Norwegian Ministry of Digitalisation and Public Governance

Strategy

The Digital Norway of the Future

National Digitalisation Strategy 2024–2030

The Digital Norway of the Future

National Digitalisation Strategy 2024–2030

Foreword

Norway is one of the most digitalised countries in the world, and with this strategy, the Government is laying the foundation for us to become the global leader. Digitalisation is not goal in itself. Rather, it is the tool we need to realise the new opportunities and solve many of the major societal challenges we are facing.

We know that our population is ageing and that we need to mobilise a larger workforce. We know that the business sector needs a stronger foundation and greater access to both skills and data. We know that we need to create new jobs, while reducing emissions and taking better care of the natural environment. And we know that we need greater investments in climate change adaptation, safety and digital infrastructure.

Digitalisation can aid us in all these transitions. Thus, digitalisation is not mainly about technology. It is about the people the technology is intended to serve, and how we use technology to build a safe and equitable society with abundant opportunities.

This strategy charts the course for digital Norway towards 2030 with the aim of making Norway the most digitalised country in the world.

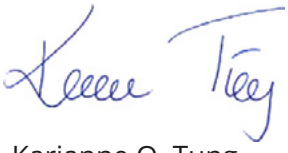
At the same time, digitalisation comes with great responsibility and challenges. We have experienced how screen use affects our children, how disinformation is spread at record speed and how “deep fakes” challenge trust in society. We have also witnessed how some people can quickly be left behind with technology developing more rapidly than ever before.

Our children and young people need to have digital confidence and critical thinking skills. Older adults need to be able to understand and navigate the digital society. Everyone must be included and have equal access. This is a matter of trust and fairness. Digitalisation must benefit all members of society.

To be able to trust technology and that it will be used in our best interests, we must take the helm and steer the course of its development. Technology should not control our society; we should control technology. This is to the benefit of us all. Precisely because this tool is a means to achieving the goal and not the goal in itself.

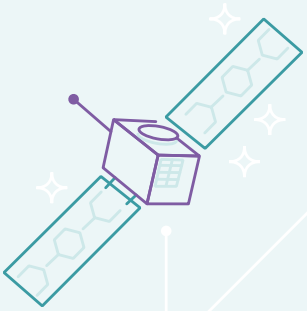
We will implement the strategy in close collaboration with the Norwegian Association of Local and Regional Authorities, the social partners and the business sector. Together, we will leverage digitalisation to build and secure our country.

Jonas Gahr Støre
Prime Minister



Karianne O. Tung
Minister of Digitalisation and Public Governance

Contents



NATIONAL DIGITALISATION STRATEGY 2024–2030

Prerequisites

1 Strengthening governance and coordination in the public sector
2 Ensuring a secure and future-oriented digital infrastructure
3 Bolstering security, emergency preparedness and crime prevention
4 Ensuring appropriate and safeguarded privacy for all
5 Securing future-oriented digital competence

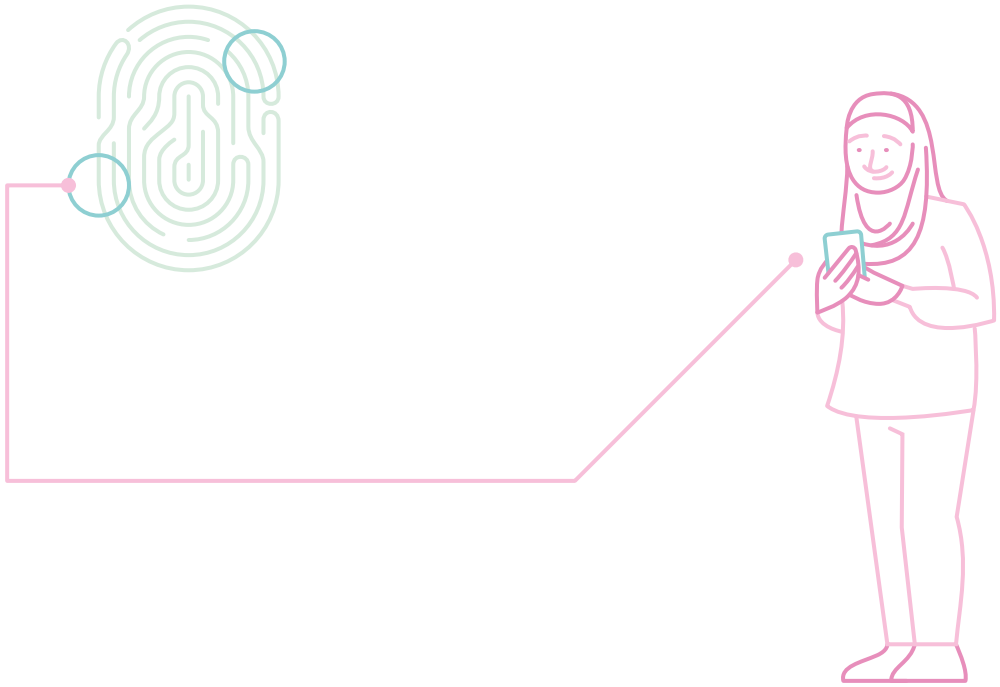
Prioritised areas

6 Increase data sharing and harness the opportunities in data and data-driven innovation
7 Harness the opportunities of AI
8 Accelerating the green and digital transitions
9 Promote an adaptable and innovative business sector
10 Maintaining trust, strengthening inclusion, and safeguarding considerations for children and young people

1

Norway – the most digitalised country in the world

In 2030, Norway will be the most digitalised country in the world and will have succeeded in the digital transformation of our society. Digitalisation will make everyday life easier and safer for citizens, make businesses more competitive and improve the public sector.



The Government's fundamental goal is to create a safer and fairer Norway with opportunities nationwide. This entails a policy that gives people the opportunity to enjoy a good quality of life.

We have a good starting point. Norway is already a good country to live in. People have opportunities to develop, contribute and create value. Trust in society is high, and social and geographical differences are small. Our welfare state makes knowledge, healthcare and assistance in various life situations available to all.

Now we are faced with new tasks. In the report on *Long-term Perspectives on the Norwegian Economy*,[1] the Government highlights three key societal challenges for the years ahead:

> *Competition for labour:* Caregiving tasks are increasing, yet the number of working-age individuals available to perform them is not keeping pace.
>
> *Need for adaptation:* Increased global tensions, climate and environmental changes, and declining petroleum activity are driving changes that underscore the need for prudent and responsible resource management.
>
> *Continued good distribution:* Little inequality and stable access to welfare services must be preserved in the face of transitions, and as many people are living longer than before.

Digitalisation is an important part of the solution to societal challenges. Digitalisation allows us to achieve higher quality public services, greater value creation and a society where everyone has opportunities, regardless of where they live or work. At the same time, we must ensure that we have sufficient control over digitalisation and that it takes place in a safe, secure and trustworthy manner. It is particularly important that technology is introduced and used with caution in relation to children and young people.

About the digitalisation strategy
This strategy charts the course for a digital Norway, with a high level of ambition and clear goals.

It describes the following prerequisites that must be in place in order for the digitalisation of society to succeed: *strengthening governance and coordination in the public sector, ensuring a secure and future-oriented digital infrastructure, bolstering security, emergency preparedness and crime prevention, ensuring appropriate and safeguarded privacy for all and securing future-oriented digital competence*.

Furthermore, the strategy describes the following priority areas where efforts must be strengthened in order to realise the full potential of digitalisation: *increasing data sharing and harnessing the opportunities in data and data-driven innovation, leveraging opportunities in artificial intelligence, speeding up the green and digital transition, promoting an adaptable and innovative business sector while maintaining trust, strengthening inclusion, and safeguarding considerations for children and young people*.

The overriding goal of the digitalisation strategy is to make Norway the most digitalised country in the world by 2030. To achieve this, the Government will:

STRENGTHENING GOVERNANCE AND COORDINATION OF THE PUBLIC SECTOR
In the run-up to 2030, the Government will implement stronger cross-sectoral governance and coordination of digitalisation, so that we can harness the immense potential we currently have. We will create strong synergies between Norwegian and European digitalisation policy. The Government is seeking a change of pace in public sector digitalisation.

We shall have a public sector that offers better, more seamless digital services to citizens and the business sector. We shall use digitalisation for de-bureaucratisation and ensure that professionals can devote more of their skills to providing good services to people. We shall introduce labour-saving technology through trust-based and participatory digitalisation.

Goal 2030: Norway shall rank first among OECD countries for public sector digitalisation. We are currently ranked fourth.[2]

ENSURING A SECURE AND FUTURE-ORIENTED DIGITAL INFRASTRUCTURE
Towards 2030, the Government will establish high-speed broadband and good mobile coverage for all, and ensure that we have robust electronic communications networks and services nationwide. We shall ensure a well-functioning shared digital ecosystem for interaction and service development in the public sector.

Goal 2030: Everyone in Norway should be offered high-speed broadband with at least 1 Gbit/s download speed. Currently, 95.1 per cent enjoy such access.[3]

BOLSTERING SECURITY, EMERGENCY PREPAREDNESS AND CRIME PREVENTION
Towards 2030, the Government will strengthen national cyber security and emergency preparedness to safeguard critical societal and fundamental national functions. To strengthen our work on national security and emergency preparedness, we will actively use digital technologies. The national capacity to combat cybercrime will also be strengthened.

Goal 2030: All government agencies have evaluated, improved or renewed their information security management systems. Currently, 80.9 per cent have done so.[4]

Goal 2030: 90 per cent of municipalities have evaluated, improved or renewed their information security management systems. Currently, 66.7 per cent have done so.[5]

ENSURING APPROPRIATE AND SAFEGUARDED PRIVACY FOR ALL

Towards 2030, the Government will safeguard privacy in all digitalisation efforts. All relevant IT solutions in the public sector shall have built-in privacy protection, and we shall ensure citizens' privacy in their interaction with the Tech Giants.

Goal 2030: We shall ensure a 20 per cent increase in citizens' confidence in the public sector's privacy protection efforts. Citizens' confidence on this issue has decreased by 12 per cent since 2010.[6]

SECURING FUTURE-ORIENTED DIGITAL COMPETENCE

By 2030, the Government wants to ensure that Norway has access to the necessary digital competence, both as a basic skill in all relevant education programmes and as specialised skills. Technology subjects will be prioritised in education. We will ensure that the public sector and the business sector have access to the necessary skills to succeed in the green and digital transition.

Goal 2030: The proportion of government agencies struggling to recruit ICT specialists has decreased by 15 per cent. Currently, 82.5 per cent of government agencies struggle to recruit ICT specialists.[7]

Goal 2030: Less than 55 per cent of enterprises report unmet ICT skills needs. Currently, this figure is 64 per cent.[8]

HARNESSING THE POWER OF ARTIFICIAL INTELLIGENCE, DATA AND DATA-DRIVEN INNOVATION

Towards 2030, the Government will establish a national infrastructure for artificial intelligence (AI), placing Norway at the vanguard of ethical and safe AI use. The business sector shall have favourable framework conditions for developing and using AI. The public sector shall utilise AI to develop better services and solve tasks more efficiently.

Goal 2030: All government agencies use AI as part of their task management. Currently, 43 per cent of them do so.[9]

Norway will also be a leader in value creation with data and in data-driven research and innovation. We will participate in the EU's data space initiatives where relevant.

Goal 2030: 60 per cent of private sector enterprises utilise data from the public sector. Currently, this share is 42 per cent.[10]

PROMOTE AN ADAPTABLE AND INNOVATIVE BUSINESS SECTOR AND ACCELERATE THE GREEN AND DIGITAL TRANSITION

In the run-up to 2030, the Government will facilitate the strengthening of the business sector's competitiveness through the innovative use of data and digitalisation. The conditions for start-up enterprises shall be favourable. We shall ensure that digitalisation and the use of data reinforce our advantages in key industries, such as health, energy, aquaculture and other maritime industries.

We shall prioritise lifelong learning offerings in areas that are necessary for the future business sector.

We shall facilitate the green and digital transformation of the business sector.

