Digitalisation Agency (Digdir) was charged with collaborating with DFØ on this assignment.

1.2 Objectives and mandate

The aim of the project was to assess an appropriate organisation for the enforcement of the EU's Artificial Intelligence Act in Norway. The assessments were to be independent and based on the Artificial Intelligence Act and governance policy considerations for the organisation of supervisory tasks.

On the basis of the assessments, the Norwegian Agency for Public and Financial Management (DFØ) was then to recommend a national management structure for enforcement of the AI Act. This includes the organisation of the supervisory function, distribution of the roles and responsibilities of the supervisory authority, establishment of an associated system for processing complaints and appeals, and designation of a national accreditation authority. In addition, the financial and administrative consequences of the recommended proposal for the new organisation were to be described.

1.3 Approaches and delimitations

In the project planning stage, the following questions were prepared:

Organisation of the supervisory function:

- How to define and delimit roles and responsibilities for the new supervisory function?
- How to organise the interaction with the EU?
- Which other market surveillance authorities should be assigned supervisory responsibilities pursuant to the AI Act?
- Which organisation will best meet the competence requirements defined in the AI Act?
- To what extent should the new supervisory function be organised centrally as a single unit?
- Should a new administrative body be established or should the supervisory function be assigned to an existing agency?
- Which agencies (bodies) would it be most relevant to assign the new supervisory function to?
- If the tasks are assigned to an existing agency, what changes will be required in the relevant agency?
- How to avoid (or possibly address) grey areas that overlap with other agencies' (bodies') area of responsibility?
- How should the relationship with the responsible ministry be organised to meet the need for autonomy in this area?
- What are the financial and administrative consequences of the proposed organisation?

Organisation of the accreditation function

- Where should the accreditation function be placed?
- Which agencies are potential candidates?
- How are the roles and responsibilities distributed between the supervisory body and the accreditation body? Can the same agency have both functions?
- What are the economic and administrative consequences of the proposal for the organisation of the accreditation function?

Organisation of the complaints and appeals system:

- Should the complaints and appeals body be organised as a separate agency (with its own secretariat) or should these tasks be assigned to other complaints and appeals handling bodies?
- What are the economic and administrative consequences of the proposal for the organisation of the complaints and appeals system?

Funding models:

- Which funding models are most appropriate for the supervisory function, the accreditation function and the complaints and appeals function, respectively?

The questions were defined more precisely and elaborated on as the project progressed and we became more familiar with the field. Our discussions have focused in particular on how to interpret the role as single point of contact and coordinating market surveillance authority. Our point of departure has been a two-tiered model, based on the proposal in the AI Act for a

governance structure outlined in Annex I of the Act. We have not taken a stance on how the responsibility for the high-risk areas and systems described in Annex III should be distributed.

As regards funding models, this has proved difficult to discuss on a general level.

1.4 Methods

The report is based on document analysis and qualitative interviews with representatives of different stakeholder groups. The discussions and assessments are based on analysis of the regulations and the underlying data, the Norwegian Agency for Public and Financial Management's previous reports (www.dfo.no) and the Agency's general knowledge of the organisation and functioning of the public administration.

See Appendix 1: *Data collection and method* for more detailed information on data collection and analysis.

1.5 Reading guide

Given the requirements and frameworks ensuing from the EU's Artificial Intelligence Act, the structure of the report reflects the six minimum requirements in the Instructions for official studies and reports as follows:

1. What is the problem and what do we want to achieve? – *Chapter 1*
2. What measures and/or organisational solutions are relevant? – *Chapters 2 and 3 and Appendix 2*
3. What matters of principle do the measures and/or organisational solutions raise? – *Chapters 4–6*
4. What are the positive and negative impacts of the proposed measures and/or organisational solutions, how permanent are they, and who will be affected? – *Chapters 4–6*
5. What measures and/or organisational solutions are recommended and why? – *Chapters 4–6*
6. What are the prerequisites for successful execution? – *Chapters 4–6*

Chapter 2 provides a brief introduction to the AI Act. There is a more comprehensive description and discussion in Appendix 2.

Glossary

The table below presents the key concepts from the EU's Artificial Intelligence Act. With some exceptions, especially in Appendix 2, the terms in the right-hand column are used.

Table 1: Concepts

The AI Act	This report	Explanation
Artificial Intelligence Act	Artificial Intelligence Act	
National competent authorities	National competent authorities	

The AI Act	This report	Explanation
European Artificial Intelligence Board	European Artificial Intelligence Board	
Market surveillance authorities	Market surveillance authorities	
Single point of contact (SPC)	Coordinating market surveillance authority	
Notifying Authority	Notifying Authority / Accreditation body[1]	The term "notifying authority" refers to bodies responsible for accreditation assessments and monitoring of assigned accreditations. Formal designation and notification / registration with the EU is not included in the role of "notifying authority", which we have chosen to call "accreditation body". As a result of the fact that the accreditation authority as a whole is split, the Act's "notifying authority" is not translated as "accreditation authority". See Section 5.3 for a more detailed discussion.
Notified body	Technical conformity assessment body	
	Regulatory sandbox	A controlled testing environment for businesses that want to experiment with new products, technologies and services under the supervision of the authorities (cf. Section 2.1 on sandboxes). According to the AI Act, relevant sandboxes must have a particular focus on fostering innovation.
Digital Services Act (DSA)	Digital Services Act (DSA)	An EU Regulation to protect consumers' fundamental rights on digital platforms.[2]

[1] It is uncertain what the correct translation into Norwegian of "notifying authority" is, but we have noted that the Danish version of the EU's Artificial Intelligence Act uses the term "bemyndigende myndigheter" ["authorising authorities"] and the Swedish translation uses "anmälende myndigheter" ["reporting authorities"].

[2] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

2 The EU's Artificial Intelligence Act and enforcement structure

2.1 The Artificial Intelligence Act

The Artificial Intelligence Act is a new regulatory framework for artificial intelligence that was adopted in spring 2024. The purpose of the AI Act is to improve the functioning of the EU's internal market and promote the development and uptake of human-centric and trustworthy artificial intelligence. The Act seeks to strike a balance between supporting innovation and possible benefits of AI against risks and possible harmful effects for fundamental rights (cf. for example, Article 1 and Recitals 1 to 8).

As part of the balancing of benefits and risks, the EU's Artificial Intelligence Act adopts a risk-based approach. Requirements are stipulated for systems based on the risk they are assumed to represent. The point of departure is that AI systems are allowed, unless the risk is of such a scope that it must be limited or cannot be accepted. Systems involving an unacceptable risk are prohibited, while high-risk systems must meet a range of specific requirements. It is assumed that the majority of AI systems will fall outside the scope of the EU's Artificial Intelligence Act because they will not be high-risk.[3]

Beyond the limitation of systems with an unacceptable risk and the requirements for high-risk AI systems, the AI Act sets transparency obligations in Chapter IV for certain AI systems, such as systems that produce "deep fakes". In addition, there are requirements for so-called "General-purpose AI models" in Chapter V of the Act.

As EU legislation and due to its risk-based approach, the EU's Artificial Intelligence Act does not give Member States the right to impose stricter restrictions on AI systems than those authorised by the Act (cf. Recital 1).

The EU's Artificial Intelligence Act does not primarily grant rights to individuals that the subjects of the obligations are to safeguard. This distinguishes the Artificial Intelligence Act from rights-based regulations such as the General Data Protection Regulation (GDPR). Although there are some minor elements of rights legislation in the Artificial Intelligence Act, the Act is fairly clearly a product safety regulation. The Act is similar to and should be seen in

[3] The impact assessment by the European Commission in April 2021 estimated that 5–15% of the AI systems in the EU would be categorised as high risk. Research from appliedAI in 2022 showed that 33% of the surveyed start-ups would classify their systems as high risk, while 15% were uncertain (see AI-Act-Impact-Survey_Report_Dec12.2022.pdf (frb.io)). A 2023 study found that 18% of over 100 AI solutions were categorised as high risk, and for around 40% it was unclear (see AI-Act-Risk-Classification-Study-appliedAI-March-2023.pdf (frb.io)). This may indicate that the proportion of high-risk systems may be larger than previously assumed.

the context of existing product safety regulations, in particular the EU Market Surveillance Regulation.[4]

The AI Act's position as a product safety regulation means that the Act sets requirements for AI systems that are to be placed on the EU market. Most of the requirements laid down in the Act are incumbent on the supplier of an AI system, but other players in the value chain must also meet certain requirements. The requirements must largely be met during the development of the system, before it is put into service, but some rules also apply to the use of the system. The requirements stipulated in the AI Act will be elaborated on in more detail in technical standards. The European Commission has tasked the standardisation organisations CEN and CENELEC with developing standards by 2025.

The Artificial Intelligence Act contains several measures to ensure that the Act is complied with in line with its purposes. The enforcement of the Act is described in more detail in the next section. Closely related to this is the establishment of regulatory sandboxes (cf. Article 57 of the AI Act). This is a special measure to foster innovation (cf. Recital 139). Emphasis is placed on alleviating the burden for very small businesses by prioritising their access to the sandboxes and in some cases reducing the expectations in relation to the most expensive requirements (cf. Article 63 and Recital 146).

2.2 Enforcement of the EU's Artificial Intelligence Act

The starting point in the original proposal from the European Commission was that there should be a central supervisory authority in each Member State, and the European Commission proposed a separate "national supervisory authority" role.[5] The European Parliament also had a "national supervisory authority" role in its proposal.[6] However, the Council's proposal did not call for a separate role of this nature and allowed for greater flexibility.[7] The finally adopted Artificial Intelligence Act aligns with the Council's proposal and does not stipulate a "national supervisory authority" role. The EU's Artificial Intelligence Act does not call for a central supervisory authority for Member States and does not use terms such as AI supervisory authority or algorithm supervisory authority.[8]

[4] Much of the Artificial Intelligence Act relates to elements that are central to existing product safety regulations, such as the Medical Devices Regulation – Regulation (EU) 2017/745. These elements include the use of technical standards, common specifications, conformity assessments, quality management systems, risk management systems, CE marking, market surveillance, notified bodies, and registration in European databases.

[5] See, for example, the Commission's proposal, Article 59 (2). EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

[6] TA (europa.eu)

[7] pdf (europa.eu) Article 59 (2).

[8] In recent years, there has been talk about the need to supervise AI and algorithms among politicians and in the public debate; see, for example, Case no. 3 [10:56:53] - stortinget.no and Hvordan kan vi holde algoritmene i ørene? Forskningsmiljøer står klare til å hjelpe [How can we keep the algorithms in check? Researchers are ready to help] (aftenposten.no). Also in connection with the EU's Artificial Intelligence Act, some have used the term AI supervision, see, for example, Danskenes KI-tilsyn legges til Digitaliseringsstyrelsen [Denmark has designated the Danish Agency for Digital Government as its

Thus, there will not be one single authority in the Member States that will be responsible for enforcing the EU's Artificial Intelligence Act. The point of departure for the EU's Artificial Intelligence Act is existing product safety regulations, entailing that several authorities will have roles under the Artificial Intelligence Act, and that enforcement is distributed across the different sectors. There are two key elements in the Artificial Intelligence Act related to the governance structure: 1) follow-up during the product development stage, and 2) post-market monitoring.

The first relates to the development of AI products to be made available on the EU's internal m**arket.** The requirements laid down in the Artificial Intelligence Act depend on the risks associated with the individual product and will be elaborated on in standards. For high-risk artificial intelligence products, a conformity assessment is required to ensure that the systems meet the requirements of the Act and the appurtenant standards. A conformity assessment documents that the requirements have been met and that the system can be CE marked before being placed on the market.

Normally, the developer conducts the conformity assessment itself. However, for certain systems, a third-party assessment by a conformity assessment body is required. These are most often commercial players competing to provide conformity assessment services. The conformity assessment bodies are approved as "notified bodies" by the accreditation body ("notifying authority"). The accreditation bodies are public authorities responsible for establishing and implementing necessary procedures for "the assessment, designation and notification of conformity assessment bodies and for their monitoring". Articles 70 and 28 (1) of the EU's Artificial Intelligence Act state that at least one accreditation body must be established or designated. See Appendix 2, Section 1.3.

The second element concerns the monitoring of AI products on the market.
Monitoring AI products on the market involves ensuring the proper use, correct classification and sound management of changes and new risks. The party that has developed the AI system has a number of different follow-up obligations, but in addition, there will be several "market surveillance authorities" responsible for monitoring the products on the market.

At the national level, at least one market surveillance authority must be designated (cf. Article 70 (1) of the AI Act). However, the Act paves the way for the existing supervisory authorities, especially for product safety regulations, to also act as market surveillance authorities for AI products within their areas. Examples of these kinds of authorities are the Norwegian Medical Products Agency (DMP), the Norwegian Labour Inspection Authority (Arbeidstilsynet), the Norwegian Directorate for Civil Protection (DSB) and the Norwegian Communications Authority (Nkom). Making existing actors responsible for monitoring products on the markets will ensure market surveillance authorities for AI products have the competence required to monitor specific sectors, such as medical equipment. The specific authorities involved and the range of tasks and roles of the market surveillance authorities are discussed in Appendix 2, Section 1.2.

AI supervisory authority] - Digi.no - News Studio. What meanings the different politicians and debaters ascribe to the term probably varies quite widely.

For high-risk systems as specified in Annex III of the AI Act, the Act does not designate specific market surveillance authorities. The Member States must themselves assess how these areas are to be handled in concrete terms (see the discussion in Appendix 2, Section 1.2.1).

Collectively, the market surveillance authorities and accreditation bodies (the "notifying authorities") are referred to as "national competent authorities". One of the market surveillance authorities must be designated as a "single point of contact": "Member States shall designate a market surveillance authority to act as the single point of contact for this Regulation" (cf. Article 70 (2)).

The Member States have the opportunity to deviate from the enforcement solution proposed in the Artificial Intelligence Act. They are free to choose how they want to organise the market surveillance authorities and accreditation body (cf. for example, Article 70 (1); cf. Article 74 (4), (7) and (8)). However, even if the AI Act's starting point for enforcement is departed from, several of the roles will already be determined and distributed. In other words, the following must be appointed at a national level:

- A coordinating market surveillance authority ("single point of contact")
- An accreditation body ("notifying authority")
- A complaints and appeals handling body[9]

In addition, it will be necessary to clarify which authorities are going to be responsible for market surveillance of the AI systems specified in Annex III of the AI Act.

2.3 Requirements pertaining to the designation of authorities to enforce the Artificial Intelligence Act

The designation of authorities pursuant to the EU's Artificial Intelligence Act must be in line with the requirements imposed by the Act, including the requirements regarding the organisation of the "national competent authorities" defined in Article 70. For notifying authorities, the requirements are elaborated on in Article 28. For the market surveillance authorities, the requirements are elaborated on in Article 74 and in particular in the Market Surveillance Regulation, to which these authorities are subject.

Requirements regarding independence

The requirements regarding independence for the national competent authorities are discussed in more detail in Appendix 2, Section 1.4. The conclusion is that the relevant authorities must be sufficiently independent that they can act completely freely and be objective in their assessments and tasks. This means that they must be shielded from any instructions and external influence. The specification "without bias" in Article 70 indicates

[9] The EU's Artificial Intelligence Act does not mention the right to appeal to a second level in connection with the handling of complaints and appeals. Nor does the EU Market Surveillance Regulation say anything about this. This is probably due to the wide variation in governance structures across the EU/EEA area; for example, France, Italy, Germany, Austria and Sweden have some form of specialised courts for administrative matters (cf. https://e-justice.europa.eu/19/EN/national_specialised_courts?SPAIN&member=1)

that it is not only formal roles and connections, but also more informal connections that may lead to the authority not being sufficiently impartial. Article 70 does not contain any additional terms such as "complete" or more detailed requirements regarding independence. This indicates that independence is more moderate than for regulations that do have these kinds of qualifiers, such as the General Data Protection Regulation (GDPR) and the EU Digital Services Act (DSA).

Article 70 of the Artificial Intelligence Act does not indicate from which connections independence must be ensured. Article 28 stipulates more specific requirements regarding the accreditation bodies' independence from the conformity assessment bodies. Similar requirements have not been defined for the market surveillance authorities. In Appendix 2, Section 1.4.2, dependence on suppliers in a market, political governance, and other special interests are highlighted as possible connections for market surveillance authorities that may be in breach of the requirement for independence in Article 70 (1). However, the degree of independence required and from whom will have to be determined in a specific assessment of the relevant authority.

The requirements regarding independence in existing product safety regulations can provide good guidance on what kind of independence is required in practice. Article 70 of the Artificial Intelligence Act corresponds largely to requirements in existing product safety regulations, such as Article 11 of the EU Market Surveillance Regulation. The Norwegian Medical Products Agency, the Norwegian Directorate of Health, the Norwegian Public Roads Administration, the Norwegian Labour Inspection Authority and the Norwegian Communications Authority are all examples of authorities that must be subject to the corresponding requirements regarding independence and impartiality ensuing from Article 11 of the EU Market Surveillance Regulation. Thus, the independence that these authorities have today is the same as that required under the Artificial Intelligence Act.

Requirements regarding competence

The Act sets requirements regarding the competencies and expertise that the market surveillance authorities must possess. They are required to have in-depth knowledge and expertise in several relevant fields, including AI technologies, data and data computing, personal data protection, cybersecurity and fundamental rights, as well as risks related to health and safety (cf. Article 70 (3)). In addition, they must have knowledge and understanding of relevant standards and legal requirements. These competencies must be assessed and, if necessary, updated on an annual basis.

See the more detailed discussion of competence in Section 4.2.1.

Requirements regarding a sandbox

Each Member State is required to ensure that at least one competent authority establishes a national sandbox within 24 months of adoption of the Regulation. The main purpose of this is to foster innovation and resolve issues that raise legal uncertainty, as stated in Recitals 138 and 139. This requirement means that at least one of the competent authorities must have the resources, infrastructure and expertise to provide testing, guidance and trials of innovative AI solutions.

The notifying authority and the market surveillance authority can be placed in the same body

It is possible to place the role of notifying authority (the accreditation body) in the same body as a market surveillance authority (cf. Appendix 2, Section 1.5.1).

The notified bodies that are directly designated in the EU's Artificial Intelligence Act and the notifying authorities cannot be placed in the same body

For notifying authorities, the requirements for independence are elaborated on in Article 28, with particular emphasis on the independence from third-party conformity assessment bodies ("notified bodies"). This means that roles such as market surveillance authority and accreditation body cannot be placed in the same organisation if the market surveillance authority is also to act as a third-party conformity assessment body. This is of significance to the market surveillance authorities as defined in Article 74 (8) (cf. Article 43 (1), third paragraph; cf. Appendix 2, Section 1.5.2).

3 Organisation of the governance structure for AI in other EU and EEA countries

To date, few Member States have made a final decision on where to place the market surveillance authorities for AI and in particular the role of single point of contact vis-à-vis the EU.[10] In this section, we will compare the bodies concerned with their equivalents in Norway (in parentheses). It should be noted that the assessment of which Norwegian bodies are the most similar is preliminary and has not been investigated in any great depth, meaning errors may have been made.

Denmark has officially designated the Agency for Digital Government "Digitaliseringsstyrelsen" (roughly equivalent to the Norwegian Digitalisation Agency – Digdir) as its coordinating supervisory authority.[11] In Spain, a new entity, AESIA, has been established to monitor and ensure the implementation of the Artificial Intelligence Act at the national level.[12] In Luxembourg, it has been decided that the National Commission for Data Protection will have a coordinating role and will probably also serve as the single point of contact (SPOC). In Italy, a new bill has been presented that among other things designates the Agency for Digital Italy (roughly equivalent to the Norwegian Digitalisation Agency) and the National Cybersecurity Agency (roughly equivalent to Norway's National Security Authority – NSM) as the national supervisory authorities for artificial intelligence in line with Article 70 of the Artificial Intelligence Act.

It is expected, but has not been finally decided, that in the Netherlands the Dutch Authority for Digital Infrastructure – RDI (roughly equivalent to the Norwegian Communications Authority – Nkom) will have a coordinating role and also serve as the single point of contact (SPOC), while the Dutch Data Protection Authority will be in charge of supervision of prohibited systems.

In Austria, a number of bodies have been established to support AI development, including an AI Advisory Board, an AI Service Centre, an AI Stakeholder Forum, and an AI Policy Forum. The AI Service Centre is currently located at the Austrian Regulatory Authority for Broadcasting and Telecommunications (roughly equivalent to the Norwegian Communications Authority – Nkom). They provide guidance and advice on the EU's Artificial

[10] As per June 2024

[11] Rollen som national tilsynsmyndighed med EU's AI-forordning skal varetages af Digitaliseringsstyrelsen [The role as national supervisory authority pursuant to the EU's AI Act to be held by the Danish Agency for Digital Government (digst.dk)

[12] BOE-A-2023-18911 Royal Decree 729/2023, of 22 August, approving the Statute of the Spanish Agency for the Supervision of Artificial Intelligence.

Intelligence Act and will help companies comply with the requirements in the Act at the time of entry into force. [13]

In Lithuania, the Innovation Agency (roughly equivalent to Innovation Norway) has been designated as the notifying authority and tasked with establishing a sandbox in line with the EU's Artificial Intelligence Act. They are currently making preparations for this with three employees dedicated to tasks related to the notifying authority role and two employees for the sandbox, with plans for expansion in 2025. It is expected that the Communications Regulatory Authority of the Republic of Lithuania (roughly equivalent to the Norwegian Communications Authority – Nkom) will be designated as the coordinating market surveillance authority, although a final political decision has yet to be made.

Several Member States, such as Sweden and Germany, have started or are about to start studies to determine where to place the coordination role. At the time of writing, we are not aware that any further decisions have been made. However, through the work on this report and dialogue with other Member States, we have made some general observations. It seems most countries are considering bodies within digitalisation, digital security or telecommunications and the Internet of Things (IoT) for the coordination role pursuant to the EU's Artificial Intelligence Act.

Discussions with Member States have revealed that there is widespread agreement that expertise in standardisation, experience with concrete guidance on AI, harmonisation and technological expertise are the key factors when determining where to place the coordinating role. Guidance and harmonisation are widely highlighted as weighty factors in the early phase of the implementation of the Artificial Intelligence Act.

[13] Artificial Intelligence (digitalaustria.gv.at)

4 Monitoring compliance with the Artificial Intelligence Act

The discussions in this chapter are based on our analysis of the EU's Artificial Intelligence Act and adjacent regulations (cf. Chapters 2 and 3 and Appendix 2), opinions voiced in the interviews, and the Norwegian Agency for Public and Financial Management (DFØ)'s knowledge about the organisation of the public administration in Norway. The starting point for the discussions is how the various governance structures and organisations work today with their current mandates and tasks. New roles and tasks will of course necessitate changes, without us being able to say at the present time what – or how extensive –these changes might be. Among other things, there may be a need to move or separate certain tasks in order to have relatively similar tasks all performed by a single body or avoid serious conflicts of roles related to the weighting of various interests and considerations.

4.1 Supervision as a public administrative function

The organisation of public administrative tasks in general
In any organisation of the government administration, there is a horizontal dimension and a vertical dimension.

The horizontal dimension reflects the division of tasks and responsibilities between different parallel agencies, where the organisation is characterised by degree of specialisation. A high degree of specialisation entails that specific objectives and types of tasks are largely organised into their own separate administrative bodies. A low degree of specialisation often results in large, merged administrative bodies covering a variety of objectives and types of tasks.

The vertical dimension reflects lines of governance and the distribution of responsibilities between hierarchical levels within the same administrative area. The organisation is primarily characterised by the degree of autonomy within its field and budgetary freedom of action in relation to the governing body. Full autonomy within its area of responsibility means that the Ministry is formally prohibited from instructing and/or overturning the agency's decisions on matters within its field. By contrast, an agency that is subject to ongoing instruction, be it formal or real, has very little autonomy in its field.

Supervision can be seen as one of the main functions of the central government
The core of the supervisory role is the specific monitoring of the compliance by the subject of the obligations with a norm already established by law, regulation or individual administrative decision, and reactions in the event of non-compliance.

In the broadest sense, the term "supervision" can be understood as a generic term for all activity or use of instruments implemented to follow up on the intentions of a regulatory framework (cf. White Paper – Report no. 17 to the Storting (2002–2003)). This often includes

information, advice and guidance, area monitoring and responsibility for contributing to the development of sectoral policy in the area.

With a view to ensuring the legitimacy of the supervisory bodies as specialised bodies and bodies governed by law, it has been argued that such bodies should be given increased formal independence, in particular by removing the ministries' authority to issue instructions (cf., among others, White Paper – Report no. 17 to the Storting (2002–2003)). The counterargument has been that the independence of the supervisory authorities must not be at the expense of the need for political governance. According to the public inquiry committee charged with preparing a new Public Administration Act, questions about independence should be assessed individually for each supervisory area and in light of the individual tasks that the supervisory body has, rather than for the body as a whole (Official Norwegian Report NOU 2019, p. 525).

In the Norwegian government administration, it has been common for an administrative body to both grant permits and supervise compliance with the conditions for the permits. The Public Administration Act Committee discussed whether this is an unfortunate mixing of roles: ought the supervisory tasks to be carried out in a separate independent administrative body? However, the Committee also identified various disadvantages of this kind of system and did not recommend that the roles be separated in this way. However, in order to achieve a clearer distinction between the different roles, several administrative bodies that have a certain scope of monitoring and supervision responsibilities have organised this work into a separate unit or department.

Several attempts have been made to categorise different types of supervisory functions, usually based on the considerations they have primarily been tasked with addressing (cf. for example, the White Paper on government supervision – Report no. 17 to the Storting (2002–03) and the report from the Norwegian Directorate of Public Management (Statskonsult) memo no. 2000:8). For our purposes, it may be sufficient to highlight the difference between so-called market surveillance or product safety supervision on the one hand and rights protection supervision on the other.

Market surveillance / product safety supervision is aimed at ensuring that markets function as intended and/or that products that are (to be) traded on a market comply with specific safety requirements, such as with respect to fire. Examples of supervisory bodies where these kinds of considerations are central are the Norwegian Competition Authority, the Norwegian Directorate for Civil Protection (DSB) (with respect to fire protection and electrical safety) and the Norwegian Communications Authority (Nkom).

Rights protection supervision is intended to ensure that users' and citizens' rights are safeguarded. Examples of supervisory bodies where these kinds of considerations are central include the Norwegian Data Protection Authority (privacy protection) and the Norwegian Consumer Authority (consumer protection).

4.2 The premises in the Artificial Intelligence Act

In this section, we discuss different types of premises in the EU's Artificial Intelligence Act, with regard to both competencies and tasks, and what requirements and challenges these may pose for the government administration in Norway.

4.2.1 Different types of AI competence are a challenge

The EU's Artificial Intelligence Act sets requirements regarding the competencies that the market surveillance authorities must have (cf. Section 2.3). There are requirements for expertise in AI technologies, data and data computing, personal data protection, cybersecurity, fundamental rights, health and safety risks, as well as supervision of products and knowledge of relevant standards and legal requirements. In addition, these competencies must be assessed annually and updated as necessary.

In its 2023 "Future of jobs report", the World Economic Forum (WEF) predicts that the growing use of AI and new technologies will lead to massive changes in workplaces and sought-after skill sets. It is estimated that the demand for expertise in AI and machine learning – which constitutes the fastest growing area of employment – will increase by 40 percent in the period 2023–2027. Along with an expected increase in demand for big data and information security analysts in the order of 30–35 percent and 31 percent respectively, the need for expertise in these areas will be significant.[14]

Several surveys and studies have shown that access to knowledge about artificial intelligence is a challenge for both the private and the public sector in Norway. The Confederation of Norwegian Enterprise (NHO)'s "skills barometer" for 2023 shows that one in three companies has challenges meeting their needs for expertise within ICT in general, while one in four companies report that they have challenges recruiting the necessary experts within AI in particular. Rambøll's *IT in practice 2023* also shows that an increasing number of organisations are reporting a shortage of people with digital competencies. The fact that these challenges will only get worse is also supported by Abelia's 2023 Adaptability Barometer. This shows that Norway is falling behind on both general and specialist expertise in ICT.

It is also challenging for the public sector to recruit experts in ICT. According to the Employment Barometer for 2023, ICT competence is the competence that most employers report as very challenging to recruit. The 2023 figures from Statistics Norway show that 9 out of 10 central government agencies that have tried to recruit ICT specialists experienced problems.[15] While things are going well in terms of connectivity, digitalisation of public services and technology among the public and in companies, there is a general lack of access to and education of specialist expertise in technology and ICT.[16] On the local government level too, there are major gaps. The smallest municipalities experience less access to

[14] https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf
[15] https://www.ssb.no/teknologi-og-innovasjon/informasjons-og-kommunikasjonsteknologi-ikt/statistikk/digitalisering-og-ikt-i-offentlig-sektor

technical expertise than the larger ones.[17] Given the developments in the area since 2019, there is every reason to believe that these problems will be even more dire in 2024.

In several reports, the Norwegian Agency for Public and Financial Management (DFØ) has written about the general lack of ICT competence and public agencies' desire for a higher degree of knowledge exchange. Public agencies are perceived to be competing with each other for the necessary expertise in the area of ICT. In their report *Mapping of status, challenges and needs in the Norwegian public sector* (2019), Broomfield and Reutter identified a general need for both competence raising and sharing of competencies among public enterprises. However, the survey also found that the largest companies were usually able to recruit good candidates in the field of AI, including experts in programming, legal and other AI-relevant specialist expertise. Recruitment challenges also have a geographical dimension in that it is consistently more difficult to recruit important expertise to jobs outside the major cities. This is especially true of legal competence.[18]

The overall picture reveals that central government agencies have a significant unmet need for expertise. The need is regarded as largest for the competencies that are particularly relevant in the field of AI, primarily technological, legal, technical and engineering expertise.[19] In Proposition no. 1 to the Storting (2023–2024) – the Fiscal Budget, the Government has therefore proposed to increase the funding for research on the consequences of AI, digital security, innovation and benefits by at least NOK 1 billion.[20] The Norwegian Universities and Colleges Admission Service ("Samordna opptak") also reports that the largest increase in the number of study places is being planned in information technology. The second largest increase is in technological subjects.

4.2.2 Possible tasks for the role as single point of contact and coordinating market surveillance authority

The EU's Artificial Intelligence Act builds on a number of premises for how the governance structure in the AI area should be organised in the individual Member State (cf. Section 2.1). A key topic is what the tasks of the coordinating market surveillance authority for the Artificial Intelligence Act will be (cf. Section 2.2). The coordinating market surveillance authority will or may be responsible for the following tasks:

- Being a single point of contact vis-à-vis the EU and participate in forums in connection with the EU's Artificial Intelligence Act. Coordinating and disseminating information to and from the EU will be a central task, including contributing to the EU's database on high-risk systems, for example
- Coordinating and facilitating a harmonised role towards the public through collaboration among the various competent supervisory authorities, between

[17] https://www.vestforsk.no/sites/default/files/2023-03/VFrapport7_2022_KI_i_offentlig_sektor.pdf,
[18] DFØ report 2022:5 *Færre og bedre – en evaluering av statsforvalterstrukturen [Fewer and better – an evaluation of the County Governor structure]*
[19] https://nifu.brage.unit.no/nifu-xmlui/bitstream/handle/11250/2646485/NIFUrapport2019-30.pdf?sequence=1&isAllowed=y
[20] Proposition no. 1 to the Storting (2023–2024)

specialist authorities and supervisory authorities, and between different categories of user, with special emphasis on the local government sector, and supervision
- Having a special responsibility for ensuring supervision of compliance with the Artificial Intelligence Act, or referring parties to the relevant market surveillance authority, in areas where the responsible authority cannot, does not wish to or does not have the skills required to perform supervision
- Providing information, advice and guidance to other market surveillance authorities on the supervision of AI
- Having a general information and advisory function on matters concerning AI and opportunities and barriers related to AI (cf. for example, the Norwegian Digitalisation Agency (Digdir)'s guide and the report by the Norwegian Association of Local and Regional Authorities – KS)[21]
- Ensuring the establishment and operation of a regulatory sandbox for the Artificial Intelligence Act that provides detailed guidance and testing of regulations in accordance with standards developed at EU level, or helping ensure that an existing sandbox meets the requirements pursuant to the Artificial Intelligence Act.

The coordinating authority does not necessarily have to operate the regulatory sandbox, but it will be natural for the single point of contact and the coordinating market surveillance authority to have a role here, in order to ensure equal and harmonised advice, guidance and information and a harmonised and common understanding of the Act (cf. Section 4.4.2).

In addition to the role as the single point of contact vis-à-vis the EU, a large part of the assumed tasks will be coordinating the market surveillance such that the sectoral supervisory authorities are in agreement in their understanding and use of the Artificial Intelligence Act, and that the Act is implemented in line with its purpose.[22] This will include:

- Allocating cases related to the AI Act that do not naturally belong under existing authorities for the product safety regulations and/or where there is doubt about sectoral affiliation, or possibly assuming responsibility for their supervision (a "catch-all" function)
- Assisting other market surveillance authorities in resolving particularly difficult technical and/or legal issues
- Advising and guiding other market surveillance authorities on the establishment and implementation of AI supervision, and possibly also assisting and "lending out" expertise in connection with the execution of supervision

[21] KS/Sopra Steria: Barrierer og muligheter i kommunal sektors arbeid med KI [Barriers and opportunities in the municipal sector's work on artificial intelligence]

[22] Samordningspunkt for markedstilsyn (SLO) i henhold til EUs markedstilsynsforordningen ligger hos Direktoratet for samfunnssikkerhet og beredskap (DSB) [The coordination point for market surveillance (single liaison office – SLO) pursuant to the EU Market Surveillance Regulation is the Norwegian Directorate for Civil Protection (DSB)]. The single liaison office shall contribute to the sharing of experience and knowledge related to general market surveillance across authorities – nationally and internationally. The single liaison office differs from the coordination of market surveillance pursuant to the EU's Artificial Intelligence Act, which is intended solely to coordinate the supervision of products that use artificial intelligence.

4.2.3 Many of today's supervisory bodies will have their responsibilities extended

At least 12 of today's supervisory bodies will have their responsibilities extended under the Artificial Intelligence Act

Given that existing sectoral supervisory bodies will also be responsible for supervision of AI in their respective sectors, at least 12 different sectoral supervisory authorities will be made responsible for supervision pursuant to the EU's Artificial Intelligence Act (cf. Appendix 2, Section 1.2.1). It follows from the Act that the following authorities shall act as market surveillance authorities in their respective areas:

- The Norwegian Ocean Industry Authority
- The Norwegian Directorate for Civil Protection
- The Norwegian Environment Agency
- The Norwegian Maritime Authority
- Norwegian Customs
- The Norwegian Building Authority
- The Norwegian Communications Authority
- The Norwegian Railway Authority
- The Norwegian Labour Inspection Authority
- The Norwegian Medical Products Agency

In addition, the Financial Supervisory Authority of Norway will be the market surveillance authority for high-risk AI systems that are made available on the market, put into service or used by financial institutions regulated by EU regulations for financial services. For high-risk systems listed in Annex III, the Act does not specify any market surveillance authorities except for certain biometric systems. This is discussed in more detail in Section 2.2 and Appendix 2, Section 1.2.1. For some areas in Annex III, the market surveillance authority will need to be one of the following:

- The coordinating market surveillance authority
- An existing market surveillance authority – for example the Norwegian Labour Inspection Authority for high-risk AI related to the labour market (cf. Annex III (4))
- Another authority – for example the Directorate of Education for high-risk AI related to education (cf. Annex III (3))

All of these will or may be market surveillance authorities in the field of AI and will have to build up, or possibly procure in some other way, relevant AI competencies and capacity.

The impression from the interviews is that some of the sectoral supervisory authorities that are either assigned special responsibilities in the Act or that must be assumed to have (now or in the future) many high-risk systems already have some expertise in AI or are in the process of acquiring it. Others have not come very far in their thinking about this or assume that AI and the Artificial Intelligence Act will have relatively little impact on their supervisory practices, at least in the short term.

Both supervisory bodies and the subjects of supervision will have a great need for support and guidance

A general impression from the interviews is that both supervisory bodies and the subjects of supervision have large needs for support and guidance – both to understand and interpret the regulations and to know what they need to do to comply with the regulations. All the market surveillance authorities must in principle be able to answer questions and provide advice and guidance on the regulations and monitor compliance with the standards.

From the perspective of the deployers, it is positive that the supplier side will have their responsibilities extended under the Act. At the same time, we got the impression that the deployer side must also be involved in processes to ensure that the advice, guidance and information they receive are targeted and adapted to their needs. This is especially true for local government authorities (the municipalities). For example, representatives of the municipal authorities have pointed out that market surveillance in the AI area should be as harmonised as possible and have as similar an approach and practice as possible.

In the interviews, some supervisory authorities that enforce so-called technology-neutral legislation pointed out that the EU's Artificial Intelligence Act is less relevant to them, at least in the short term, and that there is little point in them building up specialised expertise in AI. If the relevant market surveillance authorities do not have sufficient expertise or resources to be able to meet the need for support and guidance, or if they themselves have questions, they must have a place they can turn to for advice and guidance, and possibly to get assistance in conducting supervision. The question is whether this task can or should be assigned to the coordinating market surveillance authority or whether it should be organised in some other way.

One possibility is that any requests for advice, guidance or assistance related to these kinds of partially "uncovered" areas should be met by the coordinating market surveillance authority (cf. Section 4.2.2). It can then assess whether any of the market surveillance authorities with AI expertise can perform the necessary supervisory tasks because they have experience with similar issues and/or standards, or that the coordinating market surveillance authority itself carries out the supervision. In the long term, it may be appropriate to build up a pool of experts in the coordinating market surveillance authority that can assist other market surveillance authorities with AI supervisory tasks –with costs being covered by the latter..

Another possibility could be that the authority concerned buys supervisory services and expertise for assessment against the standards externally, and then uses the findings as a basis for a decision. In this case, the coordinating market surveillance authority ought to be able to assist with an overview of independent service providers, perhaps in particular on the technological side, or perhaps enter into framework agreements for this type of services. This kind of arrangement might also be useful for the other market surveillance authorities if they occasionally have challenges recruiting and retaining the necessary expertise.

Is there a need for an independent AI board?

In the interviews, a number of people raised the issue of whether some kind of specialist advisory board or body consisting of representatives from leading research environments, technology companies, the government administration, etc. could be established. In its report on generative AI, the Norwegian Board of Technology also recommends establishing a working group under the auspices of the Skate Forum (an advisory body for strategic cooperation on digitalisation of the Norwegian public sector) for the coordinated and continuous handling of issues related to AI in the public sector.[23] This board could then be charged with following the developments in the field of artificial intelligence. It could advise the government on how the public sector can deploy AI in a safe and cost-effective way, and how it can regulate it based on the risks and challenges that arise. One option could be to establish a new AI board and assign the secretariat function to, for example, the Norwegian Digitalisation Agency (Digdir). Another option might be to modify or expand the Digitalisation Council's mandate, and ensure that its members have particular expertise in the field of AI.

4.3 Discussion of possible candidates for the single point of contact and coordinating market surveillance authority

The general impression is that other countries are primarily considering assigning the role as single point of contact and coordinating market surveillance body to bodies that are largely equivalent in Norway to the Norwegian Data Protection Authority (Datatilsynet), the Norwegian Digitalisation Agency (Digdir) or the Norwegian Communications Authority (Nkom), or establishing a new body as Spain has done (cf. Chapter 3). This equivalence is based on our knowledge of the government administration. At the outset, we considered various other options, but soon found that the bodies we were considering would have a relatively peripheral connection to AI-related supervision and/or did not want a coordinating role in this area. Importance has also been attached to the fact that there were no other realistic alternatives in our interviews with different stakeholders.

Against this backdrop, we have chosen to discuss the following four organisational options for the role as the coordinating market surveillance authority, including the role as Norway's single point of contact:

1. Establishment of a new body
2. The Norwegian Data Protection Authority (Datatilsynet)
3. The Norwegian Digitalisation Agency (Digdir)
4. The Norwegian Communications Authority (Nkom)

It is important to emphasise that we have chosen to delimit our discussion to four more or less "separate" alternatives. In practice, there are of course many other variations and

[23] Generativ kunstig intelligens i Norge [Generative Artificial Intelligence in Norway] – The Norwegian Board of Technology (teknologiradet.no)

combinations of roles and tasks that could also have been discussed. However, we hope the discussion of these alternatives will be able to provide a relevant basis for decision-making for alternative solutions too.

In the discussions of the different alternatives, we have taken the following criteria into account:

- **Purpose-effectiveness:** To what extent does the alternative safeguard the purposes of the Act, i.e. market regulation / monitoring, supervision / surveillance, innovation and safety?
- **Independence from political governance:** How to ensure a good balance between independence and governability?
- **Role clarity:** To what extent might the role as single point of contact and coordinating authority conflict with the proposed organisation's other roles and tasks?
- **Expertise – current and access:** What competencies and expertise do the different proposed organisations currently have, and what will they need to be able to perform the tasks related to the role as single point of contact and coordinating authority?
- **Cost-effectiveness:** What costs will a new or expanded role entail for the individual agency?
- **Feasibility and flexibility:** What elements must be in place for the alternative to be implemented, and how flexible is it with regard to changes over time?

Finally, we provide an overall assessment of the strengths, weaknesses and suitability of the individual proposed organisations for the role as single point of contact and coordinating authority for the AI Act.

4.3.1 New body as single point of contact and coordinating market surveillance authority

Establishing a new body would enable tailoring

Establishing a new national coordinating market surveillance body would be very expedient in terms of purpose-effectiveness in the sense that the body could be tailored to meet the objectives and purposes of the Act. In the governance of the body, harmonisation, coordination and supervision in "uncovered" areas would be the main tasks, as opposed to an additional secondary task alongside a number of others.

The body's degree of independence could be adapted to the requirements in the Act – and established practice

In terms of independence from political governance, it would also be possible to tailor the degree of independence. As described in Section 2.2.2, the best solution seems to be a moderate degree of independence. This is not only because it seems appropriate that the independence of the new body would not differ significantly from the independence of the other defined sectoral supervisory authorities in the field of AI, but also in order for overarching authorities to have the opportunity to exercise governance, in connection with developments in the field of AI. Continued development of technologies and areas of application for AI may create a need for continuous updating of expertise and adaptation of the regulations and other roles of the new body. This will require dialogue with the Ministry,

and in this case it will not be helpful to have removed the Ministry's right to issue instructions.