Goal 2030: Norway shall be the leading country in the Nordic region for digital innovation. Currently, Norway is below average.[11]

Goal 2030: Norwegian enterprises shall become the best in the Nordic region at using new technologies such as cloud services, IoT, big data analysis and AI. Currently, Norwegian enterprises are below the Nordic average.[12]

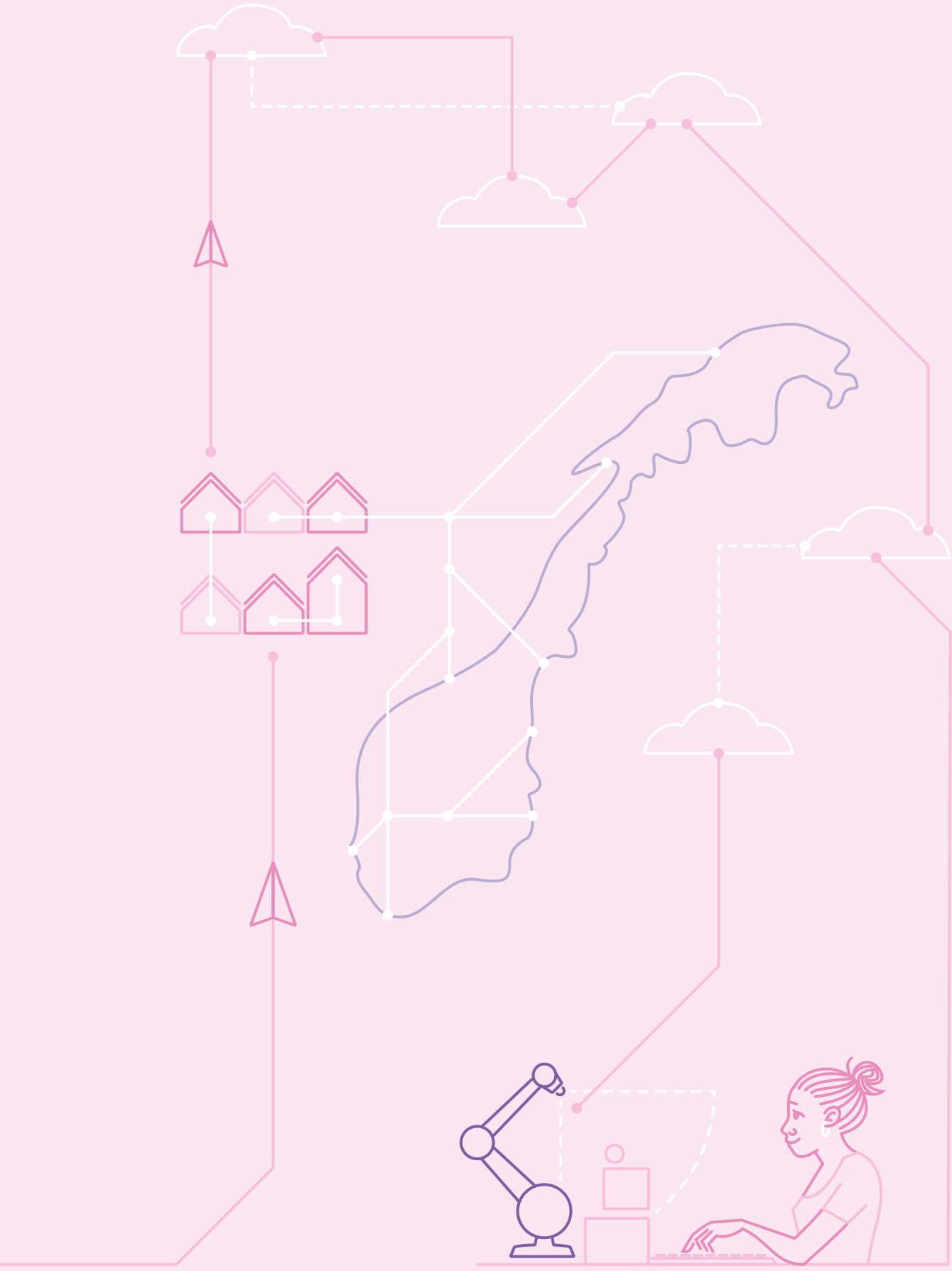
Goal 2030: The amount of electrical and electronic waste per person shall be reduced by 32 per cent. Currently, this figure stands at 26.8 kilos per person.[13]

MAINTAINING TRUST, STRENGTHENING INCLUSION, AND SAFEGUARDING CONSIDERATIONS FOR CHILDREN AND YOUNG PEOPLE

Towards 2030, the Government will ensure that everyone can take part in digitalisation. We will strengthen our efforts to increase the digital competence of those groups experiencing digital barriers and digital exclusion. We shall make sure that everyone is offered an electronic identity. We shall strengthen the population's resilience to digital disinformation. Children and young people shall be ensured a safe digital upbringing. We shall ensure a good digital-analogue balance in kindergartens, schools and in the leisure time of children and young people.

Goal 2030: The number of persons over the age of 12 in Norway who have a high-security eID shall be 5 million. Currently, this figure is 4.5 million.[14]

Goal 2030: 95 per cent of the population should have basic digital skills, and everyone should be offered the opportunity to develop such skills. Currently, 86 per cent of the population has digital skills.[15]



2

Norway's digital status

In recent years, Norway has undergone an extensive digital transformation. In practice, we currently live in a thoroughly digitalised society. Norway has a well-developed communications infrastructure, and most people have access to high-speed broadband.

The OECD Digital Government Index[16] assesses the efforts made by governments to establish the foundations necessary for a digital transformation of the public sector. In 2023, Norway ranked fourth among OECD countries. Norway is at the forefront in many areas, including as user-oriented digitalisation[17] Norway also ranks highly in various international assessments, though it is not at the top.[18]

There are still many areas with significant potential to better leverage opportunities for gains in digitalisation. The report *Rikets digitale tilstand* [Digital State of the Realm] indicates that we have not made sufficient progress in implementing the public sector digitalisation strategy for 2019-2025. Several other reports and investigations indicate that we need to renew and streamline existing solutions. We must also become better at harnessing the potential of data and reaping the benefits of digitalisation initiatives. This is supported by findings in the *National Audit Office of Norway's investigation of the authorities' facilitation of the sharing and reuse of data in public administration*.[19]

A number of studies show that the development of AI, especially generative AI, has immense potential for value creation. Both the public sector and the business sector must become even better at leveraging the potential of enabling technologies such as AI and 5G. A 2023 investigation by the National Audit Office of Norway[20] shows that government and state-owned enterprises are exploring the opportunities offered by AI to improve services and streamline work processes. Many organisations have launched AI projects, but only a few have reached the stage where their solutions are being put into practice.

Nor have we made as much progress as we would have liked in our work on seamless, user-oriented services, even though surveys[21] indicate that increasing cross-sectoral collaboration is yielding results. For the digitalisation of the public sector to succeed, we need a high level of trust in the public sector. Both *IT i praksis for 2023*[22] [IT in practice for 2023] and *the Norwegian Citizen Survey for 2024*[23] indicate that trust in the public sector is under pressure. This trend must be reversed.

If Norway is to succeed with the digital transition, we are entirely dependent on the business sector succeeding. In Norway, more than 90 per cent of enterprises are small compared to most countries in Europe. It is therefore challenging for them to keep up with the digital transition. This may be due to a lack of skills and access to risk-mitigating financing. Effective collaboration between the public and private sectors and favourable framework conditions are needed to succeed in the digital transition of the business sector in the years ahead.

Everyone should have the opportunity to participate in the digital society. New inequalities in society may arise if parts of the population do not have access to digital services, are unable to participate digitally or are digitally vulnerable. This applies to around 850,000 people today. We must therefore combat digital exclusion.

Children and young people are growing up in a society where digital media plays a major role. Digitalisation can challenge their growth and learning environment. It is particularly important to safeguard children's privacy and consumer protection, and the right to protection from harmful content. It is also important to prevent online abuse and be aware of the effects that the use of digital media can have on the mental health of children and young people.

Finally, both rapid technological developments and the geopolitical situation are challenging our security and emergency preparedness. The Norwegian National Security Authority's report *Nasjonalt digitalt risikobilde 2023* [National Digital Risk Situation 2023][24] clearly describes an uncertain and unpredictable landscape, where advanced technologies introduce new threats and vulnerabilities. We shall safeguard and secure Norway amidst digital development.

OECD ANALYSES ON DIGITALISATION IN NORWAY

On behalf of the Ministry of Digitalisation and Public Governance, the OECD has conducted analyses of digitalisation in the public sector and in society at large, and has issued recommendations for strengthening such efforts.

Box 2.1 **OECD assessment of digitalisation in the public sector[25]**

The OECD recommends strengthening the governance and coordination of digitalisation policy, ensuring more a coherent prioritisation of investments in digitalisation initiatives, and strengthening work on digitalisation-friendly legislation. It points to the need for sustainable governance and funding models for national joint solutions and recognises the potential for greater sharing and use of public data. Furthermore, it recommends a more strategic and coordinated approach to the use of AI in the public sector. It is also important to swiftly implement the EU's AI Act into Norwegian law. Finally, the OECD believes that we should focus even more on quality of use and user involvement in the development of public digital services.

Box 2.2 **OECD assessment of digitalisation in society[26]**

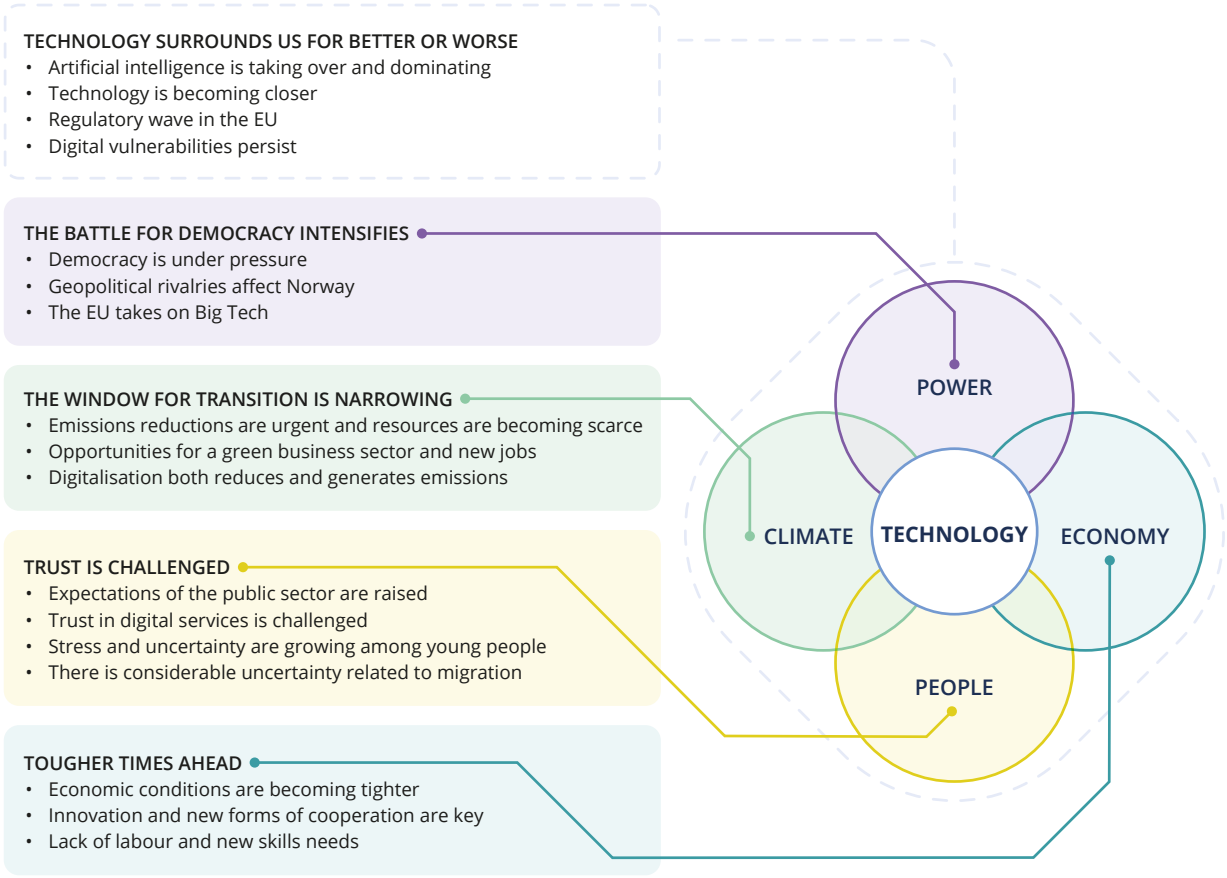
The OECD recommends that Norway improve its ability to adopt new technologies and develop digital competence to increase innovation and competitiveness. The digitalisation of small and medium-sized enterprises must be strengthened. Attention must be given to ensuring that digital competence is developed among both current and future employees. Further investment is needed in digital innovation, access to venture capital and measures to support the emergence of digital start-ups, particularly in terms of scalability. The OECD recommends a better facilitation of the sharing of data both within the business sector and between the public and private sectors. Households and enterprises should be ensured access to high-speed broadband, including in more sparsely populated areas. Targeted efforts must also be made to include groups that experience digital barriers and digital exclusion. For Norway to remain at the cutting edge, the OECD believes that digitalisation policy must be developed and implemented in a flexible and coordinated manner.