A new body would be able to have a clear and unambiguous role

Unless the new body is given any other tasks that may to varying degrees constitute a conflict of interests, a new body would have a relatively clear and unambiguous rolewith respect to market surveillance in the field of AI. In general, however, there may be some inherent contradictions between the supervisory and harmonisation roles.

For the supervisory role, it is about the necessity of balancing the information and advisory role against the supervisory and compliance assessment role. In order to avoid having to supervise their own advice and recommendations, the supervisory body must primarily provide guidance on the regulations, as opposed to giving advice on what the individual enterprise should do to comply with the rules. This will always be a balancing act that requires high awareness of the different roles.

For the harmonisation role, it is about ensuring equal treatment in different fields of affairs and between the coordination role and any supervisory tasks. Own cases cannot be prioritised at the expense of the whole. There is a fundamental bias in the current governance system – where "own" sector tasks are often given priority over coordination tasks. Established interests and incorporated practices can also lead to skewed priorities when different disciplines are to be harmonised. A new body will be more easily able to handle challenges related to harmonisation, collaboration across traditional boundaries and role conflicts than existing bodies that have to prioritise between existing and new tasks – and between supervisory tasks and coordination tasks.

Extremely challenging to recruit the necessary expertise in the short term, given the great uncertainty about needs and scope

There is still great uncertainty about the scope and weighting of different types of expertise that a new body would need. What is important in the short term? What will be important in the longer term? It will entail great risk and be very demanding to establish a new agency under such uncertain circumstances.

In addition, there is uncertainty about market surveillance in areas that have not been predefined in the Act. If all this is to be gathered into a single, new market surveillance authority, it will require a very broad range of expertise in a single organisation, the purchase of services in the market, or close collaboration with relevant specialists.

One variant of the option of establishing a completely new body could be to transfer some expertise from existing supervisory bodies, for example expertise in information, advice and guidance tasks from the Norwegian Digitalisation Agency (Digdir), and perhaps also the Authority for Universal Design of ICT, and in addition gradually build up and recruit the necessary expertise as the AI Act evolves. As discussed above, the purchase or contracting of supervisory services and expertise for assessment against the standards may also be a relevant solution in the event of a lack of competencies.

It takes time and is costly to establish and build up a completely new agency
There is currently great uncertainty regarding the implementation of the Artificial Intelligence Act – with regard to competence requirements, capacity needs, harmonisation needs, organisation, etc. However, it is safe to assume that a coordinating market surveillance authority will be fairly modest in size to begin with. It will not be very cost-effective to build up a separate administration for this. An alternative could be to establish a new unit linked to an existing supervisory body with a functioning administration that can provide premises and administrative services for the new unit.

This kind of solution does not mean that the new unit would be organised as an integral part of the supervisory body in question. To avoid any possible conflicts between roles, it may be pertinent to have relatively loose ties to the supervisory body, where the new unit can draw on the host organisation's experts and competencies to a certain extent, or possibly that tasks and expertise are transferred from this and other relevant agencies. Later on, once experience has been gained with the chosen solution, it can then be considered whether the new unit should be spun off as a separate body.

High level of uncertainty about the scope of tasks and competence needs makes this option demanding to implement, but it would be flexible in connection with new tasks
As discussed, it would be demanding to establish a new body as long as there is such great uncertainty about how it would be organised, the scope of its tasks, the kinds of competence it would need, and where it is to be located. At the same time, a new regulatory body, tailored especially for the tasks of single point of contact, coordination and supervision / market surveillance, would probably be flexible in terms of its ability to take on tasks related to new legislation adopted or proposed by the EU in the digital area.

A decision to create a new body would trigger a new decision-making process on where the new body should be located. We know from experience that these kinds of processes are very demanding, in part because it is difficult to achieve consensus on the choice of site.

In summary: A new body would be a purpose-effective solution, but there is considerable uncertainty associated with the competencies that would be required, how long it would take to set up, and the costs
A new body would allow for tailoring, but it would be demanding to establish as long as there is such great uncertainty about how it would be organised, the scope of its tasks, the kinds of competence it would need, and where it should be located.

4.3.2 The Norwegian Data Protection Authority as the single point of contact and coordinating market surveillance authority

The Norwegian Data Protection Authority (Datatilsynet) is an ordinary, gross-budgeted administrative body under the Ministry of Digitalisation and Public Governance (DFD). It covers both the public and private sectors, and supervises the processing of personal data pursuant to, among other things, the Norwegian Personal Data Act, the Norwegian Police Register Act, the Norwegian Health Registry Act, the Norwegian Health Research Act, the Norwegian Health Insurance Act and the Norwegian Schengen Information System (SIS) Act and associated regulations. Regulations on camera surveillance and employers' access to

electronically stored material are also supervised by the Norwegian Data Protection Authority. Administrative decisions made by the Norwegian Data Protection Authority pursuant to these Acts of law can be appealed to the Norwegian Data Protection Board.

The Norwegian Data Protection Authority's main tasks are:

- Processing tip-offs and complaints and appeals
- Supervisory and conformity assessment activities
- Information, advice and guidance activities
- Active participation in the public debate on data protection issues, including through consultative statements on legislative proposals and public inquiries

The Norwegian Data Protection Authority may experience a conflict between the objectives related to the data protection legislation and the objectives of the EU's Artificial Intelligence Act

Although the Norwegian Data Protection Authority is a supervisory and conformity assessment body, it is primarily a rights protection authority and has limited experience with market surveillance / product safety supervision. As we will return to in our discussion of role clarity, the Norwegian Data Protection Authority will have to deal with balancing two slightly different objectives if they are responsible for both the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act.

The Norwegian Data Protection Authority has statutory independence in data protection cases, but will not need to have it in an AI context

The Norwegian Data Protection Authority has statutory independence and cannot be instructed about the processing of individual cases or about its activities pursuant to Section 20 of the Norwegian Personal Data Act and Article 52 of the General Data Protection Regulation (GDPR). If the Norwegian Data Protection Authority were to be given responsibility as Norway's market surveillance authority, less autonomy will probably be desirable than under the data protection legislation. Although the Ministry neither shall nor wishes to overrule the supervisory body in individual cases, it may need to change the system for the exercise of supervision, prioritise special supervisory areas or sectors, etc. If the Norwegian Data Protection Authority is designated as coordinating market surveillance body, it must be stated in legislation and regulations which autonomy the Norwegian Data Protection Authority is to have pursuant to the EU's Artificial Intelligence Act.

Administrative decisions made by the Norwegian Data Protection Authority related to the processing of personal data can be appealed to the Norwegian Data Protection Board. The King and the ministries cannot overturn the administrative decisions of the Norwegian Data Protection Authority (Section 20 of the Norwegian Personal Data Act). Based on the discussion of requirements regarding independence (cf. Section 2.2 and Appendix 2, Section 1.4), this goes beyond the requirements stipulated in the AI Act. As discussed above, this could be resolved by special rules governing complaints and appeals system stipulated in Acts of law and regulations.

There is scepticism towards the Norwegian Data Protection Authority as the coordinating market surveillance authority

The Norwegian Data Protection Authority is not a supplier of products and services that compete in a market or that will be subject to market surveillance / supervision in the field of AI.

Important objectives of the Artificial Intelligence Act include promoting innovation, competition on equal terms, etc. (cf. Section 2.1). Considerations such as privacy, data protection and data security will need to be balanced against more considerations and considerations that are more equally weighted than is the case with only assessing against the requirements of the General Data Protection Regulation (GDPR). However, the Norwegian Personal Data Act also defines cases where exemptions from personal data legislation can be made. The Data Protection Authority must therefore already sometimes weigh up different considerations against each other.

In our interviews, especially with representatives from industry and the supplier side, but also from the health side and other parts of the public sector, questions have been raised about whether the Norwegian Data Protection Authority's clear and visible role as a rights protection authority in the area of privacy is consistent with a role as a product supervisory authority in the field of AI. Some interviewees have expressed that the Authority's mandate (cf. the Ministry of Digitalisation and Public Governance (DFD)'s main instruction for the Norwegian Data Protection Authority[24]), which states that the Authority has a role as an ombud and must participate in the public debate on privacy and data protection, might cause privacy and data protection to be afforded greater attention than other considerations (such as innovation, public health, discrimination, etc.).

The Norwegian Data Protection Authority itself is reluctant to use the term "ombud", because they find that it sends incorrect signals about the role the Norwegian Data Protection Authority plays. However, as long as the term "ombud" continues to be applied to the Norwegian Data Protection Authority, this supports the doubts – justified or not – about how impartial the Authority's assessments would be. These kinds of doubts may serve to undermine trust and the Authority's legitimacy among the subjects of supervision.

In this context, it is relevant that the Artificial Intelligence Act mentions national data protection authorities as possible market surveillance authorities for systems for biometrics to be used for law enforcement purposes, border management, justice and democracy, and the systems as mentioned in Annex III, points 6, 7 and 8, of the AI Act. The Artificial Intelligence Act therefore clearly does not consider the relationship between data protection and innovation to be problematic in these areas. It is also relevant that some EU countries are considering assigning the national market surveillance function to their national data protection authorities (cf. Chapter 3).

Some interviewees also referred to the fact that the Norwegian Data Protection Authority's combined advisory and supervisory role might be challenging. In order to avoid supervising

[24] Main instructions for the Norwegian Data Protection Authority

its own recommendations, the Norwegian Data Protection Authority primarily provides general and overall guidance on what the regulations say. It is important to emphasise that this issue will apply to all supervisory authorities and supervisory activities. It therefore cannot be an argument against assigning the national market surveillance function to the Norwegian Data Protection Authority.

The Norwegian Data Protection Authority has a lot of legal expertise and supervisory experience, especially on data protection, privacy and data processing, but more limited expertise on AI and experience with product supervision

Since 2018, the Norwegian Data Protection Authority has been responsible for monitoring compliance with the General Data Protection Regulation (GDPR). This has given them a lot of insight into and expertise on EU legislation and EU processes, both of which are necessary and useful for the role as Norway's single point of contact and harmonisation body. It also has a lot of experience with combining advisory and information work on the one hand with supervision on the other. The Norwegian Data Protection Authority also has experts in ICT and AI, including in connection with the Authority's sandbox, but the team is fairly small. Product safety supervision will also require expertise in standardisation, which the Authority currently has limited experience in.

As discussed above, the national data protection authorities are one of the options suggested in the EU's Artificial Intelligence Act for market surveillance related to law enforcement, border management, justice and democracy (cf. Appendix 2, Section 1.2.1). In this case, product safety competence will need to be built up in order to be able to perform these tasks. The Norwegian Data Protection Authority has experience in supervising different sectors and administrative areas, but they do not have specific expertise in disciplines other than their own areas (privacy and data protection, data security, etc.). In some cases, this will entail a need to collaborate with relevant specialist authorities. However, experience from the General Data Protection Regulation (GDPR) and sandbox practices will be useful here.

Since 2021, the Norwegian Data Protection Authority has built up extensive expertise on the use of sandboxes and on sandbox methodology. The Norwegian Data Protection Authority's regulatory sandbox for AI was established as a measure under the Solberg Government's *National Strategy for Artificial Intelligence*, which was published in 2020. The original assignment and the goal of the Data Protection Authority's sandbox was to stimulate innovation that would promote ethical and responsible development of artificial intelligence (AI) based on respect for privacy and data protection. From 2023, the mandate was extended to include other privacy-friendly innovation and digitalisation. The sandbox assists individual players in their innovation and digitalisation projects through dialogue-based guidance. In order to scale up the positive impact of the sandbox, the specific assessments from the projects are communicated in as generic a form as possible so that other players can get inspiration and learn.

An evaluation of the sandbox from 2023 carried out by Agenda Kaupang shows that the sandbox has yielded good results, but also that this has been an ongoing development

process over time.[25] The evaluation points out that the sandbox is primarily aimed at legal aspects of the use of artificial intelligence and that the Norwegian Data Protection Authority has limited technological expertise. Among other things, this has meant that the Norwegian Data Protection Authority could not provide assistance on the more technical aspects of artificial intelligence in the projects. In light of this, the evaluation recommended that the Norwegian Data Protection Authority should strengthen its technical competence in order to be able to provide a more comprehensive perspective on the use of digital technology.

Although the sandbox for artificial intelligence will have a different and broader perspective, our assessment is that the Norwegian Data Protection Authority will nevertheless have a lot of things in place with regard to the methodology and expertise to implement sandbox processes.

It follows from the Norwegian Data Protection Authority's mandate that they primarily have a user perspective. If it is to act as a national market surveillance authority, that part of the Norwegian Data Protection Authority that works with AI, and possibly also the management of the Norwegian Data Protection Authority, must adopt more of a manufacturer and supplier perspective. As stated in Chapter 2, the subjects of supervision will be located along the entire value chain, but with particular emphasis on the manufacturer and supplier side. This will probably result in a need for a different mix of competencies than the Authority currently has.

For a relatively small organisation with limited resources, AI tasks will require additional resources

Like most of the other interviewees, the Norwegian Data Protection Authority expressed that it is demanding to estimate how many resources a new role and extended supervisory responsibility would entail. It is difficult to estimate both how much supervision the market surveillance function will entail and the scope of the work on the practical supervision.

The Norwegian Data Protection Authority is currently a relatively small organisation measured by number of full-time equivalents – about 60 full-time equivalents according to the annual report for 2023 – compared with the other two agencies we have considered in detail. This probably means there will be less room to manoeuvre and flexibility in dedicating resources and expertise to new AI tasks, at least in the short term. The annual report for 2023 states that the Authority is currently chronically under-resourced, and that the Norwegian Data Protection Authority needs significant strengthening in order to be able to fulfil its existing tasks and challenges.[26] The relatively long processing times compared with countries like Sweden and Denmark bear witness to this. Any new tasks related to an expanded supervisory role will therefore require additional resources, regardless of whether the single point of contact and harmonisation functions are assigned to the Norwegian Data Protection Authority or not. Since there is already a shortage of resources, with the

[25] Rapport Datatilsynet: Evaluering av sandkassa [Report The Norwegian Data Protection Authority: Evaluation of the sandbox]
[26] The Norwegian Data Protection Authority's Annual Report for 2023

Authority's current portfolio of tasks, it will probably also be challenging to transfer resources and expertise from existing task areas in the short term.

The sandbox is funded through an inter-ministerial collaboration. In 2023, the Ministry of Local Government and Regional Development (KDD) contributed NOK 3 million, while the Ministry of Trade, Industry and Fisheries (NFD), the Ministry of Labour and Social Inclusion (AID), the Ministry of Education and Research (KD) and the Ministry of Health and Care Services (HOD) each contributed NOK 1 million. The resources are spent on payroll expenses, execution of projects, preparation of advisory materials and communication activities.

In summary: Despite its extensive and good expertise, the Norwegian Data Protection Authority's privacy and data protection role will challenge the legitimacy of the Authority as a neutral market surveillance authority

Although not directly aligned with the EU's Artificial Intelligence Act and product supervision, the Norwegian Data Protection Authority has a lot of expertise and experience in tasks related to information, advice, guidance and (rights) supervision. However, it has limited resources to spare for new tasks and will require new, fresh resources to be able to perform any coordinating market surveillance function in accordance with the AI Act. It may also be necessary to use resources to "prove" to the industry and the supplier side that they are able to handle surveillance of the AI market without bias.

4.3.3 The Norwegian Digitalisation Agency (Digdir) as the single point of contact and coordinating market surveillance authority

The Norwegian Digitalisation Agency (Digdir) is an ordinary, gross-budgeted administrative body under the Ministry of Digitalisation and Public Governance (DFD). It performs a number of different tasks (cf. the instruction from the Ministry of Digitalisation and Public Governance).[27] Its main tasks include:

- Contributing to the development and implementation of the government's ICT policy
- Defining the premises for digitalisation and comprehensive information management
- Facilitating the development of digital services for the general public, local authorities and business sector
- Operating and managing national components and common solutions.
- Monitoring compliance with the universal design of ICT (through the Authority for Universal Design of ICT)

The Authority for Universal Design of ICT is a product inspection that checks that the requirements in the Regulation on universal design of information and communication technology (ICT) solutions of 21 June 2013 are complied with in the public and private

[27] Main instructions for the Norwegian Digitalisation Agency (Digdir)

sectors. The Authority is organised as an independent unit under the director of the Norwegian Digitalisation Agency (Digdir).

With the exception of the Authority for Universal Design of ICT – and the national services – the Norwegian Digitalisation Agency (Digdir) primarily relates to the public sector.

As of today, it is only in its role as the Authority for Universal Design of ICT that the Norwegian Digitalisation Agency makes administrative decisions that can be appealed. The Ministry of Digitalisation and Public Governance (DFD), as the governing ministry, is then the appeals body.

The Norwegian Digitalisation Agency's role as a driver of digitalisation, innovation and efficiency is compatible with the main purpose of the EU's Artificial Intelligence Act
According to the Ministry's instructions for the Norwegian Digitalisation Agency (Digdir), the Agency shall contribute to digitalisation, improved efficiency and modernisation, including innovation by and within the government administration. This must be regarded as coinciding closely with the main purpose of the EU's Artificial Intelligence Act. The Norwegian Digitalisation Agency has an advisory and guidance role with respect to artificial intelligence and EU regulations (cf. for example, Guide on responsible use and development of artificial intelligence and EU regulations on the sharing and use of data.

The Norwegian Digitalisation Agency is subject to political governance
As an ordinary administrative body, the Norwegian Digitalisation Agency is subject to the Minister's right to issue instructions and is therefore not independent of political governance. With regard to the Authority for Universal Design of ICT, it is enshrined in the Norwegian Digitalisation Agency's instructions that this role must be exercised independently of the Agency's other tasks, but this independence is not enshrined in law or in the Universal Design Regulation. Since the governing ministry is the appeals body for any administrative decisions made by the Authority for Universal Design of ICT, the Authority for Universal Design of ICT is therefore also currently fully subject to political governance.

The Norwegian Digitalisation Agency's role as a provider of national components may conflict with the role of a strong and legitimate supervisory body
The Norwegian Digitalisation Agency (Digdir) develops and operates a number of central national components and services where AI is likely to become important in the future in order to ensure good and cost-effective services. Digdir has a supplier role in this area, and the work on the national services constitutes a significant part of Digdir's operations, but at the same time they do not compete in a market. Nevertheless, the combination of being a provider and having the role of coordinating market surveillance may represent a conflict of interests, especially because with time AI solutions and systems will be developed and become an integral part of the national solutions Digdir operates (cf. the discussion of independence in Section 2.3 and Appendix 2, Section 1.4).

Authorities that monitor compliance with a regulatory framework will often themselves have to comply with these regulations in their own operations. For example, the National Archives of Norway must comply with the Archives Act in their tasks; the Norwegian Labour

Inspection Authority must comply with the working environment legislation, etc. There is also reason to believe that all public agencies, including market surveillance authorities, will deploy AI solutions to a greater extent in the future and thus have to fulfil the obligations of the EU's Artificial Intelligence Act for the deployment of AI systems. However, the primary subject of the obligations ensuing from the Artificial Intelligence Act is parties that develop AI solutions. Digdir (due to its role as a provider) is therefore more likely to be subject to supervision pursuant to the AI Act than other authorities.

One argument in support of a combined supervisory and provider role is that this can ensure better underlying knowledge and better access to competence in the role of market surveillance authority. In extension of this, it should also be noted that Denmark has decided to assign the coordinating market surveillance function to its Agency for Digital Government, which admittedly has greater supervisory responsibilities from before than Norway's Digdir, but which is also the provider of various national solutions and app services. However, the benefits of combining these roles must be weighed up against the disadvantages associated with the potential for mixing of roles and the possible lack of confidence from other subjects of supervision.

Responsibility for the supervision of Digdir's products and services might therefore need to be assigned to one of the other market surveillance authorities, such as the Norwegian Communications Authority (Nkom) for example. However, this could undermine Digdir's authority in the coordinating role if / when it were to become a subject of supervision due to tip-offs from the business sector, local government or other players who have contacted the relevant market surveillance authority because they are dissatisfied with the services that Digdir provides. It might also be challenging for the collaboration between the relevant market surveillance authority and Digdir as the coordinating authority.

The Norwegian authorities have previously given priority to ensuring complete independence for supervisory roles, and in some cases this has led to the separation of the supervisory activities of an agency out into a dedicated body. Examples include the establishment of the Petroleum Safety Authority Norway (now the Norwegian Ocean Industry Authority) and the Civil Aviation Authority as separate bodies. In both of these cases, the risk of a mixing of roles was a main reason for the separation. A more drastic alternative could be to separate the unit responsible for national services out as an independent body. This was assessed as recently as 2018–2019, but at that time it was decided to leave things as they are, because the national services were also regarded as a powerful harmonisation tool.