The OECD's analyses and recommendations correspond well with the rest of the knowledge base. Studies on digitalisation conducted by, among others, Statistics Norway, the Norwegian Agency for Public and Financial Management and the Norwegian Digitalisation Agency, paint a similar picture.

DRIVERS AND TRENDS AFFECTING DIGITALISATION

Drivers in society such as technological development, climate change, migration, pandemics, geopolitical security and other factors create challenges and uncertainty. These factors impact the digitalisation of society. Identifying drivers helps us to equip ourselves for the future, even if developments take unexpected turns. The Norwegian Digitalisation Agency and the Norwegian Board of Technology have described the drivers and technological trends that may affect Norwegian society towards 2030.[27]

Figure 2.1 **Drivers and trends towards 2030**

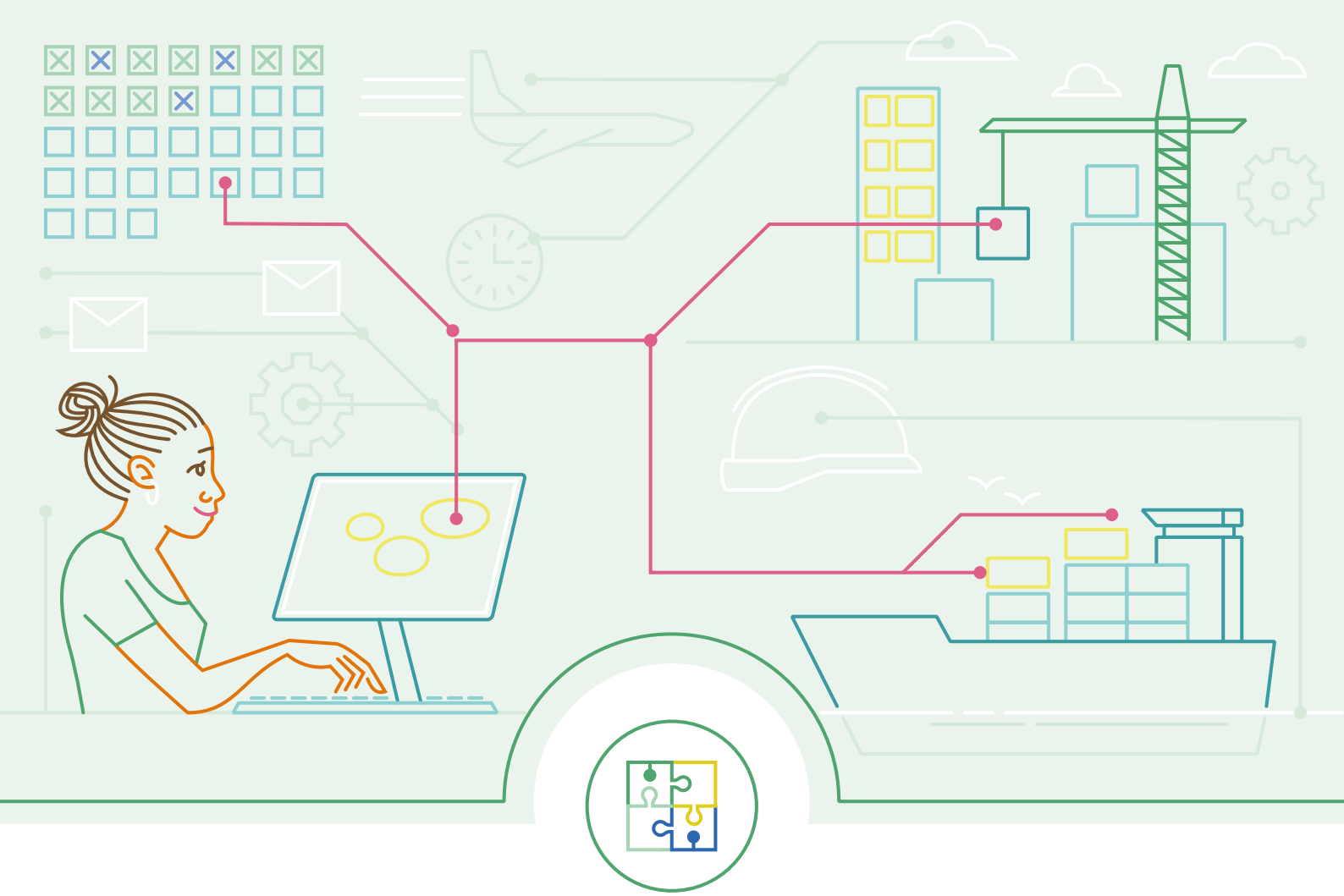


The drivers and trends are changing rapidly, with new developments emerging. The rapid pace of change means that we need to monitor societal developments closely. The OECD recommends that all countries work on insights regarding the future. The Government has therefore established a digitalisation forum where developments in trends and society in general are discussed annually, including with the social partners. In addition, the public administration must develop capacity and skills in order to gain insight into important developments and trends.

3

We shall strengthen the pre-requisites for digitalisation

Some prerequisites need to be in place in order to succeed with the digitalisation of our society. These form the foundation for digital development. With a solid foundation in place, we will be better positioned to accelerate our efforts in priority areas moving forward.



3.1 Strengthening governance and coordination in the public sector

Goals

In the run-up to 2030, the Government will ensure stronger cross-sectoral governance and coordination of digitalisation, so that we can harness the immense potential we currently have. We will create strong synergies between Norwegian and European digitalisation policy. The Government is seeking a change of pace in public sector digitalisation.

We shall have a public sector that offers better, more seamless digital services to citizens and the business sector. We shall use digitalisation for de-bureaucratisation and ensure that professionals can devote more of their skills to providing good services to people. We shall introduce labour-saving technology through trust-based and participatory digitalisation.

3.1.1 Strengthened governance of digitalisation policy

STATUS

Several societal challenges must be solved across sectors and administrative levels. Digitalisation is a tool for solving these challenges. In order for citizens and the business sector to experience seamless and comprehensive digital services, the entire public sector, irrespective of whether they are central or local government agencies, must cooperate to develop the services.

To make better use of the opportunities offered by new technologies and digitalisation, it is therefore necessary to consider how to manage and coordinate digitalisation across sectors and administrative levels. It is also necessary to enhance collaboration between the public and private sectors. In January 2024, the Government established the Ministry of Digitalisation and Public Governance. Among other things, the Ministry has been assigned primary responsibility for developing and coordinating digitalisation policy that encompasses both the private and public sectors, and will be a driving force for developing new public digital solutions. Extensive collaboration with additional actors is needed to succeed in this effort.

The Norwegian Association of Local and Regional Authorities is the Government's partner in digitalisation efforts in the public sector and is responsible for appointing municipal sector representatives to national councils, committees and digitalisation projects. It is important that the association coordinates the municipal sector's digitalisation efforts in relation to the central government and business sector.

According to the Digitalisation Circular[28], government agencies are to follow principles for coordination with and involvement of the municipal sector in national digitalisation efforts that affect the municipal sector. These principles are equality and influence, representativeness and continuous involvement.

A prerequisite for seamless and comprehensive services across central and local government is digital maturity from all parties. Municipalities vary in terms of the progress of their digitalisation efforts, and a lack of skills and capacity increases the risk of smaller municipalities being marginalised from the digital community.[29]

Box 3.1 **KS digitale fellestjenester AS and Novari IKS**

KS digitale fellestjenester AS [Norwegian Association of Local and Regional Authorities' Joint Digital Solutions] (KS Digital) was established in the autumn of 2023 and develops, operates and manages joint digital services for the municipalities and county authorities. KS Digital will assist the Norwegian Association of Local and Regional Authorities in meeting its members' digitalisation needs and will contribute to improved efficacy. Several of the services have been developed by KS Digital in collaboration with central government actors in order to realise seamless services. *Novari IKS* is an intermunicipal company that manages and further develops the county authorities' shared IT systems within upper secondary education and training, transport and technology.

Collaboration between the public and private sectors is important for making the most of our resources. The programme *digital samhandling offentlig privat (DSOP)*[30] [Public–Private Digital Cooperation (PPDC)] is an example of successful collaboration.

Box 3.2 **Public–Private Digital Cooperation**

The Norwegian Tax Administration, the Brønnøysund Register Centre, the Norwegian Digitalisation Agency, the Norwegian Labour and Welfare Administration, the Police, the Norwegian Mapping Authority and the financial industry are collaborating on the digitalisation of key societal processes through the PPDC programme.

This collaboration is based on a portfolio approach where the PPDC programme designs project initiatives that balance efforts and benefits for all parties involved. The programme assumes that the social partners will participate in all the projects and that they will contribute both during the various project phases and to the establishment of good operating and management routines.

Legislation determines the framework for digitalisation. Therefore, it is important to assess the legislation early on in the process of digitalisation initiatives. The legislation is intended to safeguard fundamental rights, including the right to privacy, freedom of expression and non-discrimination. Challenges in this domain include that technological development is outpacing legislative efforts and that the legislation is not technology-neutral or fails to address emerging needs. Furthermore, doubts may arise as to the scope of action provided by the legislation.

Digitalisation measures may necessitate a review of whether the state of the law must or should be changed. In addition, it is always necessary to consider how fundamental rights can be safeguarded when assessing what should be digitalised, what technology should be used, and whether the gap between existing and necessary legislation requires further legislative development. The National Audit Office of Norway has pointed out that although the public sector already shares data, there is significant potential for greater sharing. Increased data sharing requires, among other things, that legal issues are clarified and that privacy is safeguarded.[31]

CHARTING THE COURSE TOWARDS 2030

In order to strengthen the coordinating role of the Ministry of Digitalisation and Public Governance, the Government will further develop existing digitalisation policy instruments while also developing new instruments. Several actors and policy instruments can be included in this work, including the Norwegian Digitalisation Agency, SKATE (management and coordination of services in e-government), Stimulab, *medfinansieringsordningen* [the Co-Financing Mechanism], the Digitalisation Circular and other legislation. Important steps in the coordination

also include developing common standards and architectures, and contributing to increased use of joint solutions. Digitalisation also increases the need to safeguard cross-cutting considerations and investments across sectors, which requires the establishment of enabling mechanisms.

The Government will ensure a comprehensive and long-term prioritisation of digitalisation initiatives in the public sector. This prioritisation will be based on a comprehensive overview of digitalisation initiatives in the sectors, provide predictability and chart the course. It must be based on professional recommendations and consistent and transparent criteria, and it must have a multi-year perspective. The prioritisation is intended to ensure that the funds are allocated to the areas with the greatest need and that provide the greatest benefit to society.

To help ensure that even more beneficial digitalisation initiatives are implemented, the Government will strengthen the Co-Financing Mechanism. This scheme is a well-established and unbureaucratic policy instrument aimed at realising socio-economically beneficial measures that would otherwise not have been implemented.

When government agencies collaborate on digitalisation initiatives, it is challenging to identify models for cost-sharing and benefit calculation, including incentive mechanisms for working across sectors and administrative levels. Actors who make investments are not always the ones who reap the benefits. For instance, data sharing and solutions within the public sector often incur costs for the solution developer, while the benefits are enjoyed by others. One measure to meet this challenge is to establish good models for cost-sharing and benefit realisation in cross-cutting digitalisation initiatives. The Norwegian Agency for Public and Financial Management has therefore been commissioned to map various models for cost-sharing across sectors and administrative levels, as well as experiences with the models.[32]

Together with its members, the Norwegian Association of Local and Regional Authorities has established a number of councils and committees to help coordinate and harmonise local government digitalisation efforts. Strategic coordination currently takes place through a joint governance structure for digitalisation.[33] The Norwegian Association of Local and Regional Authorities' tasks will be solved in close collaboration with *regional digitalisation networks*. These networks are owned and managed by the municipalities and play an important role in contributing to the development of skills, the sharing of experience and the dissemination of joint solutions. The digitalisation networks also play a role in the introduction of national joint solutions and services for use in local government. Models should be established that contribute to an increased implementation of digitalisation in local government. The digitalisation networks play an important role in this effort.

Most municipalities actively engage in ICT projects, although some municipalities have lower levels of activity.[34] The Government wants to prevent excessive digital inequalities between municipalities. Better collaboration on digitalisation across sectors and administrative levels is necessary to ensure efficient resource utilisation and better services. Therefore, the Government will strengthen its collaboration with the Norwegian Association of Local and Regional Authorities on digitalisation across sectors and administrative levels.

PPDC has helped us realise major benefits for citizens, the business sector and the public sector through collaboration and interaction. One example is the consent-based loan application process. The Government will identify new areas for collaboration on digitalisation between the public, private and voluntary sectors.

The Government will strengthen its work on digitalisation-friendly legislation. In order to develop good digital services, we need to facilitate interdisciplinary collaboration from the outset, so that services and legislation are developed simultaneously.[35] Development work must take place at the intersection of language, law and technology. The legislation must be designed so that the digitalisation measures can be implemented technically, while digitalisation measures must simultaneously comply with the legislation. This interaction is necessary to strengthen the work on digitalisation-friendly legislation and clear language. The Norwegian Resource Centre for Sharing and Use of Data under the Norwegian Digitalisation Agency is a key interdisciplinary environment for work on digitalisation-friendly legislation. To be able to assist all sectors with the development of digitalisation-friendly legislation, the capacity of the resource centre should be increased.

THE GOVERNMENT WILL

- Strengthen the coordination and implementation of digitalisation initiatives across sectors
- Ensure a comprehensive and long-term prioritisation of digitalisation initiatives in the public sector
- Strengthen the Co-Financing Mechanism for socio-economically beneficial central government measures
- Identify new areas for collaboration on digitalisation between the public and private sectors
- Further develop the collaboration with the Norwegian Association of Local and Regional Authorities on digitalisation in the public sector
- Establish legislative development on digitalisation, data sharing and AI
- Strengthen efforts on digitalisation-friendly legislation and clear legal text

3.1.2 Create synergies between Norwegian and European digitalisation policy

STATUS

The EU has an ambitious digitalisation policy based on the overarching Digital Decade strategy.[36] Legislation, funding, and skills development through programs are important policy instruments for achieving the goals of the strategy. In addition, a great deal of sectoral European legislation is being developed that guides and supports digitalisation in the various sectors of society. In a challenging geopolitical context, the EU wants to be a global actor in the field of technology. The EU is challenging the large global technology companies through legislation in a manner that individual countries like Norway cannot.

Many of the EU's digitalisation policies affect Norway. Most of the legislation becomes Norwegian law via the EEA Agreement, and Norway participates in several EU programmes. The DIGITAL programme represents a concerted effort to enhance the competitiveness of European businesses, ensure better and more efficient solutions for the public sector, lay the foundation for a green transition and strengthen Europe's cyber security and sovereignty. The strategy for Norway's participation in DIGITAL[37] sets out goals and key priorities for Norway's participation in the programme, as well as specific focus areas to ensure that we maximise the benefits of our participation. Other EU programmes also support the digitalisation ambitions, such as the EU's research and innovation framework programme, Horizon Europe.

We are also working closely with our Nordic-Baltic neighbours on digitalisation, particularly within the framework of the Nordic Council of Ministers.[38] The Nordic Council of Ministers promotes joint Nordic solutions in areas where the Nordic countries can achieve better results by working together than by solving tasks separately. The Nordic cooperation also allows our countries to have a united voice in relation to the EU.

CHARTING THE COURSE TOWARDS 2030

It is important to create strong synergies between Norwegian and European digitalisation policy. Implementation of legislation from, and cooperation with, the EU can help to develop Norwegian digitalisation policy. For instance, the EU has in recent years adopted legislation that facilitates data sharing. Implementing such legislation into Norwegian law can help us achieve Norwegian policy goals of increased value creation using data.

Through the DIGITAL programme, Norway can, among other things, gain access to infrastructure and expertise that is useful for Norwegian actors. There is potential to include more Norwegian actors in the DIGITAL programme.

EEA cooperation requires continuous updates to the EEA Agreement with relevant EU legislation. *Utvalget for utredning av erfaringer med EØS-avtalen* [Committee for the Assessment of Experiences with the EEA Agreement][39] believes it is a significant challenge that the EEA backlog has grown over the past decade, and that Norway

must help to reduce the backlog. As part of the work to reduce the backlog, the Committee believes that Norway should look at the possibility of standardising and thus streamlining the work on EEA adaptations.

Close monitoring of legislative developments and policies in the EU helps ensure that we are better prepared for legal changes that will also apply in Norway. A more proactive and coordinated approach to work in the EU can also give us the opportunity to influence legislative and policy development. The Government will monitor legislative developments in the EU and implement adopted EEA-relevant EU legislation quickly, among other things to ensure the Norwegian business sector has the same competitive conditions as the rest of Europe.

Table 3.1 **Key EU digitalisation legislation***

Connectivity/security etc.	**Data/artificial intelligence**	**Platform regulation**
Cyber Competence Centre and Network of National coordination Centres (EU) 2021/887	Data Governance Act (EU) 2022/868	Regulation on addressing the dissemination of terrorist content online (EU) 2021/784
Roaming Regulation (EU) 2022/612	EU - EU Data Privacy Framework (EU) 2023/1795	Regulation laying down rules to prevent and combat child sexual abuse
NIS2 Directive (EU) 2023/2555	Regulation on precedural rules relating to the enforcement of GDPR	Digital Markets Act (EU) 2022/1925
EU Secure onnectivity Programme - IRIS2 (EU) 2023/588	Data Act (EU) 2023/2854	Digital Services Act 2022/2065
European Chips Act (EU) 2023/1781	Artificial Intelligence Act	Common Charger Directive (EU) 2020/2380
Cyber Resilience Act	Interoperable Europe Act (EU) 2024/903	Regulation on the temporary derogation from directive 2002/58 – conbating online Child Seual Abuse (EU) 2024/1307
Regulation on electronic Identification and Trust Serviced (eIDAS 2.0) (EU) 2024/1183	Open Data Directive (EU) 2019/1024	Regulation on the transparency and targeting of political advertising (EU) 2024/900
Proposal for an ePrivacy Regulation	Regulation on the free flow of non-personal data (EU) 2018/1807	Regulation on Single Digital Gateway (EU) 2018/1724

*The various pieces of legislation are at different stages in the EU legislative process and in their implementation into Norwegian law.

THE GOVERNMENT WILL

- Actively participate in the design of the EU's future long-term digitalisation programmes
- Reduce the backlog in the implementation of adopted EEA-relevant EU legislation on digitalisation into Norwegian law
- Conduct a comprehensive assessment of Norway's participation in the EU's future long-term programmes

3.1.3 A coordinated and innovative public sector for citizens and the business sector

STATUS

Overall, citizens are satisfied with both central and local government services; however, average satisfaction has declined since 2017.[40] Although there have not been major changes from year to year, satisfaction in 2023 reached its lowest level since 2010. Users often experience that the provision of services is fragmented.[41] Several government agencies are therefore working purposefully to create coherence in the provision of services, including through the work on seamless services within the seven selected life events.[42]

By cooperating across sectors, administrative levels and industries, we can create seamless services. The principles[43] that have been established for collaboration between the central and local government on digitalisation have contributed to improved collaboration and more joint projects. However, many of these projects involve one specialised central government sector in collaboration with local government. One example of a cross-cutting collaboration is DigiUng.

Box 3.3 **DigiUng and Ung.no**

Through the DigiUng collaboration, public services and information for young people are developed and gathered in one place – ung.no. The Government has decided that ung.no will be the central government's primary channel for digital information, dialogue and digital services for children and young people. The local government sector also has digital services that are part of DigiUng. Ung.no is a good example of collaboration across sectors and administrative levels. It is also a good example of digitalisation to reach a specific target group in society.

Ung.no is a user-friendly gateway to quality-assured information, guidance and support services run by the public administration across sectors. It also offers a question-and-answer service where young people can ask questions. The target group is young people ages 13 to 20. In 2023, ung.no had 21,926,392 visits and around 110,000 enquiries to the Q&A service. This clearly shows that ung.no has a broad reach and is an important tool for reaching out to children and young people.

Digitalisation offers great opportunities to develop health and care services for the benefit of all. The goal is for both citizens and healthcare professionals to have secure access to relevant health information when they need it. The main responsibility for digitalisation lies with the actors in the health and care sector. Digital interaction, enhanced comprehensive information management and increased standardisation will ensure that up-to-date health information is secure, of good quality and easily accessible. The Government's strategy for digitalisation in health and care services is presented in Report to the Storting (white paper) 9 (2023-2024) *Nasjonal helse- og samhandlingsplan* [National Health and Cooperation Plan].

To be able to introduce digital services and to automate services, we depend on citizens' trust in the public administration. A key success factor in leveraging new technologies is the ability of organisations to involve employees and employee representatives. The introduction of new technology may require changes in working methods and new skills requirements. The Trust Reform[44] is closely linked to the Government's ambition to leverage technology and digitalise the public sector. The goal is to ensure greater well-being and better services to citizens and the business sector. If people find that services are of high quality, they will have greater trust in the public sector. In order to reap the benefits, free up time in primary services and maintain people's trust in the public sector, we need to put digitalisation on the agenda in the collaboration of the parties, both locally and centrally.

CHARTING THE COURSE TOWARDS 2030

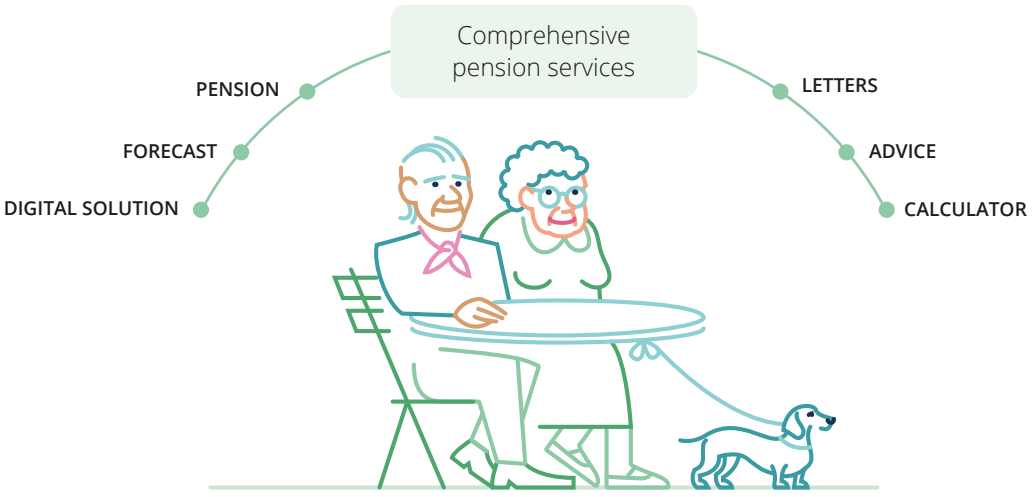
We want to make it easier for citizens, the business sector and voluntary organisations to interact with the public sector. They should experience seamless and comprehensive digital services, irrespective of the provider. Actors must work together if we are to achieve this ambition. Services should inspire trust, be universally designed and be more adapted to individual needs. Services for children and young people should be age-appropriate. Employee representatives in government agencies shall be a significant contributor to the development of services.