The Norwegian Digitalisation Agency's role as a driving force for digitalisation and innovation may be perceived to be incompatible with a neutral market surveillance role
A role as a driver of a particular development entails working at system level to bring about changes related to services, quality, cost-effectiveness, etc. While this is positive, a role as a driver might also pose challenges regarding neutrality in different areas (cf. the discussion of independence in Section 2.3 and Appendix 2, Section 1.4). This may lead to disagreement with other players about assessments and priorities. In the Norwegian Agency for Public and Financial Management (DFØ)'s opinion, it can be queried whether the Norwegian

Digitalisation Agency (Digdir)'s role as an active driver and definer of premises for digitalisation, innovation, and now AI, can be deemed to be compatible with the role as a neutral market surveillance authority, where the consideration of innovation is to be weighed up against other considerations. Such potential conflicts of interest must be assessed against the consideration of the supervisory body's legitimacy. It is not enough to maintain that the supervisory authority is impartial and neutral if others perceive it differently. Here it is also worth noting that some of the interviewees pointed out that Digdir already has many different roles and that it does not seem appropriate to assign it additional roles.

The Norwegian Digitalisation Agency has a lot of expertise in information, advice and guidance, but little practical supervision expertise – with some exceptions

As the government's foremost tool for digitalisation of the public sector, Digdir has extensive across-the-board expertise in the field of digitalisation. Information, advice and guidance related to digitalisation in general and AI in particular have been and continue to be an important task for the Agency.

Given Digdir's various tasks linked to digitalisation and comprehensive information management, it goes without saying that they have a great deal of technological expertise, and probably also more specialised AI expertise – both technological and legal – than many other central government agencies. In recent years, the Agency has built up expertise in innovation, information security and developments related to AI. In June 2023, on commission from the Ministry of Local Government and Modernisation (KMD) – now the Ministry of Digitalisation and Public Governance (DFD – Digdir published the first version of its Guide on responsible use and development of artificial intelligence. The Agency also has experience with coordination across sectors (cf. for example, the SKATE Forum). In addition, they are familiar with and participate in the development of standards and other development work in the EU.

Although Digdir has good technological and legal expertise, this is still largely focused on information, advice, guidance and some regulatory work within the public administration. Digdir is not primarily a supervisory organisation and has little practical competence in supervision[28] – neither rights protection supervision nor product supervision. The competence it does have can be found in the Authority for Universal Design of ICT, but since the Authority for Universal Design of ICT is an "independent entity" according to the instructions, this is competence that only to a very small extent flows to other parts of the organisation. The opposite is probably also true. The Authority for Universal Design of ICT does not draw more on Digdir's broad information, advice and guidance expertise related to digitalisation and AI than other supervisory bodies do. Nor is it given that Digdir / the Authority for Universal Design of ICT will become a market surveillance authority under the EU's Artificial Intelligence Act.

[28] In the area of electronic identity verification (eID), the Norwegian Digitalisation Agency (Digdir) collaborates with the Norwegian Communications Authority (Nkom) on requirements for suppliers of market-based eID services and has a formal role related to the notification of eID schemes to the EU. This involves some kind of technical supervision of the providers of eID services and solutions.

New tasks will require additional resources

The Norwegian Digitalisation Agency (Digdir) cannot provide an exact estimate of what the addition of a new role for the Agency would entail in terms of extra use of resources. This would depend both on what tasks and functions are assigned to Digdir and how extensive and resource-intensive the tasks actually are.

In the longer term and depending on how extensive the supervisory tasks assigned to the coordinating market surveillance authority are, Digdir would need to build up specific competencies in the areas of supervision and standardisation. This could be done as part of the existing Authority for Universal Design of ICT, as a new AI market surveillance entity in line with the Authority for Universal Design of ICT, or integrated into the portfolio of Digdir's other tasks. Whichever solution is chosen, this will require additional resources.

The Norwegian Digitalisation Agency has a flexible organisation that makes it possible to move expertise at relatively short notice

The Norwegian Digitalisation Agency (Digdir) is a relatively large organisation and has a non-local organisational structure with about 380 employees across three locations. This means that they would be able, to some extent, to move existing competencies to a new AI body, possibly by expanding the Authority for Universal Design of ICT, relatively quickly. However, unless additional resources are allocated, this would have to be at the expense of other tasks, at least over time. Since there is still so much uncertainty about the scope of the supervisory function, it is also an advantage that Digdir has an important advisory function and other tasks in the field of digitalisation, independently of the EU's Artificial Intelligence Act. This would make it relatively easy to move resources to other parts of the organisation as needed, at least in a transitional phase.

In summary: The Norwegian Digitalisation Agency (Digdir) has a lot of relevant AI expertise, but it is not a supervisory body, and some of Digdir's other roles may give rise to conflicts of interests

Digdir scores high on relevant expertise in digitalisation and has earmarked resources that already work with information, advice and guidance on AI in general and the EU's Artificial Intelligence Act in particular. The biggest challenges are its lack of supervisory competence and the incompatibility of Digdir's potential role as a neutral market surveillance authority with its roles as a provider of important national services, where AI will eventually probably play a central role, and as a "spearhead" for digitalisation and use of AI in the public administration.

4.3.4 The Norwegian Communications Authority (Nkom) as the single point of contact and coordinating market surveillance authority

The Norwegian Communications Authority (Nkom) is an ordinary, gross-budgeted administrative body under the Ministry of Digitalisation and Public Governance (DFD). The Ministry of Transport and Communications (SD) is the responsible governing body for matters in the postal area. Nkom is intended to be self-funded. The industry players

therefore pay sector taxes and fees pursuant to the Regulations of 17 January 2024. The sum that Nkom can collect in taxes and fees is set in the fiscal budget each year.

According to the Ministry of Digitalisation and Public Governance (DFD)'s main instruction for the management of the Norwegian Communications Authority (Nkom), Nkom is "*the central executive supervisory and administrative authority for services within postal, electronic communication and electronic trust services in Norway".* Nkom shall pave the way for innovation and use of new technology and manage and assign frequencies for mobile telephony, radio and television and, on application, telephone number resources to operators.

Nkom is a product safety supervisory authority and is responsible for the following tasks, among others:

- Managing and assigning frequencies for mobile phone, radio, television and (on application) the telephone number resources to operators
- Supervising sales of radio, telecom terminal and network equipment to check that the products comply with the regulations and monitoring the electronic communications industry's prices and offers to consumers
- Supervision of the administration of Norwegian domains and the top-level domain ".no".

This means that Nkom is a market control authority with experience in and routines for monitoring that electronic equipment placed on the market has been conformity-assessed, documented and labelled in accordance with applicable procedures and meets the requirements that have been set for the products in EEA regulations.

The Norwegian Communications Authority (Nkom) has its head office in Lillesand and has regional offices in Lødingen, Trondheim, Bergen and Oslo. 90% of its 170 employees work at the head office.

The Norwegian Communications Authority's primary objective is to ensure innovation and healthy competition in the area of electronic communications, including reliable and secure use of the internet.

Nkom has continuously had to deal with innovation and development of new technologies, such as AI, and is concerned with both the opportunities (innovation, competition, efficiency, quality of service, etc.) and challenges (market failures, end-user interests and security in relation to critical infrastructure). In its written response to the question about the pros and cons of EU's Artificial Intelligence Act from their point of view, Nkom stated that they regard the AI Act as an opportunity for "...safer and more responsible innovation".

Nkom has recently been made responsible for supervision of data repositories and data storage in Norway, and is a relevant candidate for the role of coordinating body for the EU Digital Services Act (DSA). This would help ensure that different aspects of data storage and sharing can be seen in context. From a user perspective, this will be an advantage.

The Norwegian Communications Authority is subject to political governance

With the exception of one area, Nkom is subject to political governance. In the main instruction for Nkom, it is nevertheless stated that *"It follows from the Act in what circumstances the National Communications Authority is exempt from instruction."* (Section. 3.2.1). In practice, this only applies to the area of market regulation.

Complaints and appeals about administrative decisions made by the Nkom are currently submitted to the governing ministry, i.e. the Ministry of Digitalisation and Public Governance (DFD). In the draft new Electronic Communications Act, which is currently awaiting consideration by the Storting, it is proposed, among other things, that a separate appeals board for administrative decisions made by Nkom be established (cf. Proposition no. 93 to the Storting (2023-24) – Bill and Draft Resolution; see also Chapter 6 on our proposal for a complaints and appeals system).

The Norwegian Communications Authority has a number of different roles without this appearing to cause major role conflicts

As discussed in Section 4.3.1, all supervisory bodies will face a possible conflict of interests between the body's role as a supervisory authority and the needs of the subjects of supervision for information, advice and guidance. Most supervisory bodies find ways to handle this. Some choose to separate the two functions organisationally. However, this can also pose challenges, because good information, advice and guidance usually improve when the information on the rules and regulations is supplemented by first-hand experience and examples.

There may also be a role conflict in Nkom's role related to assigning frequencies – which they subsequently supervise. According to Nkom, this is common practice in most countries and is seldom regarded as problematic.

The Norwegian Communications Authority is a product safety supervisory authority with a high level of technological, legal and standardisation expertise, but with less cross-sectoral and advisory expertise

Nkom already has extensive specialist expertise in several of the areas highlighted in Article 70 (4) of the EU's Artificial Intelligence Act, including understanding AI technologies, computer and internet technology, regulation of products and equipment, and cybersecurity. This means they would be able to perform supervision pursuant to the Artificial Intelligence Act when this is necessary within their own sector, and probably also supervision of technologically advanced systems and solutions within other sectors. Nkom's supervision in the field of electronic communications falls under the EU's harmonised framework "New Legislative Framework" (NFL), to which the Artificial Intelligence Act also refers. Through this harmonisation, Nkom has experience in the development of regulations and reporting of the findings of supervision in the digital field at the EU level.

Nkom finds that they have good, stable expertise in the areas highlighted in the EU's Artificial Intelligence Act. Given that it may take slightly longer to recruit new experts to Nkom's head office in Lillesand, it might constitute a challenge with respect to competencies and recruitment if Nkom is assigned a coordination role related to both the Digital Services Act

(DSA) and the Artificial Intelligence Act – in addition to having been given an extended role and responsibilities in connection with data centres in Norway. Assuming it takes longer to recruit the necessary and relevant expertise to Lillesand than it would to jobs in more central parts of Norway, this may lead to capacity challenges if Nkom is assigned several new tasks at the same time.

Nkom has extensive experience with product safety supervision through its responsibility for supervision of products that communicate via a radio interface or via copper and/or fibre-optic cable. Among other things, they have participated in EU and international work in committees and in connection with development of regulations and standardisation work. Within Nkom's areas of expertise, they have experience with different forms of sanctions in the event of non-compliance with the requirements.

Nkom is primarily a sectoral authority. Nkom deals mostly with electronic communications operators, i.e. providers, suppliers, operators and manufacturers of electronic communications services and products, but it also has contact with county authorities, local government authorities, other public authorities, and interest organisations and consumers to build up greater understanding of the services offered by the electronic communications operators. However, compared with the other two candidates, they have limited experience with the deployers of AI.

The sector for which they are authority means that Nkom has some expertise in a number of different sectors. However, this expertise will only be related to electronic communications services and products. If Nkom is appointed as Norway's national market surveillance authority, they will be dependent on good collaboration with relevant sectoral authorities, as well as having to build up their own sectoral competencies in other sectors where they may be given greater supervisory responsibility.

This extended supervisory responsibility will in particular apply in areas and sectors where AI competence has not been built up as part of the supervisory competence (cf. Annex III of the AI Act). Areas for which the local government authorities are responsible, such as education and the welfare sector, are examples of the kinds of areas that might be involved. Although Nkom has contact with the County Governors and the County Emergency Preparedness Councils, especially in the area of security and emergency response, and also receives a special earmarked grant for guidance to county authorities on the government's broadband subsidy, Nkom still has limited experience with information, advice and guidance to at the local government level.

We get the impression that Nkom also currently has limited experience with sandbox methodologies, but that they have a project under way in this regard in collaboration with the electronic communications authorities in other Nordic countries and a private player to develop a form of sandbox in the electronic communications area using a "traffic light" system.

Nkom's head office is located in Lillesand on the south coast of Norway. This promotes the geographical decentralisation of (highly skilled) central government jobs, but might also

make it more demanding to recruit the necessary experts. However, with regard to new recruitment, Nkom's location in Lillesand may also benefit from its proximity to the University of Agder, which has a focus on programmes of study in technology and AI and more recently also law.[29]

Fee financing of supervision of AI systems may entail challenges with respect to equal treatment

Unlike the Norwegian Data Protection Authority (Datatilsynet) and the Norwegian Digitalisation Agency (Digdir), most of Nkom's activities are funded by taxes and fees. If this makes it easier to also fund supervision of AI systems by fees, this could be an advantage from a budgetary standpoint. However, it might also present challenges related to the equal treatment of the subjects of supervision. Today, Nkom primarily supervises relatively large professional players on the manufacturer, supplier and importer side. These are players who are used to having to bear costs related to controls and supervision. It is unlikely to be unproblematic to impose a tax or duty for all types of supervision pursuant to the EU's Artificial Intelligence Act. Again, issues may arise linked to the equal treatment of the subjects of supervision. There is no mention of funding schemes in the Act.

Depending on the scope and organisation, Nkom will need additional resources to build up and maintain the harmonisation and advisory roles entailed by the role as national market surveillance authority.

Many new tasks in parallel might pose a capacity challenge for the Norwegian Communications Authority

Nkom has just been made responsible for supervising data repositories in Norway. While it would promote harmonisation of responsibilities and tasks, the addition of multiple new tasks at the same time will also entail challenges for Nkom's competence and capacity. This could become a challenge, at least in the short term.

In summary: The Norwegian Communications Authority (Nkom)'s main strength is their experience and expertise in product supervision of digital services and products

Nkom has a lot of product supervisory expertise that forms a good starting point for advice and guidance and other forms of support to other market surveillance bodies that have not built up – or that do not see a need to build – extensive AI supervisory competence themselves. At the same time, Nkom will need to build up expertise related to information, advice and guidance on the EU's Artificial Intelligence Act aimed at the government administration and society at large.

[29] NOKUT akkrediterer master i rettsvitskap ved UiA og UiS [NOKUT accredits the Master of Laws programmes at the University of Agder and the University of Stavanger] | The Norwegian Agency for Quality Assurance in Education (NOKUT)

4.4 Recommended organisation – single point of contact and coordinating market surveillance authority

4.4.1 The chosen solution should be reassessed once more experience has been gained

Immaturity and uncertainty make it difficult to make clear recommendations
Immaturity, both in the Norwegian government administration and in many other EU and EEA countries, makes it difficult to come up with a clear recommendation. Both the scope of the supervisory tasks and the costs are highly uncertain at the present time. Our recommendations must be seen in light of this. It is important not to choose a model now that it will be difficult to adapt or modify as we see how the Act works and is practised both in the rest of the EU / EEA and in the government administration in Norway.

It is our impression from the interviews that different parties attach different importance to the various considerations that the Act is intended to address. Some are most concerned with the fact that the EU's Artificial Intelligence Act is primarily intended to promote innovation and cost-effective solutions in the safest and most reliable way possible. Others are most concerned with ensuring protection of personal data and privacy (cf. also the Norwegian Data Protection Authority's latest annual privacy survey). This survey found that 69 percent of respondents believe that artificial intelligence will challenge privacy and the protection of personal data by too much personal data being collected and used in ways that they do not agree with. It also found that 84 percent believe the authorities should take an active role in the regulation of artificial intelligence, although only 33 percent believe that the authorities are actually capable of doing so.[30] Some are most concerned with various ethical issues and challenges that the Act appears not to take into account to any significant extent, such as gender equality and anti-discrimination considerations as well as sustainability and energy consumption. This would entail a range of different risk assessments and reflects different expectations of the role of the market surveillance authorities.

Experiences from other countries are also enlightening. Most countries have not yet decided on their organisational model. Following discussions between the ministries, Denmark has, as mentioned in Chapter 3, chosen the Danish Agency for Digital Government as its market surveillance authority and decided that the Danish Data Protection Agency and the Danish Agency for Digital Government shall collaborate on the regulatory sandbox. The further process between the bodies that will be ascribed tasks pursuant to the Act must clarify the finer details of the allocation of tasks and responsibilities.

[30] Personvernundersøkelsen 2024 - tall og trender [Privacy Survey 2024 – Figures and Trends] | the Norwegian Data Protection Authority]

In light of the great uncertainty, we believe it will be appropriate to reassess the allocation of tasks and responsibilities after a certain period. We think this should ideally be done once there is more experience in the field, after, say, three to five years. It is interesting to note that a Swedish study[31] on the EU Digital Services Act (DSA), which has many of the same roles as the Artificial Intelligence Act, also highlighted that there is great uncertainty and that the distribution of responsibilities should be reassessed after a period, once other EU legal acts have also been implemented.

The high degree of uncertainty is also the reason why we have attached particular importance to flexibility and cost-effectiveness in our recommendations. We therefore recommend an organisation model that to the greatest extent possible is based on the different strengths and mix of expertise and competencies of the existing public administration, and which we believe will work without preventing other, perhaps more appropriate solutions in the future.

In our recommendations, we regard the supervisory function as the main task

In the choice of which body should be assigned the role of coordinating market surveillance authority, it seems logical to consider which tasks (cf. Section 4.3) will have the greatest scope and/or should be afforded the greatest weight, and then choose the body that is best suited to perform these tasks.

What will constitute the bulk of the tasks is currently highly uncertain. Perhaps it will be resource-intensive to conduct supervision in those areas not covered by other market surveillance authorities; perhaps coordinating the understanding of the EU's Artificial Intelligence Act with the other regulatory authorities will be a major task – although this is unlikely in the short term. In the first couple of years, it may also be that most of the tasks will be related to coordination, advice and guidance in connection with the incorporation of the EU's Artificial Intelligence Act into Norwegian law.

These kinds of assessments of the changing scope of the tasks are extremely uncertain and provide little guidance in trying to identify the best candidate. Instead, we will attach importance to how central the tasks will be over time in the role as coordinating market surveillance authority. This leads us to focus on the supervisory function itself and the associated coordination with the other supervisory authorities. We regard this task as the core of the role as coordinating market surveillance authority and a task that defines this role more than any of the other tasks. The other tasks can either be regarded as part of the supervisory function or are tasks that are secondary compared with the supervisory function.

As discussed at the beginning of this report (Section 1.3), the point of departure has been a two-tier model, based on the Act's proposed governance structure ensuing from Annex I. We have not considered how the responsibility for the high-risk areas and systems described in

[31] En inre marknad för digitala tjänster – ansvarsfördelning mellan myndigheter [An internal market for digital services – distribution of responsibilities between authorities], Swedish Government Official Report SOU 2023:2

Annex III should be distributed among individual agencies. This should be explored in more detail once the main organisational structure has been decided and the various players have gained more knowledge about, and are thus better able to assess, the most appropriate organisation.

The choice of geographical location of new central government jobs must be properly investigated and assessed

The Guidelines on the location of central government workplaces and central government service production are intended to contribute to robust labour markets in parts of Norway other than Oslo, key municipalities near Oslo and other major cities, and are in addition to the requirements laid down in the Instructions for official studies and reports. The Guidelines apply to the establishment of new agencies, the establishment of new entities, and expansions as a result of new tasks in existing agencies. Minor changes and adjustments within an agency are exempt. In connection with major changes, a number of different conditions must be assessed, such as the need for physical proximity to the users, access to qualified labour, and requirements for physical and digital infrastructure. In connection with processes encompassed by the Guidelines, the choice of location must be based on a written assessment.

The Guidelines must be complied with if a new body is established – regardless of whether it involves a transfer of tasks and resources from existing agencies or not. If new tasks are assigned to an existing agency, it will usually depend on the scope and/or size, in the form of new central government jobs, whether the organisation can be characterised as a new "entity" or not, and the access to technological and legal expertise. Today, the Norwegian Data Protection Authority (Datatilsynet) is located in Oslo, the Norwegian Digitalisation Agency (Digdir) has offices in Oslo, Leikanger and Brønnøysund, and the Norwegian Communications Authority (Nkom) has its head office in Lillesand and small regional offices in Lødingen, Trondheim, Bergen and Oslo.

4.4.2 The establishment of a new body is discouraged

In the Norwegian Agency for Public and Financial Management (DFØ)'s opinion, none of the four options outlined in Section 4.2 are ideal for the role as the national market surveillance role.

We do not recommend establishing a new body for a number of reasons: there is such great uncertainty about the scope and content of the national supervision; it will be demanding to recruit the necessary expertise, at least in the short term; and it will be very expensive. This is especially true if it turns out that the scope or required competencies are not as initially thought. Growing awareness of and focus on the ever-increasing deployment of AI in the government administration and society in general means that competence raising in this area is already underway in many places – with the associated capacity challenges.

With so much uncertainty about the organisation, responsibilities, scope and tasks, making use of existing professional environments will probably provide greater flexibility than

building up a new body from scratch. In this context, we would add that the inter-ministerial working group reached a similar conclusion, i.e. they advised building on an existing body (Working Group Report 2023, p. 20).

It is also often both costly and demanding to move responsibilities from existing supervisory authorities to a new body, especially if this involves geographical relocation of workplaces (cf., among other things, Asplan Viak's 2009 evaluation of the decentralisation of supervisory authorities).[32] We therefore recommend that the new AI functions initially be assigned to an existing body, but as discussed in Section 4.4.1, that the organisation of these functions be reassessed after a few years of practical experience. Among other things, it should be considered whether it is more appropriate to separate out units responsible for the supervision of AI and gather them all, and possibly also other EU supervisory functions, in one place.

Against the backdrop of this recommendation, the organisational solutions we recommend will not, in our opinion, entail extensive structural changes. This might make it easier to introduce changes at a later date, once we know more about how alternative organisational solutions work.

4.4.3 The single point of contact and coordination role should be assigned to the Norwegian Communications Authority (Nkom)

We recommend that the role as single point of contact and market surveillance authority be assigned to the Norwegian Communications Authority (Nkom), and that Nkom is thereby given responsibility for the tasks described in Section 4.2.1. In addition to the role as single point of contact and the coordination function, the Norwegian Communications Authority (Nkom) will, unless otherwise decided by overarching authorities, be responsible for inspections that do not belong to other market surveillance authorities (cf. Annex I and III of the Regulation) as well as providing advice, guidance and information on the Regulation to other stakeholder groups.

Nkom is a sectoral supervisory authority that has extensive experience with product safety supervision in areas related to digital communication and internet solutions and systems. As we understand it, they will in principle be able to operate the supervisory function as soon as it is established. Although it is currently uncertain how much and how extensive supervision there will be to begin with, this is still an advantage compared to the Norwegian Digitalisation Agency (Digdir) and the Norwegian Data Protection Authority. Nkom has the opportunity to use its existing capacity and expertise, while both the Norwegian Data Protection Authority and the Norwegian Digitalisation Agency (Digdir) would have to build up or acquire expertise related to supervision of product safety to a greater extent.

The expansion of Nkom's role in the data storage area and possibly responsibility for coordination pursuant to the EU Digital Services Act (DSA) will probably serve to strengthen

[32] Tilsynsevaluering_komparativ.pdf [Comparative evaluation of supervisory authorities]

Nkom's cross-sectoral and harmonisation competencies. The new Electronic Communications Act highlights that both market regulation and consumer rights are to be strengthened.

The Norwegian Data Protection Authority and the Norwegian Digitalisation Agency (Digdir) both have significant legal expertise and extensive experience with information and advisory work. In addition, the Norwegian Data Protection Authority has broad experience with supervisory work, whereas Digdir has extensive technological expertise. Although Digdir is responsible for supervision in the area of universal design of ICT, it cannot be characterised as a supervisory organisation. Both Digdir and the Norwegian Data Protection Authority have limited experience with product safety supervision related to digital systems and solutions. Digdir in particular also has limited experience with and knowledge of the supplier side and the market. Nor is it certain that the Norwegian Data Protection Authority and/or Digdir will be designated as market surveillance authorities pursuant to the EU's Artificial Intelligence Act (cf. the guidelines in Annexes I and III of the AI Act).

If Digdir is chosen as the market surveillance and coordination body, in our opinion there will be a conflict of interests between the Agency's role as a supervisory body and its role as a provider of national services and components. This speaks against Digdir, in particular because Digdir's portfolio as a provider of national components constitutes a significant part of the Agency's total operations, and because Digdir will become a subject of the obligations if they develop their own AI solutions in connection with the national components and services. As stated in Section 4.3.3, it does not appear to be relevant to "spin off" the work on national components. This reinforces our assessment that Digdir's various roles may present a conflict of interest.

Another factor that ought to be taken into account if the supervisory function were to be assigned to Digdir is what this would mean for the Agency in the long term – what roles and profile should Digdir have in the work on digitalisation? Bearing in mind that one Digdir's main objectives is to define the premises for digitalisation and cohesive information management, and to be a clear voice both upwards to the Ministry, and out the rest of the administration and the general public, it can be queried whether it is appropriate for the organisation to have a stronger focus on supervision and monitoring. This will to a greater extent lead to the Agency having a more critical outward profile (cf. the feedback we have received about the role and position of the Norwegian Data Protection Authority).

The Norwegian Data Protection Authority is a supervisory organisation, but has little experience with product safety supervision. These are competencies that the Authority must build up if they are given responsibility for supervision pursuant to the EU's Artificial Intelligence Act in areas where independence is particularly important, i.e. for biometric systems related to law enforcement, border management and the judiciary; however, to date it has not been decided that or whether the Norwegian Data Protection Authority will be assigned this kind of role.

As long as the Norwegian Data Protection Authority has such a strong and clear role in the area of data protection, it will – in our opinion – be challenging for them to achieve sufficient

credibility in the role as an impartial market surveillance authority in the field of AI. This applies regardless of the fact that the Norwegian Data Protection Authority in recent years has toned down the role as an ombud that they have previously held. However, over time changes in the Artificial Intelligence Act and/or data protection legislation may lead to this changing.

4.4.4 Advice, guidance and information on the EU's Artificial Intelligence Act will be particularly important in the first few years

The Norwegian Communications Authority (Nkom), the Norwegian Digitalisation Agency (Digdir) and the Norwegian Data Protection Authority (Datatilsynet) should be tasked with collaborating on information, advice and guidance on AI and the EU's Artificial Intelligence Act

As Norway's single point of contact and coordinating market surveillance body, the Norwegian Communications Authority (Nkom) will have overarching responsibility for information, advice and guidance on the EU's Artificial Intelligence Act. The overview of possible tasks in Section 4.2.1 shows that information, advice and guidance cover different task areas. A key task will be to coordinate and facilitate collaboration with the other supervisory authorities, including providing advice and guidance and assisting less experienced market surveillance authorities in the practical execution of supervision of compliance with the product safety regulations. Other important advisory tasks will include providing information, advice and guidance on AI, providing advice and guidance to operators and suppliers, and operation of a regulatory sandbox.

It is assumed that the various information, advisory and guidance tasks will be most time-consuming and resource-intensive in the first few years. The supervisory function itself will probably have a correspondingly small scope in the first few years, and then increase in both scope and significance. This coincides well with the experiences of the Norwegian Data Protection Authority in connection with the introduction of the General Data Protection Regulation (GDPR) in 2018. In the first few years, they prioritised advice and guidance on the new regulations.

The Norwegian Communications Authority (Nkom) has an advisory role through the advice and guidance it provides in its areas of responsibility and collaborates broadly with other authorities both nationally and internationally, especially in the area of risk and emergency response. In our opinion, the Norwegian Communications Authority (Nkom) will be well equipped to provide information, advice and guidance related to the role of coordination with the other market surveillance bodies, and probably also information, advice and guidance to operators and suppliers on standards and the requirements that follow from these. However, Nkom has far less experience with cross-sectoral information, advice and guidance to deployers of AI and stakeholders covered by the EU's Artificial Intelligence Act and/or who are not directly related to the execution of supervision.

Nkom has a high level of advisory competence on product safety supervision and supervision of digital products and services. The Norwegian Data Protection Authority has a lot of expertise in information, advice and guidance related to the introduction of EU regulations aimed at both the public and private sectors, as well as experience in the operation and organisation of sandboxes with several AI projects. The Norwegian Digitalisation Agency (Digdir) has a high level of expertise in digitalisation and innovation in general and on AI and the EU's Artificial Intelligence Act in particular. Although Digdir's information work has primarily been directed at the public sector, much of its expertise and advisory material will probably also be relevant to commercial players and the general public.

It is important that information, advice and guidance in the field of AI are harmonised and that systems are established for flow of information and collaboration. To ensure this, especially in the first few years, we believe it will be important to build on and make use of existing expert environments and their comparative advantages. We therefore recommend that the Nkom, Digdir and the Norwegian Data Protection Authority be tasked with collaborating on information, advice and guidance on AI. They must work together to agree on an appropriate distribution of tasks.

A key objective of the proposed organisation is to ensure a cohesive, harmonised guidance and advisory service. In our assessment, it will have a major positive impact if key players in the field of digitalisation establish good, constructive collaboration. In our view, mandatory collaboration between government agencies with different perspectives will serve to contribute to more cohesive guidance and advisory services.

The collaboration should include the establishment and operation of a regulatory sandbox

In our opinion, the regulatory sandbox should also be a collaborative undertaking, in a similar vein to in Denmark, where the regulatory sandbox for the EU's Artificial Intelligence Act and the General Data Protection Regulation (GDPR) will be jointly managed by the Danish Agency for Digital Government and the Danish Data Protection Agency.[33] Similarly, Sweden has decided to establish a pilot for a regulatory sandbox for artificial intelligence as a joint venture between the Swedish Companies Registration Office (*Bolagsverket*), the Swedish Tax Agency (*Skatteverket*), the Swedish Public Employment Service (*Arbetsförmedlingen*) and the Swedish Authority for Privacy Protection (IMY), which is roughly equivalent to the Norwegian Data Protection Authority.[34] Even if a sandbox pursuant to the EU's Artificial Intelligence Act has a different purpose and requirements than the sandbox pursuant to the General Data Protection Regulation (GDPR), the experiences from establishing and operating a sandbox should also be exploited here. In addition, it will be natural to involve the coordinating market surveillance authority (Nkom) in a sandbox so that their experiences can be actively used in the sandbox work and vice versa.

[33] Regulatorisk sandkasse [Regulatory sandbox] (datatilsynet.dk)
[34] https://www.imy.se/nyheter/imy-deltar-i-pilotprojekt-for-ai-regulatorisk-sandlada/

We know from the interviews that tensions are likely to arise between different considerations and regulations, such as between the regulations in the area of AI and other, more rights-based, regulations – like the General Data Protection Regulation (GDPR), for example. Collaboration on a sandbox will be able to contribute to common expertise on opportunities and limitations that follow from the AI regulations – and the data protection regulations – and thereby also to better and more harmonised information, advice and guidance for manufacturers, providers and different user groups.

A user board should be established related to the information, advice and guidance function

We also recommend that as part of this joint information, advice and guidance function, a user board be established where representatives of the various stakeholders can discuss their needs for advice, guidance and information and their needs related to implementation of and compliance with the EU's Artificial Intelligence Act. In particular, we would underline the need to involve the local government level (the municipalities), but also representatives of consumers, the business sector, and especially small and medium-sized enterprises, equality and anti-discrimination interests etc. should be included in a board of this nature.

The three agencies should be tasked with coming up with concrete proposals for how the collaboration should be organised, coordinated and resourced

It must be investigated in more detail how this kind of a collaboration should be organised and resourced; compare again with Denmark, where the Agency for Digital Government and the Data Protection Authority have been tasked with finding an appropriate organisation. We recommend that the three partners be jointly tasked with finding good solutions for this, including what resource use this will require at the various agencies. Since all three agencies are organised under the Ministry of Digitalisation and Public Governance (DFD), it may be appropriate to include identical instructions on this in the letters of allocation for the three agencies.

If such a solution cannot be implemented, an alternative could be that the Norwegian Communications Authority (Nkom) recruits, buys and/or borrows expertise that enables them to safeguard the information, advisory and guidance function alone. Another option might be to permanently transfer information skills and across-the-board expertise from other central government agencies and environments that currently have these types of competencies.

It will nevertheless be demanding to establish a clear and unambiguous division of roles and responsibilities between the various agencies' guidance, advice and information responsibilities as long as they all want tasks and responsibilities in connection with digitalisation and thus also AI. The division of roles and responsibilities in this area will therefore have to be considered in more detail once the overarching distribution of roles and responsibilities is in place, and experience has been gained of the new roles and functions.

5 The accreditation function

5.1 Accreditation in general

Accreditation means to give official authorisation or approval as trustworthy, on the basis of documented expertise and quality. Thus, accreditation requires an assessment of the entity concerned.

For government authorities, this will mean that a separate accreditation body assesses the subject of the obligations' specialist expertise, governance and quality systems, etc. and – where applicable – grants them authorisation to conduct business. The system may be such that accreditation is given to specific conformity assessment bodies that in turn check and – as applicable – certify the subjects of the obligations. Regardless, accreditation schemes will mean that the supervisory body is helped with, but not relieved of, its tasks. The supervisory body must still be able to carry out active supervision, for example in the form of random spot checks.

In Norway, Norsk akkreditering provides accreditation, primarily in more technical areas of supervision (cf. the Norwegian Act on the free trade of goods in the EEA (2013). Even if Norsk akkreditering is the accreditation body, they will not decide who will be allowed to apply for accreditation as a technical conformity assessment body in the various areas. In some cases, requirements regarding accreditation ensue from regulations, but enterprises can also apply for accreditation independently.

5.2 On accreditation pursuant to the EU's Artificial Intelligence Act

As discussed in Chapter 2.1, at least one competent authority must be appointed to the role of "notifying authority". This authority(ies) will accredit technical conformity assessment bodies ("notified bodies"), which in turn will conduct conformity assessments of AI systems, i.e. whether the systems comply with recognised standards.

According to the EU's Artificial Intelligence Act, accreditation, i.e. the role as notifying authority, encompasses the following tasks:

- Assessment, i.e. assessing conformity assessment bodies on the basis of an application,
- Designation, i.e. formally designating a conformity assessment body on the basis of an assessment (with an attached accreditation certificate),
- Notification, i.e. reporting / registering the conformity assessment body with the EU,
- Monitoring, i.e. monitoring and as applicable reassessing the accreditation.

The EU's Artificial Intelligence Act allows for two alternative ways of organising this role. One option is that all four tasks are assigned to one central government body, or if preferred distributed by sectors across several government bodies.

The other option is that this role is shared between a national accreditation body, which takes care of assessment and monitoring, and one or more government agencies, which perform the designation and notification / registration. This latter option is already known in Norway in cases where the regulations require accreditation of conformity assessment bodies. For example, a body that wants to be designated as a conformity assessment body for pressure equipment must apply to the Norwegian Directorate for Civil Protection (DSB).[35] The application must be accompanied by, among other things, an accreditation certificate issued by Norsk akkreditering confirming that the body meets the requirements for provision of conformity assessment services. Accreditation is granted after a further assessment of the conformity assessment body's quality systems and competencies. On the basis of an accreditation certificate, the Norwegian Directorate for Civil Protection (DSB) can then designate the conformity assessment body and register it with the EU.

5.3 Recommended organisation – accreditation

A main impression from the analysis of the EU's Artificial Intelligence Act and the interviews is that there is uncertainty about what the Act actually requires and when the prerequisites (the standards) will be in place. This makes it very difficult to determine how accreditation should best be organised. More knowledge is needed here, including how other EU and EEA countries choose to organise this role.

As mentioned above, the EU's Artificial Intelligence Act allows for two alternative organisations of the accreditation role. We have assumed the latter option will be the most appropriate in Norway, i.e. that the role is divided among several bodies. This means that as standards and regulations come into place, Norsk akkreditering will be assigned the tasks linked to accreditation assessment and monitoring of assigned accreditations for AI. The other two tasks related to accreditation (formal designation and notification / registration with the EU) will be assigned to the relevant specialist authorities in the sectors concerned. In this context, we have attached importance to making use of established systems. In particular, we regard it as advantageous to make use of and build on Norsk akkreditering's existing experience and expertise. We assume that this task will not have a greater scope than what Norsk akkreditering can handle.

The alternative of adding assessment and monitoring of technical conformity assessment bodies to one or more governmental bodies appears to be less appropriate, in terms of both capacity and competencies. It may also be best in term of orderliness that these kinds of assessment tasks be kept separate from the formal designation, which ought to be done by an ordinary government authority. By contrast, we see reason to allocate the other two tasks (designation and notification / registration) to existing sector authorities in order to make best use of sector-specific knowledge and to ensure that the sector authorities have a real responsibility for designation and staying up to date on the accreditations that are made.

[35] The Norwegian Directorate for Civil Protection (DSB) 2021: Veiledning til forskrift om trykkpåkjent utstyr §36 [Guide to Section 36 of the Regulation on pressure equipment]

In areas where there is no market surveillance authority, or in cases where different roles cannot be assigned to a single body (the same body cannot be both the accreditation body and the technical conformity assessment body), the task of designating accredited conformity assessment bodies should be assigned to the coordinating market surveillance authority.

6 Complaints and appeals

Since the market surveillance authorities are to make individual administrative decisions, there must be a system for appealing the decisions. Sector-specific knowledge, expertise and independence are key aspects in this context.

6.1 Organisational requirements

According to the committee charged with preparing a new Public Administration Act, the main purpose of the central government's processing of complaints and appeals is to strengthen trust and confidence in the government administration by ensuring that decisions are correct. This involves:

- Correcting errors in the legal or factual basis on which the decision was made.
- Correcting a decision when relevant factors have been overlooked, when the administrative decision does not adequately safeguard the purpose of the Act, or when the administrative decision constitutes a disproportionate burden for a private party (Official Norwegian Report NOU 2019:5).

Obligatory two-level processing sets parameters for the organisation of the handling of complaints and appeals

The government administration's imposition of duties and granting of rights are done through individual administrative decisions. Pursuant to the Public Administration Act, individuals have the right to appeal a central-government individual administrative decision and to have the decision re-considered by a body that is independent of the first level. At the same time, this requirement for two-level processing necessitates a hierarchical organisation of the central government's handling of complaints and appeals.

In practice, there are two main options for the organisation of the system after the first level has decided not to find in favour of the appellant:

a) The appeal is sent to the governing body, usually a directorate or a ministry (and in some cases the King in the Council, if a ministry was the appeals body on the first level).
b) The appeal is sent to a separate appeals board. These kinds of boards are collegial bodies specialised in handling complaints and appeals. They are independent of the ministry under which the subject of the appeal belongs. The appeals boards vary widely in terms of size, composition, rules for case processing and decision-making, etc.

Main option a) is used when there is no need to ensure political independence for the handling of the appeal. Main option b) safeguards requirements for independence from the Ministry and thus from political governance. Independence is usually formalised by the ministry's authority to issue instructions and overturn decisions vis-à-vis the board being removed by law or regulation.

Implementation of new EU regulations often necessitates the establishment of an appeals board

The 1980s and 1990s saw a surge of new independent bodies, including complaints handling bodies and appeals boards. In addition to relieving the ministries' workload, the idea was to ensure independence from political governance by formally removing the minister's authority to issue instructions. The growth in the number of complaints handling bodies and appeals boards has since been stopped, but the implementation of new EU regulations often requires independence from the governing ministry, necessitating the establishment of a new complaints handling body / appeals board.

Over the past two decades, greater emphasis has been placed on organising bodies with a view to promoting harmonisation and stronger expert environments. This is an argument against organising the handling of complaints and appeals into specialised complaints handling bodies / appeals boards, at least if they are to be specialised in very narrow fields. In connection with organisation of complaints handling bodies and appeals boards, it is particularly important to ensure sufficient capacity and competence.

In general, increased importance has been attached to building stronger expert environments to ensure the rule of law, quality, and more efficient use of resources. This is manifested in, among other things, the fact that a number of complaints handling bodies / appeals boards have been merged to have broader mandates and that two joint secretariats have been established that serve several complaints handling bodies / appeals boards at the same time.

Horizontally: **Complaints and appeals are handled centrally or decentrally**

Horizontally, the question is whether the handling of complaints and appeals should be carried out centrally in one body or decentrally as part of the administration of the sector concerned. In practice, this will mainly be a question of the need for – and access to – specialist expertise (in AI) and sector-specific knowledge.

An appeals body will need to have sufficient expertise to process an appeal about an administrative decision concerning AI, at least if the volume of cases is of such a scope that the appeals body cannot rely on contracting in, or possibly buying, external expertise the (few) times it is needed. Setting up an AI Appeals Board for each sector will be problematic in terms of acquiring and keeping up-to-date relevant AI expertise for all of them. It may also be more difficult to ensure equal treatment than if the appeals were dealt with centrally.

The main argument in favour of a decentral solution is the need for sector-specific knowledge. It follows from the EU's Artificial Intelligence Act that several of the authorities that are market surveillance authorities under existing regulations will also act as market surveillance authorities under the EU's Artificial Intelligence Act in the areas for which they are already responsible. This shows that sector-specific knowledge is considered necessary, most probably because AI will be integrated into products that are also subject to requirements (and thus also supervision) by virtue of other, sector-specific product safety regulations. This kind of emphasis on sector-specific knowledge indicates that appeals handling systems pursuant to existing market surveillance regulations can also act as the

appeals handling system for administrative decisions pursuant to the Artificial Intelligence Act.

An additional factor here is that a decentral solution will be able to benefit from established systems. Our impression from the interviews is that the current system for handling complaints and appeals in the relevant sector should also be used for appeals about administrative decisions regarding AI.

Vertically: governing body or appeals board
Vertically, questions may arise related to the two main alternatives for handling complaints and appeals: The appeal is handled by the immediate governing body or in a separate independent appeals board.

In those cases where the processing of appeals has been assigned to an independent appeals body, this is a solution that ensures independence from political governance. In those cases where the governing ministry is the appeals body, there is no political independence. The question is thus how much importance should be attached to political independence.

The EU's Artificial Intelligence Act does not appear to impose any requirements on the organisation of the handling of complaints and appeals; for example, there are no requirements concerning political independence for appeals bodies. Can we thus assume the same degree of political independence when it comes to handling appeals about administrative decisions concerning AI as has been used in the relevant sector so far? If not, a transition from the processing of appeals by the ministry to an independent appeals board in the relevant sectors should be considered.

6.2 Recommended organisation – the handling of complaints and appeals

There is also a great deal of uncertainty with respect to the scope of the handling of complaints and appeals. This includes both how many complaints and appeals there will actually be and when they will come.

Two main models have been outlined above – a single, common appeals board or that any appeals about administrative decisions made by the market surveillance body are not treated differently than other appeals, i.e. appeals about the Norwegian Data Protection Authority's supervision go to the Norwegian Privacy Appeals Board (Personvernnemnda), appeals about the Financial Supervisory Authority of Norway's administrative decisions go to the Norwegian Financial Services Complaints Board (FinKN), appeals related to the Authority for Universal Design of ICT, which is part of the Norwegian Digitalisation Agency (Digdir), go to the Ministry of Digitalisation and Public Governance (DFD), etc.