Box 3.4 **Easier interaction with the public sector – what is my pension?**[45]

Through the pension reform, each citizen has been given flexibility, but at the same time a responsibility to inform themselves about pensions and make independent choices.

In order for citizens to be able to make good pension choices, both for themselves and for society, they need to have access to good information about their own pension. They must also be able to understand and use the information. In today's pension landscape, people have to relate to multiple information channels, different processes and different pension providers to gain an overall understanding of their pension. This can make it difficult to gain an overview and insight into the pension choices they face.

Digitalisation, in conjunction with new technology and new methods, can form the basis for seamless and comprehensive pension services. This requires an overarching strategy for how information about pensions is to be disseminated, as well as a strengthening of the collaboration between pension providers and other stakeholders.



Citizens should receive accurate and unambiguous information about their rights, obligations and opportunities.[46] The Norwegian public sector currently has many websites, portals and digital services aimed at users. The myriad of communication channels makes it difficult for people to locate, understand and use information from the public sector. Experience from working with the life event "Seriously ill child" shows that families with seriously ill children spend an average of 19 hours a week navigating the vast amount of information and coordinating services from the public sector.[47]

Work on seamless services within defined life events[48] shall be continued. Lessons learnt from the work that has been done are useful in the coordination and development of more seamless services.[49] An arena for exploring solutions to regulatory challenges and other barriers to collaboration may be a useful tool.

The voluntary sector is a pillar of Norwegian society and plays an important role in all arenas of society. The Government wants voluntary organisations to spend as much time as possible on generating activity and as little time as possible on paperwork. Therefore, we are continuing our efforts in the life event "Starting and managing a voluntary organisation". The aim of this work is to facilitate the sharing and reuse of data in central government grant management and realise the *once-only* principle. Voluntary organisations should not have to submit the same information to the central government multiple times.

In collaboration with the Norwegian Association of Local and Regional Authorities, the Government will investigate a single gateway to general and personalised information and to digital public services. This may include access to your own personal data, such as relevant health information. Such a single gateway will enable users to quickly and easily fulfil their obligations and apply for and receive benefits. The solution can also include digital personal assistants that provide the user with support during the process. AI may be a tool for developing such assistants.

The EU Regulation Establishing a Single Digital Gateway (SDG)[50] aims to make it easier and more appealing for European citizens and businesses to establish themselves in Norway, and for Norwegian citizens and businesses to establish themselves in the EU. This will be achieved by making 21 services available digitally across national borders in the EU. In addition, the YourEurope portal[51] will help EU citizens navigate the public systems in other EU countries, thereby making it easier for them to exercise their rights and obligations. The SDG should be understood in the context of the initiative to investigate a single gateway to general and personalised information and to digital public services.

Digitalisation must be implemented so that the public sector can fulfil its obligations under the Language Act. The public sector is to communicate clearly and accurately with citizens and use a clear Norwegian or Sámi language. When the public sector develops and utilises new ICT tools and services, the work on language must be included from an early stage in the planning process.

New technology and digitalisation can be labour-saving and contribute to reduced growth in labour needs for the entire public sector. This can help increase productivity in the public sector. Examples of labour-saving technology include welfare technology and the robotisation of administrative functions. The *Nasjonal helse- og samhandlingsplan*[52] [National Health and Cooperation Plan] states that implications for personnel must be investigated as part of the decision-making basis for all measures within the Ministry of Health and Care Services' sectoral responsibility. The Government will consider whether the investigation of implications for personnel should be a requirement as part of the decision-making basis for all public digitalisation initiatives.

Both citizens and personnel should have secure access to relevant health information when they need it. Technology and digital interaction solutions should help maintain or improve the quality of treatment for patients and users, and facilitate participation. In the National Health and Cooperation Plan, the Government has clarified the roles and responsibilities of relevant actors for digitalisation in the health and care sector. This will help ensure that the overall resources are utilised effectively and efficiently. New national needs require a faster transition from planning to trialling and introduction of digital solutions. Proposed solutions should be tested early on to allow for course adjustments along the way and enable quicker implementation. The health services must develop and adopt digital solutions to free up time for patient treatment, research, education and patient training, without jeopardising quality and patient safety.

AI has the potential to change the roles within the public sector and the relationship between government agencies and users (citizens, the business sector and the voluntary sector). How this will develop and what implications the use of AI will have over time is difficult to predict today. This is why it must be trialled in practice. AI must be used in an ethical and responsible manner, and in line with relevant legislation to ensure that its use is fair, transparent and in accordance with how we want to develop the public sector. The Government will monitor developments and continuously assess measures and the need for more regulation.

Box 3.5 **Areas where the public sector can benefit from AI**

- *Automation of routine tasks*
  AI can carry out repetitive tasks to increase efficiency and free up time for personnel, such as transcribing, writing meeting minutes, subtitling and interpreting.
- *Decision-making support*
  AI is capable of analysing vast amounts of data, offering insights that help decision-makers make more informed and faster decisions. An example from the health and care sector is the more rapid diagnosis of bone fractures.
- *Monitoring and analysis in specific areas*
  AI can analyse large amounts of data to detect patterns, deviations or risks, for example in traffic, the environment and the economy.
- *Resource allocation*
  AI can predict needs and thereby optimise resource use, such as planning personnel needs and improving resource allocation in hospitals and clinics.[53]
- *Brukertilpasning av tjenester og informasjon*
  [User adaptation of services and information]
  AI can gather information from multiple sources. This can lead to a better user experience and more efficient services, such as user-adapted information in seamless services or life events.[54]

Stimulab is a scheme that stimulates the development of user-oriented solutions involving technology. The Government will further develop schemes that facilitate innovation in public services.

The Norwegian Agency for Public and Financial Management and the National Program for Supplier Development[55] assist government agencies in carrying out innovative procurements. Innovative procurement should be used as a tool to promote innovation in digitalisation and the use of AI in the public sector.

The Government wants to reduce the business sector's costs associated with imposed regulations and the completion of public forms by NOK 11 billion by 2025. Such cost reductions can be achieved by amending acts and regulations or by making it easier for the business sector to fulfil current legislation, for example by further developing digital reporting.

Many enterprises find it difficult to navigate the business-oriented policy instrument system. Therefore, the Government has initiated the development of the *Én vei inn* [One-Stop-Shop] solution, which is a single digital gateway where enterprises can quickly receive clarification and guidance for further interaction with the policy instrument system. Innovation Norway is leading this development in close collaboration with other policy instrument actors.

THE GOVERNMENT WILL

- Continue the work on life events and strengthen the work on seamless services, in collaboration with the Norwegian Association of Local and Regional Authorities
- Investigate a single digital gateway for citizens and other users to information and digital public services
- Establish a test arena for exploring regulatory and technological challenges in the work with seamless services
- Consider whether the investigation of implications for personnel should be part of the decision-making basis for all public digitalisation initiatives
- Further develop policy instruments for digitalisation and innovation in the public sector
- Increase the share of innovative procurements in the area of digitalisation and the use of AI in the public sector
- Continue efforts to reduce the costs to the business sector associated with imposed regulations and the completion of public forms
- Further develop the One-Stop-Shop digital solution, which gives the business sector a single gateway to the policy instrument system
- Continue and strengthen the work on simplification for the voluntary sector

3.2 Ensuring a secure and future-oriented digital infrastructure

Goals

Towards 2030, the Government will establish high-speed broadband and good mobile coverage for all, and ensure that we have robust electronic communications networks and services nationwide.

We shall ensure a well-functioning shared digital ecosystem for interaction and service development in the public sector.

3.2.1 A nationwide, secure, future-oriented and accessible digital foundation

3.2.1.1 Greater coverage, capacity and competition

STATUS

Data centres and mobile and broadband networks (electronic communications networks) make up Norway's digital foundation and are a prerequisite for further

digitalisation of society. The mobile and broadband networks in Norway already have good coverage. As society is becoming increasingly dependent on the internet, it is necessary to continuously improve the digital foundation.

New services and applications based on fibre optics and 5G mobile technology are rapidly being established in densely populated areas. They provide the basis for new ways of solving tasks and increase value creation and productivity. It is important that such services are also made available in more sparsely populated areas. 100 per cent coverage is first and foremost important for each individual citizen to be able to participate fully in society, but it is also important for the development of the business sector and for the public sector to maximise the benefits of digitalisation.

Access to high-speed mobile networks is important not only where people live, but also where people work and travel. Greater coverage of mobile networks is important for the country's emergency preparedness and security.

CHARTING THE COURSE TOWARDS 2030

The Government will continue to pursue a market-based and technology-neutral policy for the development of mobile and broadband networks, and will contribute with targeted central government measures in areas where there is no commercial basis for development.

The Government's goal is for all households and enterprises to be offered broadband with a download speed of at least 100 megabits per second by the end of 2025 and at least 1 gigabit per second by the end of 2030.

To cultivate a competitive landscape, freedom of choice and to enable innovation, not least in sparsely populated areas, the Government will continue to pursue the goal of at least three fully-fledged mobile networks that can compete in both the business and consumer markets.

The Government aims to significantly improve mobile coverage (geographical coverage) in the areas of the country where the need is greatest, particularly along key transportation routes.

The Government's goal is for all households in Norway to have access to high-speed mobile networks.

Both mobile services and many other digital services are dependent on available frequency resources. These must be utilised and managed effectively to support the digitalisation of Norway.

THE GOVERNMENT WILL

- Provide high-speed broadband to households and businesses through targeted grants in areas without a commercial basis for development
- Further facilitate the development and expansion of mobile networks where people live, work and travel
- Ensure an efficient management of frequency resources that, through timely allocation, cultivate an innovation and business development landscape which takes into account societal needs

3.2.1.2 Strengthened security and emergency preparedness in the digital foundation

STATUS

The digital foundation is increasingly responsible for carrying greater values and supporting critical services for Norwegian society. At the same time, the security situation in Europe has intensified, stresses from extreme weather and natural events have put electronic communications networks to the test, and the need for emergency communication has become even more important.

In sparsely populated areas, the networks are more vulnerable than in densely populated areas, which may result in more frequent and extended network outages. Because almost all services in society are dependent on electronic communication, such outages can have major consequences. Emergency communication is also dependent on functioning electronic communication networks.

In light of the new security policy situation, the Government is using grant funds to strengthen security and emergency preparedness in offshore e-infrastructure which underpins Norwegian oil and gas production. In addition, we have upgraded the priority subscription solution to 4G and 5G, and strengthened both the fibre-optic connection to Svalbard and the redundant communication solution with the archipelago.

CHARTING THE COURSE TOWARDS 2030

The digital foundation must become more robust, and redundancy and diversity must be further developed and strengthened so that communication services can be delivered in times of peace, crisis and war.

A prerequisite for such a service provision is greater variety – both in the form of multiple different networks, such as mobile networks, fixed networks and satellite systems, and through increased diversity and redundancy in the individual networks.

The Government aims to ensure that:

- More physically separate routes are utilised by all providers of transmission networks to towns in Norway, and that such providers be required to offer redundancy in their own networks;
- Mobile operators, to the greatest extent possible, distribute mobile traffic over several independent transmission networks;
- Norway will establish high-capacity connections to more countries from all regions of the country, ensuring high-capacity, low-latency connections within the country;

The Norwegian Communications Authority has conducted regional risk and vulnerability analyses of the electronic communications infrastructure in Finnmark, Troms, Nordland, and Trøndelag, and the Government aims to have similar analyses performed throughout the rest of the country.

As a result of the security policy situation, the need for exercises and cross-sectoral collaboration has increased. Exercises and collaboration are crucial to strengthening security and emergency preparedness in the years to come.

To safeguard cyber security, we need robust satellite-based systems and services. Satellite systems will increasingly be used for communication in crises. Therefore, it is necessary to further develop and strengthen national capability and resilience in the satellite sector.

Interference with communications, caused by electromagnetic noise from electrical and electronic equipment, installations, illegal transmissions, and increasingly, illegal jamming, is a frequent occurrence. Therefore, it is important to work to prevent such disruptions from resulting in serious consequences.

THE GOVERNMENT WILL

- Ensure adequate national control of the part of the digital foundation that underpins critical societal functions
- Facilitate greater diversity and redundancy in the routing paths regionally, nationally and between Norway and abroad
- Enhance the security and emergency preparedness of the digital foundation in vulnerable municipalities and regions through targeted grants, and assess new measures in light of the changed security policy situation
- Conduct thorough risk and vulnerability analyses in all of the country's regions, and assess and implement relevant measures upon completion of the analyses
- Strengthen collaboration on security and emergency preparedness across sectors, especially the electronic communications, energy, defence and justice sectors
- Carry out a pilot project for cross-sectoral collaboration on restoring mobile coverage in the event of service outages
- Contribute to preventing and minimising the adverse effects of electromagnetic interference on electronic communications
- Contribute to creating more robust satellite-based systems and services, while further developing national capacity in the satellite sector at the Andøya Space Centre
- Strengthen Nordic cooperation on electronic communications

3.2.1.3 Data centres

STATUS

Data centres are a key component of the digital foundation and represent modern industrial construction. Data centres located in Norway, combined with a strong and robust national digital foundation, enable the production of critical digital services domestically rather than abroad. This will bolster national control and ensure opportunities for national autonomy. At the same time, flexibility may be appropriate. This means that while some services may be produced on international cloud platforms, data storage and service production can be seamlessly transferred to Norwegian data centres in the event of a crisis or emergency situation. Conversely, in some critical situations we may need to move parts of the data storage and service production out of Norwegian data centres to allied countries.

CHARTING THE COURSE TOWARDS 2030

The Government wants to facilitate data centres that contribute to value creation, enhanced security and safeguarding of Norwegian interests. Our goal is for data centres and data centre services to have proper security in times of peace, crisis and war. The most critical digital services will be delivered from data centres in Norway or from data centres located with our close allies. To increase the industry's national value creation and international competitiveness, the Government will take a strategic and comprehensive approach to increasing the net sustainability of Norwegian data centres.

For the sake of the Norwegian welfare state and a sustainable economy, it is crucial that we succeed with the digital and green transition. Data centres and artificial intelligence can and must play a role in efforts to meet the climate goals, and they can contribute to an efficient reduction in emissions. On the one hand, data centre services can support emission reductions in all sectors through digital solutions, such as more climate-friendly and efficient production processes and services in the business sector. On the other hand, data centres consume vast amounts of energy and lay claim to considerable space. The Government aims to increase the reuse of surplus heat from data centres in Norway and will work to make data centres more circular and resource-efficient. According to the Foundation for Scientific and Industrial Research at the Norwegian Institute of Technology (SINTEF), reusing surplus heat from data centres and other industries has the potential to free up more than 10 per cent of Norway's power production. The development and use of data centre-based services offer significant sustainability potential across various sectors. There is a need for greater awareness and a better framework to increase and document both the sustainability potential and impact. Effective social and project planning and targeted innovation and technology development are key elements going forward.

THE GOVERNMENT WILL

- Work to ensure that Norway is an attractive place for the data centre establishments that contribute to value creation
- Present a new data centre strategy

3.2.1.4 Work to ensure an open, free and safe internet

STATUS

New digital services bring new challenges. It is difficult to distinguish between truth and falsehood on the internet. Furthermore, we hand over considerable amounts of personal data when using digital services. Digital services provided over the internet can be misused to provide illegal products, services and content, and to manipulate users and spread disinformation.

The platform and data economy has bestowed considerable power on the major tech companies. The concentration of power in the hands of a few major global technology actors can pose a challenge to states and a threat to democracy and society. The intent of EU's new platform regulations, the Digital Services Act (DSA) and the Digital Market Act (DMA), is to contribute to solving a number of these problems.

Online fraud has become a major societal problem. In 2022, Norwegians were defrauded of over NOK 600 million, and in the first half of 2023, the corresponding figure exceeded NOK 400 million.[56] A large proportion of fraudsters employ social engineering, or phishing, to fraudulently obtain sensitive information using fake links and similar methods. Online fraud affects individuals financially and emotionally,

but it also has an adverse impact on the general trust in society. This can delay digitalisation and also has adverse effects on social participation, integration and value creation.

CHARTING THE COURSE TOWARDS 2030

The Government wants to help ensure that the internet is an open, secure and freely accessible societal resource, both nationally and globally. It is important that a country such as Norway, which has long democratic traditions and can represent a small-state perspective, takes greater responsibility in the further development of the internet. Norway will help to secure long-term strategic interests in global internet governance and set the agenda on issues of major significance. Our position is that the internet should remain an open and freely accessible arena, where anyone can freely give and receive information and claim ownership of their own information, and where fundamental human rights are protected. Norway is therefore a candidate for hosting the UN Internet Governance Forum (IGF) in 2025.

Swift incorporation of the DSA and DMA into the EEA Agreement and implementation of the legislative package into Norwegian law will help to ensure that end users and enterprises in Norway enjoy the same protection and rights as elsewhere in Europe, and to regulate the big tech companies.

For the Government, it is important to work to maintain trust in electronic communication services, and in the content communicated via these services. In addition, citizens need to become more resilient to fraud raising awareness about common fraud methods and learn how to stay safe online.[57]

Box 3.6 **National Expert Group against Digital Fraud**

The National Expert Group against Digital Fraud was established in the autumn of 2023, representing strengthened coordination and governance of efforts to combat digital fraud. The Expert Group consists of representatives from the private and public sectors and is initially a two-year project. The group is led by the Norwegian Communications Authority in partnership with the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime.

THE GOVERNMENT WILL

- Host the Internet Governance Forum 2025
- Implement the Digital Markets Act (DMA) and Digital Services Act (DSA) in Norwegian law
- Establish a national DSA coordinator who, together with other relevant authorities, will enforce the DSA in Norway
- Prevent digital fraud by further developing interdisciplinary collaboration and disseminating information to citizens
- Assess the proposals by the National Expert Group against Digital Fraud

3.2.2 A digital ecosystem for cooperation and service development

STATUS
The public sector must accelerate the pace of digitalisation, while tighter financial constraints compel us to rethink how we develop and manage digital services. Similar needs in the public sector must be solved jointly, based on the established shared digital ecosystem for collaboration and service development (shared digital ecosystem[58]).

Box 3.7 **Shared digital ecosystem for collaboration and service development**

A shared digital ecosystem will contribute to establishing digital collaboration capabilities across sectors and administrative levels. This will contribute to increased data sharing and greater value creation for society.
The ecosystem encompasses:

- Actors: citizens, local and central government, the voluntary sector and the private sector
- Framework conditions: organisation, governance, coordination and legislation
- Shared resources: joint solutions such as ID-porten and infrastructures, guides, standards, data and information sources

In a shared digital ecosystem, public and private enterprises cooperate to build comprehensive and seamless services. They interact, reuse joint solutions, and adhere to standards, principles and reference architectures. In this way, digitalisation becomes more sustainable. Joint solutions such as Altinn, ID-porten, the National Population Register and sector-specific solutions such as the municipal FIKS platform and Feide are important for establishing digital interaction capabilities. The shared digital ecosystem is being improved and developed in collaboration between the actors, but there is still a need for further development and new solutions. One example of this is the need to establish public sector solutions ensuring that individuals can be digitally represented by an authorised person should they require this.

The voluntary sector is a separate sector of society, with distinctive characteristics, and thus differs from both the public and private sectors. A shared digital ecosystem and various national joint solutions should be utilised in national services and solutions pertaining to the voluntary sector.

Geographic data (geodata) generates new value and is increasingly aiding both the public and private sectors in addressing societal challenges, such as climate change adaptation, natural hazard prevention, and biodiversity conservation. Access to geodata is also important for ensuring civil protection and managing crises. Despite the growing usage, there remains significant potential to derive even greater benefits from geodata. This requires an up-to-date and easily accessible geographic infrastructure. The national geographic information

infrastructure is an important part of the digital ecosystem and facilitates the collection, use and sharing of geographic information across the public and private sectors. The infrastructure consists of geodata, metadata and joint solutions. It is based on legal, administrative, technical and organisational prerequisites, such as the Geodata Act, the Geodata Regulations, the *Geovekst* [Geo-Growth] collaboration and the National Geodata Strategy.

The use of the joint solutions managed by the Norwegian Mapping Authority has increased considerably in recent years, from approximately 2 billion hits in 2011 to 18 billion hits in 2023. A growing number of public and private actors are using geodata to solve statutory tasks, deliver services and support business development.

CHARTING THE COURSE TOWARDS 2030

The public sector must accelerate the pace of digitalisation. To leverage the opportunities presented by technology and contribute to more efficient and sustainable digital development, we require a national architecture for collaboration. This architecture should describe the necessary resources for collaboration, such as joint solutions,[59] infrastructure for sharing data and standards, and standardised interfaces (APIs). A national architecture clarifies relationships and responsibilities and makes it easier to identify the need for measures.

The heightened security situation has rapidly and significantly altered the threat landscape for digital solutions. Attacks on digital solutions can lead to downtime for many public digital services. Consequences may also include the loss of sensitive personal information, financial losses and reduced trust in the public sector.

Organisations that are responsible for joint and sector-specific solutions must have framework conditions that enable them to remain relevant and secure. There is a need for governance and financing mechanisms, including cost-sharing models, which address the need for further development, management and operation of joint solutions.

Secure digital solutions are needed for the processing of unclassified critical national information. On behalf of the Ministry of Justice and Public Security, the National Security Authority has developed a concept for a secure national cloud.

When there is uncertainty about whether government agencies can utilise certain joint solutions without undergoing a procurement process, consideration should be given to making the use of these solutions mandatory. The Digitalisation Circular regulates when government agencies are required to use joint solutions. Greater collaboration between sectors and administrative levels indicates a need to investigate whether the requirements in the Digitalisation Circular should apply to the entire public sector, and whether they should therefore be laid down in acts or regulations. The Norwegian Association of Local and Regional Authorities will be involved in these efforts.

The business and voluntary sectors are currently unable to use joint solutions unless such use is part of the exercise of public authority. If the business and voluntary sectors are to be able to utilise all or part of the shared digital ecosystem in their service development and production, the consequences of facilitating such use must be investigated.

A key element of the digital ecosystem is access to electronic identification (eID). Today, almost a million people in Norway are prevented from participating digitally, partly because they are unable to obtain an eID with a high level of security. In April 2023, the Government adopted a new strategy for the use of eID in the public sector.[60] The measures in the strategy are followed up through an action plan.[61] Among other things, the action plan follows up on the EU's eIDAS Regulation.[62] The Regulation, which is EEA-relevant, has been revised and entered into force in the EU in 2024. The Regulation entails that the public sector shall take responsibility for ensuring that everyone has the opportunity to obtain an eID with a high level of security and offer it to users by way of a digital wallet.