Since the latter option is also common practice for other EU regulations, we propose to continue the current arrangements. In some cases, this will mean that the handling of appeals is carried out by the ministry. This applies, among other things, to the Norwegian Communications Authority (Nkom). Where the consideration of political independence

dictates that the processing of appeals should not be continued in the ministry, an exception should be made by establishing a special appeals board.

As regards the Norwegian Communications Authority (Nkom), it is worth noting that there is a proposal in the draft new Act on Electronic Communications that appeals against Nkom's administrative decisions should be transferred from the Ministry to a special appeals board. One of the reasons behind this is that the so-called Electronic Communications Directive has set "*requirements that the appeals body must be independent of the parties concerned and of interference from outside or political pressure that might obstruct an independent assessment of cases it is to deal* with." (Proposition no. 93 to the Storting (2023-24) – Bill and Draft Resolution Chap. 20).

For Nkom's current decisions, it is thus possible that the processing of appeals will be transferred from the Ministry to a special appeals board. We assume that this may at the same time serve as an appeals body for what we propose as the coordinating market surveillance authority for AI. In addition, this arrangement will be beneficial to improve the competence situation in the processing of complaints and appeals. It is also stated in the Electronic Communications Directive that the appeals body *"must have the expertise necessary to carry out its tasks."*

Sector-specific appeals handling systems are likely to be vulnerable to a lack of competence. The existing appeals boards do not have – and are hardly likely to be able to obtain and maintain – sufficient specialist expertise in AI. However, with reference to the Electronic Communications Directive, the new appeals board for the Norwegian Communications Authority (Nkom) will need to be provided with more resources to build up the necessary expertise in AI. In which case, sector-specific appeals boards will be able to transfer complicated cases pertaining to AI to this new appeals board, or borrow or hire expertise from the board to resolve the cases under their own direction.

After a few years of experience with the Act and developments in the number of appeals case, it can be considered whether to establish a joint AI appeals board for all the sectors if the recommended solution proves sub-optimal.

7 Costs and budget impact

We have concentrated our discussion on costs associated with the governance system and have not looked at what this will entail for suppliers, deployers and third-party conformity assessment bodies.

Some Member States have started looking into the size of the costs that the EU's Artificial Intelligence Act will entail. Everyone seems to agree that this will be challenging – both because the Artificial Intelligence Act had not been finally adopted at that time and also because so far no detailed information has been provided on how the supervision should or must be implemented or how extensive it will be. Firstly, it is uncertain what proportion of the AI systems will be classified as high-risk systems (cf. Section 2.1). Secondly, there is uncertainty as to how much of the supervision will be undertaken by the various national supervisory authorities. Thirdly, there is uncertainty regarding what competencies providing information, advice, guidance and supervision of AI will require in the different sectors.

The challenges associated with estimating the consequences of the Artificial Intelligence Act have much in common with what Sweden experienced when they investigated the consequences for the Swedish government administration related to the EU Digital Services Act (DSA) in 2023.[36]

7.1 Costs for the government administration in the short term and the long term

Since most Member States have not yet decided on how to organise the administrative system, the discussion so far has focused on the various tasks that follow from the Act. A distinction can be drawn here between an implementation and growth phase in the period 2024–26 and the operating phase from 2026 onwards. According to this discussion, a relatively large share of the costs will be quite low in the first few years, but will increase over time. At the same time, there will be some extra costs in the first few years related to the establishment and development of key functions, standards, supervision methods, etc.

There will be costs regardless of whether the various functions are assigned to an existing body or a new body is established. There will be costs related to establishing the new functions and competence building, etc. and costs related to supervision, coordination, and contact and dialogue with the various bodies in the EU. While costs associated with establishing functions and roles will be highest in the first few years, costs associated with ongoing tasks are likely to increase over time, in parallel with the increase in the scope of

[36] En inre marknad för digitala tjänster – ansvarsfördelning mellan myndigheter [An internal market for digital services – distribution of responsibilities between authorities], Swedish Government Official Report SOU 2023:2 (regeringen.se)

high-risk AI systems and solutions. The table below provides an overview of predicted cost items that will need to be covered in the fiscal budget.[37]

Phase	Budget impact*	Expense indicators
Establishment phase (first 1–3 years)	Establishment of a new single point of contact and market surveillance authority - Planning and facilitation, nationally and internationally, including legal and regulatory work, training, and advisory and guidance work, etc. - Recruitment and training costs (building up competence on the EU's Artificial Intelligence Act, the market surveillance function, sandbox methodology, etc.)	- Full-time equivalents required - Purchase of (expert) services - Other expenses
	Establishment of a national accreditation body - Planning and facilitation, including legal and regulatory work, training, and advisory and guidance work, etc. - Recruitment and training costs (building up competence on the EU's Artificial Intelligence Act, the role and function of the accreditation body, etc.)	
	Establishment of an appeals body, or as applicable expansion of existing complaints and appeals bodies - Planning and facilitation, including legal and regulatory work, training, and advisory and guidance work, etc. - Building up competence on the EU's Artificial Intelligence Act - Any technical obligations and provisions	
Operating phase (increasing from year 1 onwards)	Number of full-time equivalents (legal, AI, supervision, standardisation) - Single point of contact / market surveillance function - Supervisory role (central and sectoral)** - Accreditation - The handling of complaints and appeals - Guidance and assistance to all players (providers, distributors, deployers, supervisory bodies, etc.)	- Costs – office space (average) - Cost per full-time equivalent (average cost per type of full-time equivalent) - Other expenses (travel and accommodation costs, etc.)
	Costs related to (physical) workplaces: premises, office equipment, travel expenses, etc. (centrally and in the sectoral supervisory authorities)**	
	Costs related to participation in processes and interaction with EU AI bodies as well as AI market surveillance authorities in other EU and EEA countries	

* Expenses. Net budget impact will depend on which regulatory activities and accreditation/approval schemes are intended to be funded by taxes and/or fees

**Depends to some degree on how many sectoral supervisory authorities are given extended responsibilities for AI market surveillance

There will be major challenges both in estimating needs for resources in the individual year and in assessing how the resources should be distributed among the various authorities. In the first few years, most of the costs will be linked to information, advice, guidance and

[37] The overview of (possible) cost components is partly taken from preparatory assessments in the EU and partly from the guide by the former Norwegian Government Agency for Financial Management (SSØ) and the Norwegian Agency for Public Management and eGovernment (Difi) Guide – restructuring of central government agencies from 2008.

competence building. Later on – from approximately 2027 – the costs associated with supervision are likely to increase.

If our recommendations are adopted, the financing model must also be discussed. Today, the Norwegian Communications Authority (Nkom) and the Financial Supervisory Authority of Norway charge a fee for their supervisory activities. The other market surveillance authorities' supervisory activities are mainly financed by allocations paid via the fiscal budget. In isolation, it is natural to think that fee financing of the Norwegian Communications Authority (Nkom)'s and the Financial Supervisory Authority of Norway's supervisory activities should be continued, especially since supervision of AI will often be included as part of other supervisory work. At the same time, challenges may arise related to equal treatment, especially for Nkom, if they are to supervise areas and/or sectors that are not included in their original area of responsibility. The solution here may be that responsible sector authorities are charged for the costs of the supervision.

In connection with processes encompassed by the Guidelines on the location of central government workplaces, a written assessment must be used as the basis for the choice of location. Among other things, the costs of various options for location must be included in this assessment and/or documented.

7.2 Assessment of financial and administrative consequences

It is difficult to assess the budgetary consequences of the proposal for the administrative model. As discussed above, it depends, among other things, on the scope of the various tasks and which administrative and financing models are chosen.

When it comes to the choice of national market surveillance authority, this will entail a minimum of two to three full-time equivalents related to the work vis-à-vis the EU / EEA. In addition, there will be work related to the coordinator role and to information, advice and guidance, including the establishment of a national sandbox solution. If it is decided to establish a user board, or a national AI board, this will entail further expenses.

As for the rest of the system, it will depend on the number of market surveillance authorities. The more AI market surveillance authorities it is planned to have, the more resource-intensive the administration of the system is likely to be – at least in the long term. However, for most of the bodies, it will take some time before it is appropriate to carry out supervision pursuant to the EU's Artificial Intelligence Act. The resource needs are likely to be fairly limited in the first few years, and it must be possible to assume that some of the general competence building on AI can be achieved through training and re-prioritisation of resources within existing frameworks, as is the case in other public agencies.

Using figures from the central government accounts for 2023, an average expense per full-time equivalent can be calculated based on the corresponding average in eight relevant

central government agencies.[38] This gives an average cost of approximately NOK 1.04 million per full-time equivalent (measured in Norwegian kroner at the 2023 rate). If we add an overhead cost of 50 percent, related to office space, ICT equipment, etc., we get an estimated cost of about NOK 1.6 million per year (in Norwegian kroner at the 2023 rate). This estimate will entail an annual cost of NOK 8 million for five full-time equivalents, NOK 16 million for ten full-time equivalents, etc., (measured in Norwegian kroner at the 2024 rate).

As an example, two additional full-time equivalents at 12 market surveillance authorities, five full-time equivalents for the coordinating market surveillance authority (to safeguard the roles of single point of contact, coordination body and supervisory body) and five full-time equivalents for the establishment and operation of the regulatory sandbox will lead to a total resource requirement of 34 full-time equivalents. Given an annual cost of NOK 1.6 million, this corresponds to an annual cost of just under NOK 60 million, given last year's inflation and pay increase. In comparison, NOK 7 million was allocated to the Norwegian Data Protection Authority's regulatory sandbox in 2023. Based on our assumptions, this probably corresponds to four full-time equivalents.

There may be questions about how realistic it is to build up specialised technical and legal expertise related to AI in so many supervisory bodies. In addition to great uncertainty about the scope and number of subjects of supervision, many of the bodies we have interviewed stress that recruiting specialist expertise in technological competence is generally – and will continue to be – a challenge in the years to come (cf. also a study from Samfunnsøkonomisk analyse (SØA) from 2021 on supply and demand for ICT competence).[39] As discussed earlier in the report, the purchase of services and assistance in the market, possibly from one of the larger market surveillance authorities, may be a more realistic option, especially for sectoral supervisory authorities where the supervision of AI systems will not be a major component in their supervision. The purchase of services will also require resources, but will be more flexible and adapted to the needs.

It is likely that Norsk akkreditering will need significantly more resources as the standards with the associated need for accreditation are issued. However, it is reasonable to assume that the net impact on the budget will be limited to any increase in Norsk akkreditering's participation in international work. The accreditation work itself will probably be funded by fees.

[38] The Norwegian Ocean Industry Authority, the Directorate of e-health, the Norwegian National Security Authority (NSM), the Norwegian Data Protection Authority, the Norwegian Directorate for Civil Protection (DSB), the Norwegian Communications Authority (Nkom), the Norwegian Digitalisation Agency (Digdir) and the Norwegian Medical Products Agency (DMP)

[39] Norway's needs for advanced expertise today and in the future

References

Aftenposten. (2022). *Hvordan kan vi holde algoritmene i ørene? Forskningsmiljøer står klare til å hjelpe*. [How can we keep the algorithms in check? Researchers are ready to help] https://www.aftenposten.no/meninger/debatt/i/pWRzpw/hvordan-kan-vi-holde-algoritmene-i-oerene-forskningsmiljoeer-staar-klare-til-aa-hjelpe

Agenda Kaupang. (2023). *Evaluering av Datatilsynets sandkasse for kunstig intelligens:* Microsoft Word - Rapport Datatilsynet Evaluering av sandkassa (3)[Evaluation of the Norwegian Data Protection Authority's sandbox for artificial intelligence. Microsoft Word – Report Norwegian Data Protection Authority Evaluation of the sandbox (3)]

appliedAI. (2023). *AI Act Risk Classification Study*: https://aai.frb.io/assets/files/AIAct-Risk-Classification-Study-appliedAI-March-2023.pdf

Artificial Intelligence Act Impact Survey. (2022). *AI Act Impact Survey Report*: https://aai.frb.io/assets/files/AI-Act-Impact-Survey_Report_Dec12.2022.pdf

Boletín Oficial del Estado. (2023). *Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial [Royal Decree 729/2023 of 22 August approving the Statute of the Spanish Agency for the Supervision of Artificial Intelligence]:* https://www.boe.es/diario_boe/txt.php?id=BOE-A-2023-18911

Broomfield, Heather and Lise Reutter. (2019). *Kunstig intelligens/Data Science: En kartlegging av status, utfordringer og behov i norsk offentlig sektor [Artificial Intelligence/Data Science: A mapping of the status, challenges and needs in the Norwegian public sector]:* KI%2C+data+science+ +Kartlegging+av+status%2C+utfordringer+og+behov+i+norsk+offentlig+sektor.pdf (ntnu.no)

The Norwegian Data Protection Authority. (2024). *Personvernundersøkelsen 2024 [Privacy Survey 2024]*: Personvernundersøkelsen 2024 - tall og trender [Privacy Survey 2024 – Figures and Trends] | the Norwegian Data Protection Authority]

The Danish Data Protection Authority (DK): Regulatorisk sandkasse for AI [Regulatory sandbox for AI] Regulatorisk sandkasse [Regulatory sandbox] (datatilsynet.dk)

The Norwegian Data Protection Authority. (2023). *Annual report for 2023:* *https://www.datatilsynet.no/omdatatilsynet/arsmeldinger/arsrapport-for-2023/*

DFØ report 2022:5. *Færre og bedre – en evaluering av statsforvalterstrukturen [Fewer and better – an evaluation of the County Governor structure]*

The Norwegian Digitalisation Agency. (no date). *Veiledning for ansvarlig bruk og utvikling av kunstig intelligens [Guide for responsible use and development of artificial intelligence]:* Veiledning for ansvarlig bruk og utvikling av kunstig intelligens [Guide for responsible use and development of artificial intelligence] | Norwegian Digitalisation Agency (Digdir)

The Norwegian Digitalisation Agency. (no date). *EU-regelverk om deling av data [EU rules on data sharing]:* EU-regelverk om deling og bruk av data [[EU rules on the sharing and use of data] | Norwegian Digitalisation Agency (Digdir)

Digi.no. (2024). *Danskenes KI-tilsyn legges til Digitaliseringsstyrelsen [Denmark has designated the Danish Agency for Digital Government as its AI supervisory authority]*:

https://www.digi.no/nyhetsstudio/danskenes-ki-tilsyn-legges-til-digitaliseringsstyrelsen/40338?showFeed=1

The Danish Agency for Digital Government. (2024). *Rollen som national tilsynsmyndighed med EU's AI forordning skal varetages af Digitaliseringsstyrelsen [The role of national supervisory authority in connection with the EU's AI Act assigned to the Danish Agency for Digital Government]:* https://digst.dk/nyheder/nyhedsarkiv/2024/april/rollen-som-national-tilsynsmyndighed-med-eu-s-ai-forordning-skal-varetages-af-digitaliseringsstyrelsen

Norwegian Directorate for Civil Protection (DSB) (no date) *Om SLO [About SLOs].* Om SLO [About SLOs] | Norwegian Directorate for Civil Protection (dsb.no)

Norwegian Directorate for Civil Protection (DSB). (2021). *Veiledning til forskrift om trykkpåkjent utstyr §36 [Guide to Section 36 of the Regulations on pressure equipment]:* https://www.dsb.no/veiledere-handboker-og-informasjonsmateriell/veiledning-til-forskrift-om-trykkpakjent-utstyr/

European Commission (no date). *Digital Services Act*. Accessed on 13 June 2024 from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

European Commission (no date). *National specialised courts: Spain*. Retrieved from https://ejustice.europa.eu/19/EN/national_specialised_courts?SPAIN&member=1

The European Commission. (2021). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and am ending certain union legislative acts*. Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

The European Parliament. (2023). *European Parliament decision of 12 December 2023 on the Council position at first reading with a view to the adoption of a Regulation (EU) 2023/... on artificial intelligence for a competitive and sustainable Europe (Artificial Intelligence Act) (11162/3/2023 – C9-0452/2023 – 2021/0361(COD))* [Tekst vedtatt av Europaparlamentet]: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf

Council of Europe. (2022). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts* [Document ST-14954-2022-INIT]: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf

Council of Europe. (2024). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts* (Document PE-24-2024-INIT): https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf

The Norwegian The Ministry of Government Administration and Reform (FAD). (2009). *Evaluering av utflytting av statlig virksomhet [Evaluation of the decentralisation of central government functions]:* Evaluering av utflytting av statlig virksomhet - komparativ analyse [Evaluation of the decentralisation of central government functions – a comparative analysis] (regjeringen.no)

The Norwegian Ocean Industry Authority. (2024). *Written answers to questions related to AI and the EU's Artificial Intelligence Act (unpublished)*

The Swedish Authority for Privacy Protection (IMY). (2024). *IMY deltar i pilotprojekt för AI-regulatorisk sandlåda [IMY participating in pilot project for an AI regulatory sandbox]:* IMY deltar i myndighetsgemensamt pilotprojekt för AI-regulatorisk sandlåda [IMY participating in a cross-sectoral pilot project for a regulatory sandbox for AI]

Ministry of Local Government and Regional Development (KDD) (2023). *Hovedinstruks for Datatilsynet [Main instructions for the Norwegian Data Protection Authority]:* Hovedinstruks i ny mal for 2023 [New look for main instructions for 2023] (regjeringen.no)

Ministry of Local Government and Regional Development (KDD) (2023). *Hovedinstruks for Digitaliseringsdirektoratet [Main instructions for the Norwegian Digitalisation Agency (Digdir)]:* Microsoft Word - Hovedinstruks Digitaliseringsdirektoratet- 2023 [Main instructions for the Norwegian Digitalisation Agency (Digdir) – 2023] (regjeringen.no)

Ministry of Local Government and Regional Development (KDD) (2023). *Hovedinstruks for Nasjonal Kommunikasjonsmyndighet [Main Instructions for the Norwegian Communications Authority (Nkom)]*: https://www.regjeringen.no/contentassets/a4e341d613e244a48ed8146d7e345b32/2023_hovedinstruks-nkom.pdf

Ministry of Local Government and Regional Development (KDD) (2022). *Retningslinjer for lokalisering av statlege arbeidsplassar og statleg tjenesteproduksjon [Guidelines on the location of central government workplaces and central government service production]*: https://www.regjeringen.no/no/dokumenter/retningslinjer-for-lokalisering-av-statlege-arbeidsplassar-og-statleg-tenesteproduksjon/id2924136/

The Norwegian Association of Local and Regional Authorities (KS) R&D project no. 236007 (2024). *Barrierer og muligheter i kommunal sektors arbeid med kunstig intelligens [Barriers and opportunities in the municipal sector's work on artificial intelligence]*: KS/Sopra Steria: Barrierer og muligheter i kommunal sektors arbeid med KI [Barriers and opportunities in the municipal sector's work on artificial intelligence]

The Norwegian Communications Authority (Nkom). (2024). *Written answers to questions related to AI and the EU's Artificial Intelligence Act (unpublished)*

The Norwegian Agency for Quality Assurance in Education (NOKUT). (2023). *NOKUT akkrediterer master i rettsvitenskap ved UiA og UiS [NOKUT accredits the Master of Laws programmes at the University of Agder and the University of Stavanger]:* NOKUT akkrediterer master i rettsvitskap ved UiA og UiS [NOKUT accredits the Master of Laws programmes at the University of Agder and the University of Stavanger] | The Norwegian Agency for Quality Assurance in Education (NOKUT)

Proposition no. 1 to the Storting (2023–2024). Ministry of Finance.

Proposition no. 93 to the Storting (2023-24) – Bill and Draft Resolution. Ministry of Digitalisation and Public Governance (DFD): *Lov om elektronisk kommunikasjon (ekomloven) [Act relating to electronic communications (Electronic Communications Act)]:* https://www.regjeringen.no/contentassets/096a9d827c8f48c3ae8b7817fe463a25/no/pdfs/prp202320240093000dddpdfs.pdf

Norwegian Government Agency for Financial Management (SSØ) / Norwegian Agency for

Public Management and eGovernment (Difi). (2008). *Omstilling av statlige myndigheter [Reform of central government authorities]:* veilder_omstilling_gevinstkost.pdf(regjeringen.no))

Statistics Norway. (2024). *Digitalisering og IKT i offentlig sektor [Digitalisation and ICT in the public sector]*: https://www.ssb.no/teknologi-og-innovasjon/informasjons-og-kommunikasjonsteknologi-ikt/statistikk/digitalisering-og-ikt-i-offentlig-sektor

Swedish Government Official Rep SOU 2023:2: *En inre marknad för digitala tjänster – ansvarsfördelning mellan myndigheter [An internal market for digital services – distribution of responsibilities between authorities]*: En inre marknad för digitala tjänster – ansvarsfördelning mellan myndigheter [An internal market for digital services – distribution of responsibilities between authorities], Swedish Government Official Report SOU 2023:2 (regeringen.se)

The Storting. (2023). *Minutes from the meeting of the Storting on Thursday 16 March 2023* [Case no. refs-202324-0116]: https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Referater/Stortinget/2023-2024/refs-202324-01-16/?m=3

Søyland, M., Ørnes, H., & Sjøtun, S. G. (2019). *Statens kompetansebehov i den digitale fremtiden: Utfordringer og tiltak [The State's need for expertise in the digital future: Challenges and measures]* (NIFU report 2019:30). The Nordic Institute for Studies in Innovation, Research and Education (NIFU) : https://nifu.brage.unit.no/nifu-xmlui/bitstream/handle/11250/2646485/NIFUrapport2019-30.pdf?sequence=1&isAllowed=y

The Norwegian Board of Technology. (2024). *Generativ kunstig intelligens i Norge [Generative artificial intelligence in Norway]:* Generativ-KI-i-Norge_digital.pdf (wpd.digital)

Western Norway Research Institute (Vestlandsforsking). (2023). *Kunstig intelligens i offentlig sektor [Artificial intelligence in the public sector]*: https://www.vestforsk.no/sites/default/files/2023-03/VFrapport7_2022_KI_i_offentlig_sektor.pdf

World Economic Forum. (2023). *The Future of Jobs 2023*: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf

Appendix 1: Data collection and methods

The data used in this report were primarily obtained through document studies and interviews.