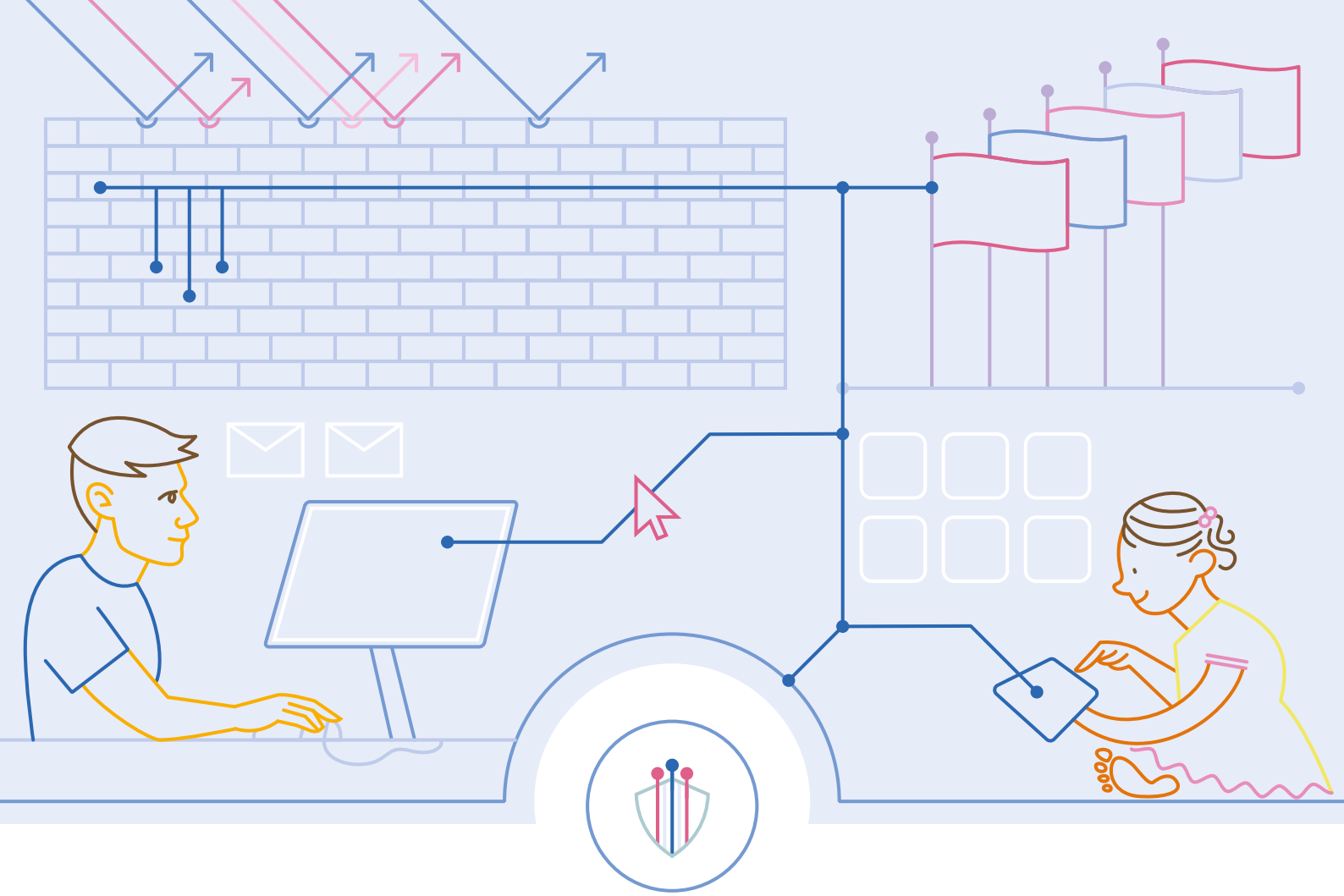
Those who are unable to use eID personally can be assisted by others via digital authorisation solutions. The National Strategy for eID in the Public Sector includes measures to develop solutions that enable access to public digital services on behalf of someone else, such as a guardian or close relative of an older adult or person with illness who requires practical assistance.

The Government wants individuals who are unable to use eID personally to be able to receive assistance from others via digital authorisation solutions.

It is important that the joint solutions in the geographical infrastructure, such as maps and map data, meet the needs of users and can utilise new technology. A key prerequisite for achieving this is sustainable financing models that can ensure the operation of joint solutions and the development of new functionality. The Government will further develop the national infrastructure for geographic information.

THE GOVERNMENT WILL

- Investigate the mandatory use of joint solutions in public service development and involve the Norwegian Association of Local and Regional Authorities in these efforts
- Ensure that joint central government solutions have a predictable financial framework for sound management, security, operation and further development
- Establish a national architecture for a shared digital ecosystem, in collaboration with the Norwegian Association of Local and Regional Authorities
- Offer everyone a high-level digital wallet using eID
- Develop solutions for digital representation, including for guardianship
- Further develop the national infrastructure for geographic information, such as maps and map data



3.3 Bolstering security, emergency preparedness and crime prevention

Goals

Towards 2030, the Government will strengthen national cyber security and emergency preparedness to safeguard critical societal and fundamental national functions. To strengthen our work on national security and emergency preparedness, we will actively use digital technologies. The national capacity to combat cybercrime will also be strengthened.

3.3.1 Digitalisation for enhanced security and emergency preparedness

STATUS

Crisis management and military operations are characterised by short timelines, complex situational overviews, and a considerable need for information that cannot be managed without the use of digital technology. This is consistent with lessons learnt during the pandemic. During crises, data sharing is necessary to

ensure adequate national situational awareness. The use of AI, in conjunction with other technologies, also enhances situational awareness and bolsters Norway's defence capability.

Digitalisation can help strengthen national security and emergency preparedness capabilities. Effects that can be achieved with digitalisation include improved interaction in the total defence and with allies. Furthermore, digitalisation can contribute to faster and more comprehensive situational awareness and strengthen the ability to manage complex threats and other security-threatening activities.

Nødnett is the Norwegian critical communication network for the police, fire and health services and other actors with emergency response and emergency preparedness responsibilities. It is also an important total defence tool. Nødnett provides secure group communication both within and across organisations. Digital solutions such as national registers, the municipal FIKS platform, infrastructure for geographic data, and solutions in the health and care services are also important for interaction between organisations in crisis situations.

Data sets from the UN's Intergovernmental Panel on Climate Change (IPCC) and historical data on Norwegian climate development are currently used to make projections about the Norwegian climate. The use of digital tools, such as simulators, contributes to better situational awareness in safety and emergency preparedness work.

CHARTING THE COURSE TOWARDS 2030

Today's complex threats and challenges affect all sectors of society. A consequence of the threat landscape could be a decline in public trust in the authorities, diminished trust between individuals, and challenges to free democratic debate. This can in turn result in dilemmas that are difficult to manage, such as a cyberattack on critical digital infrastructure, in conjunction with a disinformation campaign that gives the impression that the authorities are unable to ensure Norwegian citizens safe access to the internet.

The Government will carry out a comprehensive and sustained investment in the Norwegian Armed Forces' ICT systems, infrastructure and skills, in collaboration with relevant civilian and allied actors. To ensure national control, Norwegian crypto skills must be maintained and strengthened.[63]

Increasing complexity demands a greater degree of cross-sectoral situational awareness, along with extensive national coordination and collaboration. We must leverage digitalisation to improve national situational awareness, for example by converting vast amounts of data and information into knowledge. This will create new opportunities for the dissemination of information between citizens and national authorities, NATO and other relevant actors in the event of serious incidents such as accidents, terrorism and natural disasters. Unwanted events necessitate cross-sectoral and cross-border interaction with neighbouring countries and other allies. Digitalisation is a tool for better collaboration between actors and for strengthening our defence capability and overall civil protection.

The ability of military and civilian actors to communicate securely is a fundamental prerequisite for a shared situational understanding and a functioning total defence across the entire crisis spectrum. Therefore, the Government will continue its efforts to roll out secure ICT solutions across actors within the total defence framework.

Today's Nødnett functions well, but it is based on technology that is becoming outdated and will eventually have to be replaced with a new solution to maintain and further develop the emergency preparedness and handling capability of the emergency services. The Government wants to establish a new critical communication network with the possibility of increased and near real-time cross-sectoral collaboration and data sharing in the event of unwanted events. A concept has been chosen for group-based voice, data and video with a combination of state ownership and purchases from commercial mobile operators to capitalise on the strengths of both sectors and to ensure a solution that ensures national control.

THE GOVERNMENT WILL

- Utilise digital solutions to increase situational awareness and manage complex threats, accidents, natural disasters and other unwanted events
- Strengthen Norway's ability to conduct operations in the digital domain
- Utilise digital solutions to further develop and streamline training and exercises across sectors and administrative levels as well as with allies
- Establish secure, cross-sectoral ICT solutions with total defence responsibilities
- Continue to work on the establishment of a new critical communication network

3.3.2 Collaboration and coordination for enhanced cyber security

STATUS

The Government's strategic direction, priorities and measures to safeguard cyber security are set out in Report to the Storting (white paper) 9 (2022-2023) *National control and cyber resilience to safeguard national security.*[64] The report builds on a strategic course developed over many years, including in national strategies, white papers and investigations.

The white paper clarifies and reinforces the strategic direction. It emphasises public-private, civil-military and international cooperation and underscores the importance of involving the whole of society.

Regulatory policy instruments play a key role in making enterprises accountable. At the same time, the authorities must help coordinate, strengthen and simplify preventive security efforts. In addition to prioritising prevention, Norway must ensure that it has sufficient capacity to address the growing number of cyberattacks.

Some key measures from the report that are particularly relevant for strengthening cyber security in the future are to increase the authorities' work on coordination and governance and to support organisations in their security efforts to improve

individual digital emergency preparedness and thereby enhance collective security in society. Other measures include using regulatory policy instruments to make Norwegian businesses accountable, including further development of the Cyber Security Act, and enhancing skills in cyber security (see also section 3.5. It is also important to participate in an international cooperation to maintain the trust of international partners, including as a basis for receiving information regarding cyber threats.

The report *National Digital Risk Situation* is published annually. In the 2023 report[65], the Norwegian National Security Authority describes a challenging situation in which technological development is accelerating and technology is expanding its reach. Furthermore, generative AI challenges our ability to recognise the difference between what is real and what is fake, as well as what is true and what is false. At the same time, the gap between the competence and skills of threat actors and preventive security work is widening.

Each business is responsible for its own cyber security and must therefore ensure that its employees receive the necessary guidance and training in cyber security.

The Norwegian National Criminal Investigation Service (Kripos) estimates that generative AI will lead to an increase in both the scope and severity of cybercrime.[66] There are already threat actors using generative AI, including for large-scale phishing.[67] AI can also be used to prevent and detect cyber attacks. For instance, the Norwegian National Security Authority has further developed a warning system for digital infrastructure with AI-based sensors.

CHARTING THE COURSE TOWARDS 2030

The heightened security situation in the world means that cyber security and emergency preparedness efforts are becoming more important and are crucial for safeguarding critical societal and fundamental national functions. There is a need for increased cooperation and digital interaction within the framework of total defence[68] and with allies in NATO and the EU.

When introducing new digital solutions, consideration must be given to whether the solutions are to be available across the entire conflict spectrum (peace, crisis and war). Key digital services must remain operational when they are needed the most. They must be available nationwide under the most challenging security conditions.

The aim is to coordinate and simplify the public sector's access to advice and guidance on cyber security and necessary measures for basic security. The public sector has developed several cyber security guides. Examples include the *Grunnprinsipper for IKT-sikkerhet* [Basic Principles of ICT Security][69] and *Stifinneren* [Pathfinder].[70]

Box 3.8 **National advice and recommendations**

To enhance businesses' digital emergency preparedness and thereby Norway's overall cyber resilience, businesses must follow advice and recommendations from the authorities. Several pieces of legislation require organisations to have adequate management of their security work. Recommendations such as updating software, restricting user access rights, implementing multi-factor authentication for systems and services, and establishing emergency preparedness plans are effective measures that are relatively simple and cost-effective to implement. Among other things, the Norwegian National Security Authority has drawn up basic principles for ICT security that provide useful support in these efforts. The Government will also launch a national cyber security portal where advice from the authorities is gathered.

The local government sector is increasingly vulnerable to cyberattacks. Therefore, the Government is strengthening its work on cyber security in local government. This will enable municipalities to carry out the necessary risk and vulnerability analyses and implement measures to manage such risk. Among other things, the Computer Emergency Response Team (KommuneCERT), has been established to help increase the local government sector's ability to prevent, detect and manage cyberattacks. In 2024, the Norwegian National Security Authority will also be strengthened with new resources to focus on cyber security in the local government sector. The Ministry of Digitalisation and Public Governance will also, in collaboration with the Norwegian Association of Local and Regional Authorities, implement measures to strengthen basic cyber security in the municipalities.