Document studies

As per August 2024, there are a number of technical changes to regulations that still need to be made before the Act can be formally adopted by the EU. Chapter 2 of the report: *The EU's Artificial Intelligence Act* and Appendix 2: *Description and analysis of the Act* have mainly been written on the basis of a legal document review of the current latest version of the Act from 2 February 2024.[40] Other new EU legislation that overlaps with the EU's Artificial Intelligence Act have also been important in understanding the context and overall situation of the EU's regulation of the digital area. In addition, these parts of the report are based on other reports and documents written in connection with and as a supplement to various versions of the AI Act.

The report is also based on documents and reports on the organisation of regulatory supervision and the characteristics of various types of supervision, accreditation schemes and the handling of complaints and appeals. Both Norwegian and international documents that map the considerations to be taken into account in connection with the regulation of AI in particular have also been reviewed.

Interviews

It has been important for the project to highlight key stakeholders' views and opinions on the enforcement of the EU's Artificial Intelligence Act. We sent out more than 37 interview inquiries and conducted a total of 24 interviews with representatives from different stakeholder groups: framework setters, various types of supervisory bodies, producers of AI and users of AI.

Table 2 below shows the organisations we have interviewed.

Table 2: Interview overview

Group	Organisation
Framework setters	The Ministry of Digitalisation and Public Governance (DFD)
	The Ministry of Health and Care Services (HOD)
	The Ministry of Energy (ED)
	The Directorate of Health
	The Ministry of Education and Research (KD)
	The Ministry of Culture and Equality (KUD)
Supervisory authorities and other administrative bodies	The Norwegian Consumer Authority
	The Norwegian Data Protection Authority

[40] AG (artificialintelligenceact.eu)

Group	Organisation
	The Financial Supervisory Authority of Norway
	The Norwegian Ocean Industry Authority*
	The Norwegian Medical Products Agency
	The Norwegian Digitalisation Agency
	The Directorate of Health
	The Norwegian Directorate for Education and Training
	The Norwegian Communications Authority
	Norsk akkreditering
	The Equality and Anti-Discrimination Ombud
	DNV**
	The Danish Ministry of Digital Affairs
User groups	The Norwegian Association of Local and Regional Authorities – KS
	Abelia
	ICT Norway
	Oslo Origo
Manufacturers	Microsoft Norway

**The Norwegian Ocean Industry Authority has answered the questions in writing*

***DNV has been placed in the group of authorities that will be affected by virtue of it being a potential third-party conformity assessment body*

The interviews were conducted as semi-structured interviews and were based on an overarching interview guide.

Interviews allow us to obtain opinions and experiences from stakeholders with varying points of view. Findings and views that emerge in the interviews are important as a basis for discussing the various alternatives. At the same time, it is important to be aware that the people we interview represent different interests and stances. This means that the topics discussed in the interviews have – necessarily – varied, and that the information from the interviews must be analysed and seen in the context of the stakeholders' different objectives and perspectives.

Other sources of data

In addition to document studies and interviews, the project team has attended two international meetings where the EU's Artificial Intelligence Act and the organisation of the governance apparatus for enforcement of the Act have been discussed. One meeting was organised by the Nordic–Baltic working group on regulatory issues related to digitalisation (Nobareg), and the other by a European working group of competent authorities on AI. These meetings have been important for hearing about the work that is taking place in connection with the establishment of a governance structure for enforcement of the EU's Artificial Intelligence Act in the Nordic countries, the Baltic States and elsewhere in Europe and what considerations it is deemed important to take into account in the assessments.

Over many years, the Norwegian Agency for Public and Financial Management (DFØ) – formerly the Norwegian Agency for Public Management and eGovernment (Difi) and the Directorate of Public Management (Statskonsult) – have built up expertise on and given advice on the organisation and functioning of the government administration (cf. for

example, the overview of reports and memos on the Norwegian Agency for Public and Financial Management's website (https://dfo.no/rapporter). This type of experience-based knowledge about governance and the public administration is particularly important in discussions of different organisational strengths and weaknesses.

Weaknesses and limitations in the data basis

A number of aspects limit the usefulness of the underlying data that forms the basis for this report. First, the interviews revealed that large parts of the Norwegian public administration must be characterised as relatively immature in terms of AI and the EU's Artificial Intelligence Act. Even though we have interviewed representatives of a range of different stakeholder groups, we cannot say that they constitute a representative sample. This means that the collected data give the project very few well-considered assessments of which considerations the various stakeholder groups believe are most important in establishing a governance structure in this area. It is also difficult to weigh the different stakeholder groups' assessments up against each other. The interview material has therefore primarily been used to map the stakeholders' previous experiences with supervision, their general views on the regulation of AI, and the current situation in terms of competencies and resources. Where reference is made to interview data, it is only done on an aggregate level.

Secondly, there is little documentation of real alternatives for establishing a governance structure for the enforcement of the EU's Artificial Intelligence Act internationally. This is probably because other nations' government administrations have a similar degree of immaturity as was found in the Norwegian administration. Other than the examples mentioned in Chapter 3 of the report: *What are other countries thinking and doing?*, it is our experience that other countries have not come much further than Norway in their assessment of which authorities ought to play a central role in the governance structure.

Appendix 2: Description and analysis of selected parts of the EU's Artificial Intelligence Act

1 National competent authorities

1.1 What are national competent authorities?

Article 70 (1) of the EU's Artificial Intelligence Act states that "Each Member State shall establish or designate as national competent authorities at least one notifying authority and at least one market surveillance authority for the purposes of this Regulation."

In the list of definitions in Article 3 of the Artificial Intelligence Act, "national competent authorities" are defined in paragraph 48 as follows: "national competent authority' means a notifying authority or a market surveillance authority". According to the definition, then, all market surveillance authorities and notifying authorities are national competent authorities. It is thus not a particular role that must be given or assigned to certain market surveillance authorities and notifying authorities. This is further supported by the fact that Article 70 (4) and (5) list requirements that apply to the competent authorities, which would naturally apply to all competent authorities and not only to any specially designated authorities. Nevertheless, one of the market surveillance authorities must be designated as a "single point of contact" (cf. Article 70 (2) and the description of this in Appendix 2, Section 1.2.3.

1.2 Market surveillance authorities in more detail

1.2.1 Organisation

The starting point pursuant to Article 70 (1) is that at least one market surveillance authority must be established. However, Article 74 (3) f. indicates a number of areas where existing authorities shall act as market surveillance authorities.

Article 74 (3) states that the authorities responsible for market surveillance for the areas regulated by the Union harmonisation legislation listed in Annex I, Section A, shall also be market surveillance authorities for these areas for the purposes of the Artificial Intelligence Act. For Norway, this includes:

- The Norwegian Ocean Industry Authority
- The Norwegian Directorate for Civil Protection
- The Norwegian Environment Agency
- The Norwegian Maritime Authority
- Norwegian Customs
- The Norwegian Building Authority

- The Norwegian Communications Authority
- The Norwegian Railway Authority
- The Norwegian Labour Inspection Authority
- The Norwegian Medical Products Agency

Article 74 (6) further states that for high-risk AI systems placed on the market, put into service, or used by financial institutions regulated by Union financial services law, the market surveillance authority for the purposes of the AI Act shall be the relevant national authority responsible for the financial supervision of those institutions under that legislation. However, this is only in as far as the placing on the market, putting into service, or the use of the AI system is in direct connection with the provision of those financial services. For Norway, it can be assumed that this will be the Financial Supervisory Authority of Norway.

Article 74 (8) (cf. Annex III) states that the market surveillance authority for high-risk biometric AI systems to be used for law enforcement purposes, border management and justice and democracy, and for the high-risk AI systems listed in points 6, 7 and 8 of Annex III, shall be the competent data protection supervisory authorities under Regulation (EU) 2016/679 (the "General Data Protection Regulation") or Directive (EU) 2016/680 (the "Law Enforcement Directive") or any other authority as long as it is subject to the same conditions laid down in Articles 41 to 44 of the Law Enforcement Directive. Only the General Data Protection Regulation (GDPR) has been implemented as part of the EEA Agreement. The Law Enforcement Directive has been implemented in Norway as part of the Schengen Agreement. In Norway, the Norwegian Data Protection Authority (Datatilsynet) is the supervisory authority for these Directives. It follows from Article 74 (8) that the Norwegian Data Protection Authority or any other authority can be designated, provided that the other authority is subject to the conditions laid down in Articles 41 to 44 of the Law Enforcement Directive. This indicates that the EU's Artificial Intelligence Act regards systems related to law enforcement, border management and the judiciary as systems where it is especially important to meet specific conditions, including requirements regarding independence (cf. Article 42 of the Law Enforcement Directive)

Regardless of whether it is the Norwegian Data Protection Authority or some other authority that subject to the requirements laid down in Articles 41 to 44 of the Data Protection Directive that is designated, the exact range of systems that the authority is to supervise pursuant to the EU's Artificial Intelligence Act is somewhat unclear as the Act does not apply to systems related to national security[41] or to areas not covered by the EEA Agreement. Therefore, the area of responsibility of this authority under the EU's Artificial Intelligence Act in Norway will in principle be the areas specified in Article 74 (8) (cf. Annex III), provided that these are systems that fall within the scope of the Artificial Intelligence Act and EEA Agreement. Given the systems listed in these provisions, it is conceivable that there will be difficulties drawing up boundaries in several areas. Whether the respective authority shall

[41] Cf. among others, Article 4 (2) of the Treaty on European Union (TEU); cf. Article 3 of the EU's Artificial Intelligence Act

also be the supervisory authority for areas not covered by the EEA Agreement will be up to the individual nation to decide and is beyond the mandate of this project.

The Member States have the opportunity to deviate from the solution proposed in the Artificial Intelligence Act for market surveillance authorities and to adapt the system to national needs (cf. for example, Article 70 (1); cf. Article 74 (4), (7) and (8)). In this context, there are grounds to emphasise that the Artificial Intelligence Act has slightly different approaches to freedom of choice:

- **Market surveillance related to existing product safety regulations and the financial service area (cf. Article 74 (3), Article 74 (6); cf. Article 74 (7)):** The EU's Artificial Intelligence Act sets a specific model and appoints specific authorities for these areas. It then goes on to suggest that these requirements can be deviated from. The point of departure is thus that the specified authorities are chosen, unless a Member State wishes to choose another relevant authority as market surveillance authority in these areas. This indicates that the Artificial Intelligence Act contains a preferred solution.
- **Market surveillance related to law enforcement purposes, border management and justice and democracy (cf. Article 74 (8)):** In contrast to the situation related to product safety regulations and financial services in respect of market surveillance, there is no general starting point in the Act, which can then be deviated from in this area. For this area, a number of options are presented, with specific conditions that they must meet. This indicates that there is greater freedom of choice and that the AI Act does not have a preferred solution to the same extent.

Annex III describes several AI systems that are to be regarded as high risk. With the exception of biometric AI systems to be used for law enforcement purposes, border management and justice and democracy, and the systems mentioned in Annex III, points (6), (7) and (8) (see the discussion above), the Act does not directly designate any specific market surveillance authority. Some categories overlap with areas that are already covered by existing market surveillance authorities. For example, systems listed under point (4) of Annex III related to employment, workers management and access to self-employment will probably overlap to some extent with areas that are under the jurisdiction of the Norwegian Labour Inspection Authority.

At the same time, there are categories, such as those listed in point (5) (a) of Annex III, which deal with AI systems used to assess the eligibility of individuals for public benefits and services, which are not naturally covered by market surveillance authorities designated in Annex I, Section A, of the AI Act (cf. Article 74 (3)) If the structure of the AI Act is followed, each Member State will have to make a specific assessment in which the market surveillance authorities designated in accordance with Annex I, Section A (cf. Article 74 (3)) are assessed against the areas described in Annex III to determine whether there are areas that are not covered by the designation suggested in the Act. Then an assessment must be made, based on the individual Member State's organisation, to determine how these outstanding areas are to be covered.

1.2.2 Tasks

The market surveillance authority's tasks

The market surveillance authority is defined in Article 3 (26) as the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020 (the "Market Surveillance Regulation"). In the EU Market Surveillance Regulation, market surveillance is defined in Article 3 (3) as the activities carried out and measures taken by market surveillance authorities to ensure that products comply with the requirements set out in the applicable Union harmonisation legislation and to ensure protection of the public interests covered by that legislation.

How market surveillance is to be carried out is described both in the EU's Artificial Intelligence Act and in the EU Market Surveillance Regulation, but precise procedures for its implementation are not specified anywhere. However, Article 11 (1) and (3) of the EU Market Surveillance Regulation specify that the market surveillance authorities must carry out effective market surveillance on an adequate scale of products made available on the market. In deciding what is an adequate scale and what types of checks are to be carried out, market surveillance authorities must follow a risk-based approach taking into account the following factors:

- Possible hazards and non-conformities in the products
- Activities and operations under the control of the economic operator
- The economic operator's past record of non-compliance
- If relevant, the risk profiling performed by the customs authorities designated under Article 25 (1) of the Market Surveillance Regulation
- Consumer complaints and other information received from other authorities, economic operators, media and other sources that might indicate non-compliance.

In addition to supervision, the market surveillance authority shall establish the procedures to ensure that natural or legal persons who have reason to believe that the AI Act has been breached can submit complaints pursuant to Article 85 of the EU's Artificial Intelligence Act and Article 11 (7) (a) of the EU Market Surveillance Regulation. The market surveillance authorities must therefore develop procedures for following up on complaints or reports on issues relating to risks or non-compliance.

In order to contribute to compliance with the Act, the market surveillance authorities may, in accordance with Article 70 (8) of the AI Act, offer guidance and advice on the implementation of the Act, with a particular focus on small and medium-sized enterprises and start-ups. In this work, they shall involve other relevant authorities, as appropriate (cf. Article 70 (8) of the EU's Artificial Intelligence Act). This guidance and advice should serve as a supplement to the standards, for example by dealing with areas not covered in the standards or by helping to clarify how enterprises should navigate among the various actors, such as market surveillance authorities, conformity assessment bodies, etc.

How should the market surveillance authorities relate to standards?

According to the structure of the EU's Artificial Intelligence Act, compliance with the requirements laid down in the Act will mainly be met through conformity with harmonised

standards as referred to in Article 40 and in Recital 117. It is specified in Article 40 that if high-risk AI systems or general-purpose AI models (GPAI) are in conformity with these standards, they are presumed to be in conformity with the requirements set out in the AI Act.

For suppliers, this will in practice mean focusing on ensuring the correct understanding and application of the harmonised standards, rather than interpreting the Artificial Intelligence Act itself. For their part, the market surveillance authorities will need to conduct assessments based on whether the systems are in line with the standards that the suppliers cite in their conformity assessments. These will often be technical assessments that go beyond pure interpretation of the text of the relevant regulations and will include an analysis of various test parameters, benchmarking processes and other technical frameworks relevant to evaluating an AI system that are used in the standards.

In situations where suppliers do not use harmonised standards, a more in-depth legal interpretation may be necessary. However, assuming that robust harmonised standards are developed, it is expected that most suppliers will prefer to relate to these rather than interpret the Act directly themselves, since the standards are developed with the intention of specifying in concrete and practical terms how to meet the requirements of the AI Act.

The market surveillance authorities' powers

The market surveillance authorities have extensive powers to collect the information they need to be able to perform their tasks. These powers are mainly described in Article 14 of the EU Market Surveillance Regulation. According to this Article, the market surveillance authorities may require economic operators to provide relevant documents, technical specifications, information on the supply chain, etc. and have the power to carry out unannounced on-site inspections and physical checks of products and businesses. Further, according to Article 74 (13) of the EU's Artificial Intelligence Act, they may require access to the source code of systems, provided that the conditions defined in the Article are fulfilled.

If a product or service does not comply with the requirements of the Artificial Intelligence Act, the market surveillance authorities can, pursuant to Articles 16 and 41 of the Market Surveillance Regulation, order the supplier to take corrective action or impose penalties. The sum of penalty fines is specified in Article 99 (3) of the EU's Artificial Intelligence Act, which entitles market surveillance authorities to impose administrative fines of up to EUR 35 million or 7% of the undertaking's total worldwide annual turnover for the preceding financial year, whichever is higher.

1.2.3 Designation of a "single point of contact"

It follows from Article 70 (2) that "Member States shall designate a market surveillance authority to act as the single point of contact for this Regulation". It is thus specified that the authority that is designated as a single point of contact must be a market surveillance authority.

Other than stipulating that it is a market surveillance authority that should act as the single point of contact, the text of the EU's Artificial Intelligence Act itself provides little guidance on requirements, organisation and tasks of the single point of contact. The Preamble provides some guidance in this respect; for example, Recital 153 states that "In order to

increase organisation efficiency on the side of Member States and to set a single point of contact vis-à-vis the public and other counterparts at Member State and Union levels, each Member State should designate a market surveillance authority to act as a single point of contact." The Preamble thus states that a main objective of the single point of contact is to ensure coordination and harmonisation vis-à-vis the public, other Member States and the EU bodies.

The EU Market Surveillance Regulation has not operated with a "single point of contact", but rather a "single liaison office" (SLO) (cf. Article 10 (3)) The tasks of a "singe liaison office" are defined in Article 10 (4) which states: "The single liaison office shall at least be responsible for representing the coordinated position of the market surveillance authorities and the authorities designated under Article 25(1) and for communicating the national strategies as set out in Article 13. The single liaison office shall also assist in the cooperation between market surveillance authorities in different Member States, as set out in Chapter VI."

An important point in this regard is that the single point of contact is not intended to replace the single liaison office and that the market surveillance authorities for the AI Act will also be subject to the single liaison office. In other words, these roles are to coexist. The EU Market Surveillance Regulation thus has limited transfer value in respect of the "single point of contact" pursuant to the AI Act. The single liaison office will be responsible for general coordination under the EU Market Surveillance Regulation, while the tasks assigned to the single point of contact under the AI Act will be specific to artificial intelligence. The finer details of the distribution of tasks between the single point of contact and the single liaison office will probably have to be ironed out specifically.

At the EU level, a "European Artificial Intelligence Board" (EAIB) will be established, and one task that may be natural to assign to the single point of contact will be to represent the Member States on the EAIB. Each Member State shall have a representative on the EAIB, but the AI Act does not specifically state which authorities are to represent the Member States. In light of Article 65 (4) and Article 70 (2), it seems likely that the representatives will be from the single point of contact.

Article 74 of the Artificial Intelligence Act highlights a number of authorities that are to be the market surveillance authorities for their respective areas in accordance with Annex I, Section A. For Annex III, relevant authorities have not been specified to a similar extent. This is discussed in more detail in Section 1.2.1 of Appendix 2. It is not clear whether the single point of contact is to have tasks and responsibilities for the areas where the AI Act does not specify a market surveillance authority. One approach might be that the single point of contact acts as a "catch all" and ensures market surveillance in areas that are not currently covered. Another approach might be that the single point of contact collaborates with relevant players to determine responsibility for market surveillance in these areas. Because the EU's Artificial Intelligence Act does not elaborate on this aspect, it will have to be assessed on the national level.

1.3 The notifying authority in more detail

1.3.1 The requirements in the AI Act regarding tasks and organisation

Article 28 (1) of the EU's Artificial Intelligence Act states that Member States shall establish or designate at least one notifying authority. The same also follows from Article 70 (1).

The notifying authority shall be responsible for setting up and carrying out the necessary procedures for "the assessment, designation and notification of conformity assessment bodies and for their monitoring" (cf. Article 28 (1); cf. Article 3 (19)). The procedures shall be developed jointly by all notifying authorities in the Member States in concert.

The process whereby conformity assessment bodies apply to the notifying authority for notification and which criteria the notifying authority can prioritise are described in Article 29 f. of the AI Act. Article 31 in particular sets the requirements that a conformity assessment body must meet in order to qualify to be a notified body.

Article 28 (2) states that Member States may decide that assessment and monitoring are to be carried out by a national accreditation body and in accordance with Article 30 (2). Norway's national accreditation body is *Norsk akkreditering*. The EU's Artificial Intelligence Act only specifies that "assessment" and "monitoring" can be assigned to the national accreditation body, but not the tasks of "designation" and "notification". This may indicate that these tasks cannot be assigned to a national accreditation body. This view is further supported by Article 28 (4) of the Act, which states that the task of "notification of conformity assessment bodies" and "the assessment of those bodies" must be done by different persons. The requirement states the assessment must be done by different *persons* and therefore does not indicate that the roles must be assigned to different *authorities*. The provision nevertheless suggests that doing both tasks at the same time might constitute a potential role conflict.

Since not all tasks incumbent on a notifying authority can be assigned to a national accreditation authority, the designation of the notifying authority can be organised in the two following ways:

1. A national accreditation authority such as Norsk akkreditering is assigned the tasks of "assessment and monitoring", and another authority becomes the "notifying authority" with responsibility for the tasks of "designation" and "notification". At least one notifying authority must be established or designated. This entails that it is possible to establish more than one, for example by distributing this role according to sectors and assigning the role of notifying authority for AI to the authorities that currently serve as a notifying authority or equivalent for the sector.
2. One authority is designated as the notifying authority for AI and is responsible for all the tasks ensuing from Article 28 (1), i.e. "for the assessment, designation and notification of conformity assessment bodies and for their monitoring". In this case, this authority will also have to distribute the tasks to different persons internally in accordance with Article 28 (4). At least one such authority must be established or

designated. This entails that it is possible to establish more than one, for example by distributing this role according to sectors and assigning the role of notifying authority for AI to the authorities that currently serve as the notifying authority or equivalent for the sector.

Specific requirements regarding independence between the notifying authority and notified body are set out in Article 28 (5). These are related to, but are in addition to, the requirements regarding the independence of the national competent authorities pursuant to Article 70 (1) of the AI Act, as discussed in Appendix 2, Section 1.4.

1.3.2 Organisation of the notifying authority pursuant to the existing product safety regulations

Because the EU's Artificial Intelligence Act is a product safety regulation, organising the notifying authority in accordance with the existing product safety regulations may provide some guidance.

One example is the Norwegian Directorate for Civil Protection (DSB), which is an authority that follows up several product safety regulations, including Directive 2014/68/EU (the Pressure Equipment Directive). For the Pressure Equipment Directive, the formal responsibility for designating and notifying conformity assessment bodies" lies with the Norwegian Ministry of Justice and Public Security (JD). This responsibility has been delegated to the Norwegian Directorate for Civil Protection (DSB). The Ministry of Trade, Industry and Fisheries (NFD) notifies designated conformity assessment bodies to the EU Commission and NANDO base on behalf of the Norwegian Directorate for Civil Protection. [42] In respect of the distribution of responsibilities, the Norwegian Directorate for Civil Protection (DSB) writes:

"DSB is the designating authority and the Ministry of Trade, Industry and Fisheries is the notifying authority. DSB is responsible to inform the Ministry of Trade, Industry and Fisheries about every new designated conformity assessment body which needs to be notified further to the EU Commission.

The designation is DSB's decision, which means that the body is then formally designated in Norway. Designation as it is, cannot be used without notification and a designated body cannot perform any kind of conformity assessment activities before they are notified and registered in the NANDO base."

In addition, DSB writes that "*Designation of conformity assessment bodies according to the Pressure Equipment Directive 2014/68/EU is subject to accreditation. Norwegian accreditation (NA) is responsible for accreditation in Norway*."

Based on the organisation as it has been done for the Pressure Equipment Directive, there thus appear to be three roles at the level of notifying authority:

[42] designation-and-notification-of-conformity-assessment-bodies.pdf (dsb.no)

- The designating authority: For the Pressure Equipment Directive, this authority appears to have been assigned to the Ministry of Justice and Public Security in principle, but has been delegated to the Norwegian Directorate for Civil Protection (DSB).
- The notifying authority: For the Pressure Equipment Directive, this authority has been allocated to the Ministry of Trade, Industry and Fisheries. According to Article 28 (1) of the EU's Artificial Intelligence Act, this authority may be assigned to the same body as the designating authority.
- Accreditation: This authority is Norsk akkreditering. According to Article 28 (2) of the Artificial Intelligence Act, an authority like Norsk akkreditering can be assigned the tasks of "assessment and monitoring", but not "designation" and "notifying".

1.4 Independence requirements for national competent authorities

1.4.1 The extent of the independence requirement

The national competent authorities include both market surveillance authorities and notifying authorities. Article 70 is the main provision in respect of the national competent authorities and sets requirements concerning their independence. More detailed requirements for the notifying authorities are specified in Article 28. There is no specific provision in the EU's Artificial Intelligence Act that elaborates on the requirements for the market surveillance authorities, equivalent to Article 28 for the notifying authorities. However, it is stated in Article 74 (1) that the EU Market Surveillance Regulation applies to AI systems covered by the Artificial Intelligence Act. For the market surveillance authorities, the guidelines will thus follow from Article 70 and possibly from the EU Market Surveillance Regulation in cases where this provides specific requirements.

Article 70 of the EU's Artificial Intelligence Act states that national competent authorities shall exercise their authority "*independently, impartially and without bias so as to safeguard the objectivity of their activities and tasks, and to ensure the application and implementation of this Regulation."* Relatively similar provisions can be found in Article 11 of the EU Market Surveillance Regulation and other regulations relating to product safety.[43]

The formulation in Article 70 (cf. Article 11 of the EU Market Surveillance Regulation) contains several elements related to independence. It specifically mentions "independently", "impartially" and "bias". Neither the Preamble to the EU's Artificial Intelligence Act nor the EU Market Surveillance Regulation explain the content of these conditions in any further detail.

It follows from the wording of Article 70 that the aim is to ensure that the authorities are objective in their activities and tasks, and to ensure the application and implementation of the regulations. The authorities must therefore not be subjected to instructions or pressures that will prevent them from being objective in their tasks. A natural linguistic understanding of the term "bias" indicates that it is not only formal roles and connections that might be

[43] See also, for example, REGULATION (EC) No 765/2008

problematic, but also attitudes. The condition concerning bias may be particularly relevant in various roles that where there is no formal "connection", but which might influence the views of a national competent authority.

The wording of Article 70 does not contain any additional conditions calling for a particularly high degree of independence. Here, the Artificial Intelligence Act differs from several other EU regulations that set more qualified requirements for independence, such as Article 52 of the General Data Protection Regulation and Article 50 of the Digital Services Act, which use terms such as "complete independence". By comparison, the requirements defined in Article 70 of the EU's Artificial Intelligence Act regarding independence and impartiality are less comprehensive. The wording thus indicates a more moderate degree of independence compared with other regulations that expressly specify a high degree of independence.

Within the EU's Artificial Intelligence Act, there are also some provisions that have independence requirements that go further than what follows from Article 70.

It follows from Article 74 (8) that the market surveillance authority for high-risk AI systems for biometrics to be used for law enforcement purposes, border management and justice and democracy, as well as systems as referred to in Annex III, points 6, 7 and 8, will either be subject to the requirements of the General Data Protection Regulation or Articles 41 to 44 of the Law Enforcement Directive. This indicates that the EU's Artificial Intelligence Act considers law enforcement, border management and the judiciary as systems where it is especially important to meet specific requirements. This includes requirements regarding independence (cf. Article 42 of the Law Enforcement Directive and Article 52 of the General Data Protection Regulation), which in their wording are stricter than the requirement regarding independence in Article 70 of the Artificial Intelligence Act.

For notifying authorities, additional requirements for independence are defined in Article 28 (3)) It follows from this that notifying authorities must be established, organised and operated in such a way that "no conflict of interest arises" with the conformity assessment bodies. A natural linguistic understanding of the wording, in particular with the use of "no", indicates that the requirement for the notifying authorities' independence is somewhat stricter in relation to the conformity assessment bodies than that which follows from the general requirements for independence in Article 70 (1)).

Article 31 (5) defines special requirements for independence of notified bodies from market players within the AI value chain. This provision states that notified bodies "shall [not] be directly involved in the design, development, marketing or use of high-risk AI systems, nor shall they represent the parties engaged in those activities" (our adaptation). No such specification follows from Article 70.

The Court of Justice of the European Union has considered numerous claims related to independence. For the supervisory authorities in the area of data protection, the requirements regarding independence in the previous Data Protection Directive have been

interpreted strictly.[44] In judgment C-518/07, paragraph 18, it is stated that "*In relation to a public body, the term 'independence' normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure.*" Paragraph 19 of the judgment goes on to state that the addition of "complete" in the General Data Protection Directive indicates «*a decision-making power independent of any direct or indirect external influence on the supervisory authority*". The addition of "complete" indicates even higher demands for independence.

The Court of Justice of the European Union has issued similar opinions on independence related to Directive 2009/72 and Directive 2004/49. Here the Court of Justice of the European Union has stated that "*a status that ensures that the body in question is able to act completely freely in relation to those bodies in respect of which its independence is to be ensured, shielded from any instructions or external influence*"[45]. An important point in this statement is that the requirement regarding independence must be linked to a player or connection from which the authority's independence is to be ensured.

The relevant provisions in Directive 95/46, Directive 2009/72 and Directive 2004/49 referred to in the Court of Justice of the European Union's statements either have qualifiers such as "complete" or have more comprehensive and specific requirements for independence than follows from Article 70 of the AI Act.[46] This makes it somewhat uncertain whether the statements can be used as a general basis in connection with the Artificial Intelligence Act. At the same time, the opinion from the Court of Justice of the European Union is in itself quite general. The Court of Justice of the European Union interprets "independence" in the absence of a specific definition and considers how "independence" should normally be understood. This indicates that these statements can be applied to Article 70 of the Artificial Intelligence Act.

Factors related to the purpose of the Act may suggest that the requirements regarding independence in Article 70 of the EU's Artificial Intelligence Act should not be interpreted too strictly. As product safety legislation, the EU's Artificial Intelligence Act will be complemented by standards with specific requirements. The national competent authorities will primarily be involved in many technical assessments of whether an aspect has been complied with or not. This type of technical assessment will probably be less sensitive to influences such as political governance. This differs from supervisory authorities and institutions charged with ensuring the safeguarding of fundamental rights in rights-based laws. The fact that Article 52 of the General Data Protection Regulation sets such clear requirements in respect of independence is probably related to the authorities' role in safeguarding fundamental rights pursuant to a rights-based set of rules that often involves major discretionary assessments that could be vulnerable to that type of instructions.

[44] Cf. C-518/07 (EUR-Lex - 62007CJ0518 - EN - EUR-Lex (europa.eu)), C-614/10 (EUR-Lex - 62010CJ0614 - EN - EUR-Lex (europa.eu)), C-288/12 EUR-Lex - 62012CJ0288 - EN - EUR-Lex (europa.eu)
[45] Case C-718/18 paragraph 118 - EUR-Lex - 62018CJ0718 - EN - EUR-Lex (europa.eu), Case C-378/19 EUR-Lex - 62019CJ0378 - EN - EUR-Lex (europa.eu) paragraph 32, case C-530/16 62016CJ0530 (europa.eu) paragraph 67
[46] DIRECTIVE 2004/49, Article 21 and Directive 2009/72, Article 35.

Overall, the independence requirement dictates that the market surveillance authorities must be so independent that they can act completely freely and will be objective in their assessments and the performance of their tasks. This means that they must be shielded from any instructions and external influence. The specification "without bias" in Article 70 indicates that it is not only formal roles and connections, but also more informal connections that may lead to the authority not being sufficiently impartial. Article 70 does not contain any additional terms such as "complete" or more detailed requirements regarding independence. This indicates that the independence required in this context is more moderate than for regulations that do contain such qualifiers, such as the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA).

The Court of Justice of the European Union's statements on independence related to Directive 2009/72 and Directive 2004/49 show that independence must be assessed in relation to which actor independence is to be ensured from. This is discussed in the next section.

Because the requirements regarding independence in the EU's Artificial Intelligence Act largely coincide with the requirements regarding independence in the EU Market Surveillance Regulation, the current organisation of market surveillance authorities pursuant to the existing product safety regulations provides good guidance on what is necessary in practice. This is discussed in more detail in Appendix 2, Section 1.4.3.

1.4.2 What connections should independence be secured from?

Article 28 (3) states that notifying authorities shall be established, organised and operated in such a way that no conflict of interest arises with the conformity assessment bodies. Thus, attention is drawn to impartiality in relation to the conformity assessment bodies in particular. The Preamble does not provide any background for this distinction, but it must be assumed that it is related to the fact that the conformity assessment bodies compete to offer third-party certification. Article 28 (5) emphasises this distinction by stating that notifying authorities shall offer or provide neither any activities that conformity assessment bodies perform, nor any consultancy services on a commercial or competitive basis.

In contrast to the situation for the notifying authorities, no particular roles of the market surveillance authorities are highlighted as potentially problematic. Article 70 of the EU's Artificial Intelligence Act does not provide any further guidance, nor can anything further be inferred from Article 11 of the EU Market Surveillance Regulation. The Preamble does not provide any guidance either. For the market surveillance authorities, one approach based on the Court of Justice of the European Union's statement "any instructions or external influence" may be to assess which actors might be able to exert influence on the market surveillance authorities. In the following, we identify three possible connections that it is particularly relevant to consider.

One form of independence relates to the suppliers in a market. If the market surveillance authorities have strong links to suppliers in a market, this could pose a risk of differential treatment and affect competition. This would be contrary to the basic conditions for a free market and for the EU–EEA collaboration. There is thus reason to assume that the

requirement regarding the competent authorities' independence, and especially the independence of the market surveillance authorities, refers to independence from the suppliers in a market. This is also supported by the use of the term "impartial", indicating that all actors should be treated equally. However, the risk related to connections appears to be somewhat smaller for the competent authorities than for the notifying bodies. Article 31 (5) addresses this for notifying bodies with the wording "shall [not] be directly involved in the design, development, marketing or use of high-risk AI systems, nor shall they represent the parties engaged in those activities" (our adaptation). There is no corresponding specification in Article 70.

Another form of independence is political independence. An authority can hardly be said to be "independent" if it can be controlled politically. As can be seen from the discussion in Appendix 2, Section 1.4.1, this will mean that the authority cannot be given instructions or subjected to pressure that means that the authority is not objective in its assessments.

A third form of independence is where a government authority has a special interest that causes tensions in the safeguarding of the objectives behind the EU's Artificial Intelligence Act. This type of independence is not so much a formal independence, but rather a "bias". An example of this might be that the market surveillance authorities are subject to the same regulations that they are in charge of supervising compliance with. This situation is not unique to the EU's Artificial Intelligence Act, and the same tension arises for authorities such as, for example, the Norwegian Labour Inspection Authority, which, in addition to being the supervisory authority responsible for ensuring compliance with the Working Environment Act, must also itself comply with the Working Environment Act. Another example of this is ombuds and similar roles, which entail a special responsibility to safeguard a certain set of regulations and interests. These kinds of roles can affect how an authority approaches a regulatory framework and whether it entails a disproportionate weighting of certain considerations or interests, making it uncertain whether the authority is objective.

For the market surveillance authorities, it can be assumed that links to suppliers in a market, political governance and other special interests are all possible connections that may be incompatible with the requirements of the AI Act regarding independence in Article 70 (cf. Article 11 of the EU Market Surveillance Regulation. Whether these connections are problematic and what is necessary to ensure independence will have to be assessed specifically for each individual authority. Moreover, the discussion in this section is not exhaustive, and there may be other kinds of connections that are also relevant to the provisions.

1.4.3 A practical starting point for independence

What will be necessary in practice to ensure compliance with the requirements regarding independence in Article 70 will have to be assessed specifically in each individual case, to determine whether the relevant authority is sufficiently independent in relation to the parties and connections from which independence is required. Because the requirements for independence in the EU's Artificial Intelligence Act largely correspond to the requirements in existing product safety regulations, the organisation and independence of existing market surveillance authorities can serve as a useful guide for what will in practice be necessary for

the competent authorities pursuant to the Artificial Intelligence Act. A main principle in this context is that Article 11 of the EU Market Surveillance Regulation largely corresponds to the requirements regarding independence in Article 70 of the Artificial Intelligence Act.

The Norwegian Directorate for Civil Protection (DSB) is the "national harmonisation point for market surveillance" (also known as a "single liaison office" or SLO) for the EU Market Surveillance Regulation, with responsibility for coordinating 17 authorities in Norway. These include a variety of different administrative bodies, such as directorates, supervisory authorities and government agencies. There thus seems to be a fairly high degree of flexibility for the organisation of competent authorities under the existing market surveillance regulations. The Norwegian Directorate for Civil Protection's website[47] lists the following bodies:

- The Norwegian Labour Inspection Authority
- The Norwegian Building Authority
- The Norwegian Directorate for Civil Protection
- The Norwegian Consumer Authority
- The Directorate of Health
- The Norwegian Metrology and Accreditation Service
- The Norwegian Food Safety Authority
- The Norwegian Environment Agency
- The Norwegian Communications Authority
- The Norwegian Water Resources and Energy Directorate
- The Petroleum Safety Authority Norway
- The Norwegian Maritime Authority
- The Norwegian Railway Authority
- The Norwegian Medicines Agency
- The Norwegian Public Roads Administration
- Norwegian Customs
- The Civil Aviation Authority Norway

Several of the authorities that have roles pursuant to the EU Market Surveillance Regulation will also have roles pursuant to the Artificial Intelligence Act and thus also be subject to the requirements regarding independence in Article 70 of the AI Act. Because the requirements are relatively similar, this will have limited significance in terms of legalities. This means that if these authorities are regarded as sufficiently independent under the EU Market Surveillance Regulation, it may be assumed that they will also meet the requirements in the Artificial Intelligence Act. Because the requirements regarding independence in Article 11 of the Market Surveillance Regulation and Article 70 (1) of the Artificial Intelligence Act are fairly similar, this also means that if a strict interpretation of the independence requirements in the Artificial Intelligence Act is assumed, this will also apply correspondingly to all the authorities that are subject to Article 11 of the Market Surveillance Regulation. This allows for a broader assessment where aspects such as efficiency and feasibility are likely to also be important factors.

[47] Nasjonalt samordningspunkt for markedstilsyn [National harmonisation point for market surveillance] | Norwegian Directorate for Civil Protection (dsb.no)

1.5 Special questions regarding the relationship between the market surveillance authorities and the notifying authority

1.5.1 Can the same authority be both the market surveillance authority and the notifying authority?

One question related to the organisation of the national competent authorities is whether the Member States can assign the role of notifying authority and the role of market surveillance authority to the same body. Article 70 (1) states that Member States must "establish or designate as national competent authorities at least one notifying authority and at least one market surveillance authority".

The use of the term "and" in Article 70 (1) together with "national competent authorities" in the plural could be interpreted as indicating that these are two separate roles that must be established at different authorities. The last sentence of Article 70 (1) reads: "Provided that those principles are observed, such activities and tasks may be performed by one or more designated authorities, in accordance with the organisational needs of the Member State." This wording indicates that if the requirements regarding independence in the second and third sentences are met, the Member States are free to assign both the role of notifying authority and the role of market surveillance authority to the same authority.

1.5.2 The relationship between notifying authorities and notified bodies that are directly designated in the Artificial Intelligence Act

If the roles of market surveillance authority and notifying authority are assigned to the same authority, the question arises as to whether the market surveillance authorities that pursuant to the Artificial Intelligence Act are to act as a notified body for certain types of third-party certification can also have the role of notifying authority.

Article 43 (1), third paragraph, stipulates that the starting point is that the suppliers can choose which notified body to use, but for systems related to law enforcement, immigration and asylum, the market surveillance authority as referred to in Article 74 (8) or (9) shall act as the notified body. This authority is discussed in more detail in Appendix 2, Section 1.2.1.

Requirements are set regarding the separation of the notifying authority and the notified body in Article 28 (5). This entails that "Notifying authorities shall offer or provide neither any activities that conformity assessment bodies perform, nor any consultancy services on a commercial or competitive basis". A natural reading of the wording implies a clear distinction between notifying authorities and notified bodies. In particular, the wording "any activities" indicates that these roles should be kept separate. The consequence of this is that the authority referred to in Article 74 (8) and (9) cannot also be the notifying authority.

2 Authorities that protection fundamental rights

National public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights have the power and authority under the Artificial Intelligence Act to collect information and implement measures to ensure that AI systems do not infringe fundamental rights (cf. Article 77 of the EU's Artificial Intelligence Act). Each Member State must, within three months of the entry into force of the Act, identify and publish a list of these authorities (cf. Article 77 (2)). Below is a description of these authorities' roles and powers. In the following, these public authorities or bodies that supervise or enforce the respect of obligations protecting fundamental rights will be referred to as "rights protection authorities".

It follows from Article 77 (1) that rights protection authorities have the right to request and access all documentation created or maintained under the Artificial Intelligence Act when access to this documentation is necessary to effectively fulfil their mandates. The rights protection authority must inform the market surveillance authority of the Member State concerned of any such request. If the documentation is not sufficient to determine whether a breach of EU law has occurred, the rights protection authority may ask the market surveillance authority to organise technical testing of the AI system (cf. Article 77 (3))

According to Article 79 (2), the market surveillance authorities must inform and fully cooperate with the rights protection authorities in cases where it identifies risks relating to fundamental rights in its evaluation of an AI system. The rights protection authority must then be involved in the assessments of the system. Next the bodies must jointly assess whether further technical tests are necessary and then decide which corrective actions need to be implemented to address the risks.

The rights protection authorities will thus have an important role and powers to ensure that the deployment of AI systems does not infringe on individuals' fundamental rights. This is done partly through their own work, but also through close collaboration with the market surveillance authorities.

www.dfo.no