Cyber threats and attacks can paralyse the Norwegian business sector. Efforts and competence regarding such attacks must be enhanced. The Norwegian National Coordination Centre (NCC-NO) for research and innovation in cybersecurity is managed by the Norwegian National Security Authority and the Research Council of Norway. The centre will strengthen cyber security in Norway by supporting businesses, with a particular focus on small and medium-sized enterprises, and promoting collaboration across the sector, public sector, civil society and academia.

The voluntary sector also plays many crucial roles in war and crisis situations. Civilian sector resilience to cyber threats is a prerequisite for the Norwegian Armed Forces to be able to fulfil its missions in peace, crises and war.

THE GOVERNMENT WILL

- Launch a joint national cyber security portal for all target groups
- Improve the coordination of advice and counselling resources related to cyber security
- Strengthen the work on cyber security in the public sector, in collaboration with the Norwegian Association of Local and Regional Authorities
- Bolster civilian sector resilience through the use of digital solutions

3.3.3 Prevention of cybercrime, a shared responsibility

STATUS

The rapid development of technology provides criminals with new tools, means and courses of action. Cybercrime is becoming more organised and professional. Although a great deal of good collaboration is currently taking place, there is a need to further strengthen these efforts. For example, the police require more effective tools to obtain information about criminal activities. Prevention must be managed jointly by way of increased collaboration between the public and private sectors.

Currently, the police have the means to obtain information through investigations and use such information directly as a knowledge base for prevention and mitigation purposes. The police share their knowledge with the business sector, public administration and society at large. This is a resource-intensive endeavour and requires extensive collaboration across these sectors. This knowledge enables citizens, as well as private and public enterprises to better prevent and protect themselves against cybercrime such as online abuse, data theft, data breaches, digital fraud and ransomware.

Citizens encounter a police presence on multiple social media and gaming platforms, where they can provide tips, advice and guidance on criminal activities on the internet. The presence of the police on the internet provides a better understanding of such crimes, enabling citizens to take action and avert situations.

Kripos prevents the sharing and making available of files containing abuse and terrorist-related content online by notifying the hosting companies. In turn, hosting companies remove illegal websites after being warned by the police.

CHARTING THE COURSE TOWARDS 2030

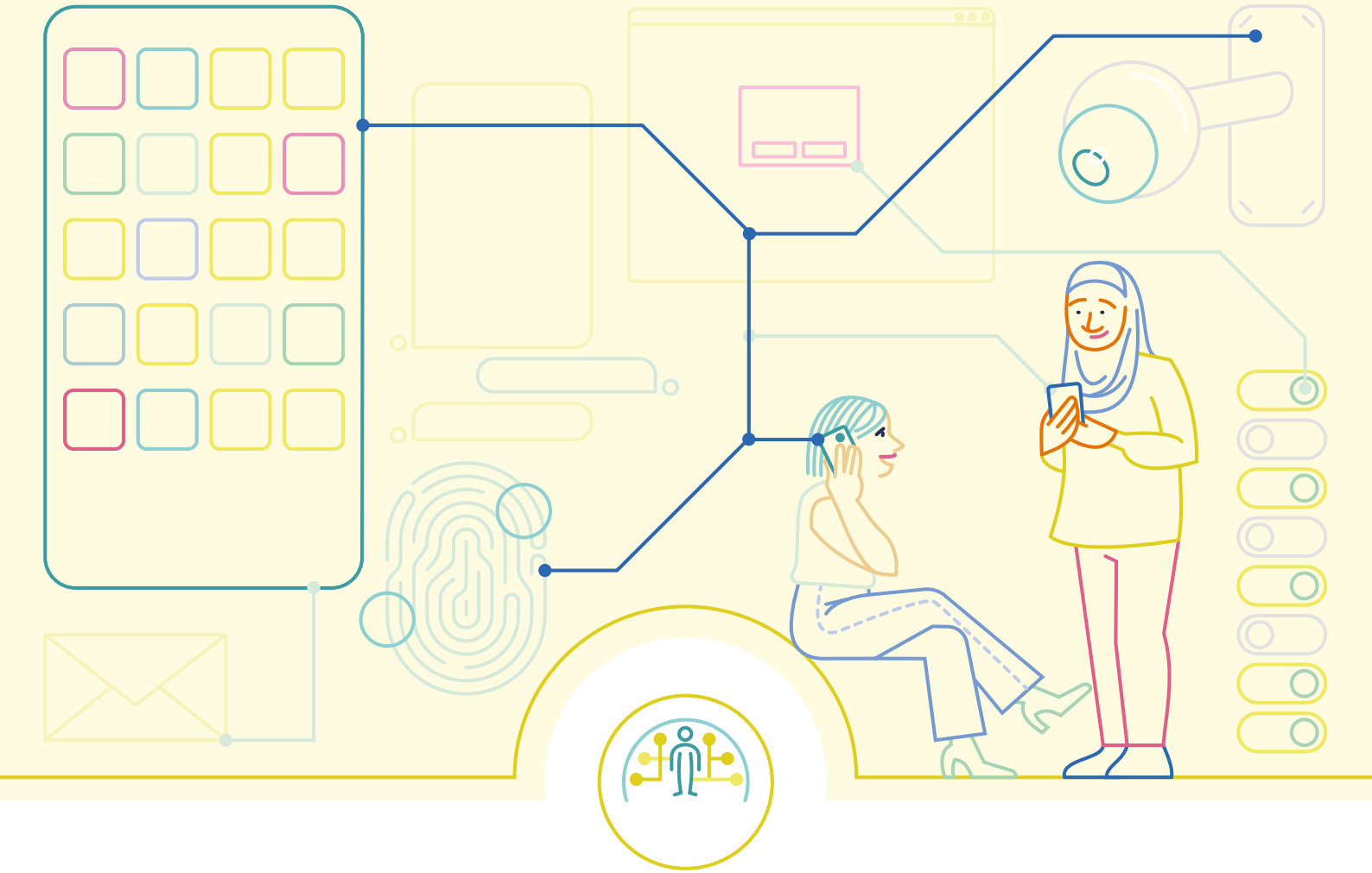
The increased capacity and ability to carry out cybercrime poses a threat to civil protection and, in extreme situations, to national security. To continue and strengthen efforts against cybercrime, including prevention, cooperation and knowledge sharing, it is necessary to strengthen the police's capacity to combat cybercrime and ensure they have access to important information.

The Government wants the police and prosecuting authority to adapt their working methods and structures to what is required to keep pace with technological developments and to make use of big data analytics and AI.

Children and young people are particularly vulnerable to the adverse effects of digitalisation,[71] including in the form of crime. Preventive efforts to keep children and young people safe online have been developed on multiple fronts. The teaching concepts *Delbart?*[72] [Sharable?] and *Dele=delta*[73] [Sharing=Participating] contribute to enhanced knowledge and awareness of the illegality of sharing sexualised images online and videos depicting violence. Kripos is creating a blocking filter for primary and lower secondary schools that blocks access to illegal websites where abuse takes place. The filter can be installed in the ICT equipment that schools distribute to pupils and is important in keeping children safe online. Efforts to keep children and young people safe online should take place in collaboration with the local government sector.

THE GOVERNMENT WILL

- Strengthen efforts to combat cybercrime
- Leverage new technology to increase the quality and effectiveness of criminal proceedings
- Strengthen preventive efforts to keep children and young people safe online
- Strengthen the knowledge base and research on cybercrime



3.4 Ensuring appropriate and safeguarded privacy for all

Goals

Towards 2030, the Government will safeguard privacy in all digitalisation efforts. All relevant IT solutions in the public sector shall have built-in privacy protection, and we shall ensure citizens' privacy in their interaction with the Tech Giants.

3.4.1 Privacy as a societal value

STATUS

Privacy is a human right, protected by the Constitution of Norway and the European Convention on Human Rights (ECHR). The protection of privacy safeguards people's integrity and private life and is also a prerequisite for other key democratic values such as freedom of information and freedom of expression. However, privacy is in a challenging position. Currently, assessments of privacy are not sufficiently comprehensive across sectors. There is a general tendency for the digitalisation of society to take place at the expense of privacy.[74] If we are to succeed with

digitalisation, people must be willing to use digital services. Citizens need to be certain that we manage data appropriately. Effective privacy protection is therefore a prerequisite for successful digitalisation.

CHARTING THE COURSE TOWARDS 2030

Inadequate privacy protection can lead to undesirable outcomes such as a chilling effect[75] and echo chambers[76], and can also be utilised for what is referred to as *nudging*.[77] To avoid such outcomes, we must emphasise privacy as a fundamental societal value. We must make the difficult trade-offs and consider matters of principle and ethical dilemmas. Privacy must be weighed against other interests. Privacy must be viewed from a holistic perspective, not just case by case, so that we can develop comprehensive privacy protection policies.

To ensure a comprehensive overview, the Government believes there is a need for an independent advisory body, similar to the Danish Data Ethics Council,[78] which can assess matters of principle that arise when privacy interests must be balanced against other weighty societal values. This ensures that privacy is a natural part of the public debate. A data ethics council can assess general ethical issues arising from digitalisation. The Government will therefore investigate the establishment of an advisory body that can assist with ethical assessments and examine privacy and digitalisation across sectors, disciplines and administrative levels.

3.4.2 Basic prerequisites for effective privacy protection

3.4.2.1 Fair balance of power

STATUS

In many cases, the uneven balance of power between users and providers of digital services can limit users' ability to safeguard their privacy.

When interacting with the public sector, citizens have limited influence over how their personal data are processed. Data are shared both within and across agencies. They may also be disclosed for research and other purposes that are not directly related to the provision of the service. Disclosure is important for the public sector to be able to provide good services. At the same time, it can be difficult for individuals to gain an overview of how their personal data are processed and thereby safeguard their privacy.

In the business sector, data-driven business models are creating new opportunities for many enterprises and have therefore become commonplace. They are based on users being offered products and services in return for the disclosure of personal data, known as *behavioural advertising*. It can be very difficult for users to understand how much data is collected, how it is used, and with whom it is shared. Companies with such business models may dominate the market to the extent that users feel there are no alternatives to their services. Thus, large multinational corporations can dictate the standards for privacy.

Interacting with social media can be challenging for children. Such platforms are rarely age-appropriate. Children are more impressionable and vulnerable when using social media than adults, and many children have had negative experiences when using social media. At the same time, research on whether, and how, social media affects children is inconsistent.

Another domain marked by an uneven balance of power is the labour market, specifically between employers and employees. The use of digital tools in working life generates a number of digital footprints. These can be used by employers to monitor and control employees.

CHARTING THE COURSE TOWARDS 2030

Extensive data sharing in the public sector means that the authorities must take particular responsibility for ensuring that individual privacy is safeguarded through clear legislation, good guidance and effective enforcement of the legislation. When the public sector processes personal data, this is usually done as part of the exercise of authority, authorised by acts or regulations. The legislation must safeguard citizens' rights and create and maintain trust among the population. The Privacy Commission, which has investigated the overall situation for privacy in Norway,[79] has highlighted several challenges and shortcomings in the current regulatory framework governing personal data. We need an effective and comprehensible regulatory framework based on thorough privacy assessments, and that safeguards the privacy of all citizens. The Government will therefore work towards a more uniform approach to the regulatory framework governing the processing of personal data, with clear and comprehensible privacy assessments.

Data-driven business models that challenge core privacy rights are problematic. The Government believes that citizens should not have to choose between digital services and effective privacy protection. Privacy shall be safeguarded in all services. Citizens must receive comprehensible information that enables them to make informed and conscious privacy choices. However, responsibility for effective privacy protection must lie with the responsible agency rather than the individual citizen. The Government will therefore explore Norway's options for regulating digital services, with a focus on evaluating the implications of a national ban on behavioural advertising. However, digital services are largely provided by service providers outside Norway. Effective privacy protection therefore hinges on international cooperation, and we will ensure effective cooperation with the EU on privacy regulation.

Digital services are a large part of the day-to-day lives of children and young people, and also a large part of their social and creative lives. Children and young people are in a different position than adults in terms of understanding the risks and consequences of their actions or recognising their rights. Therefore, children are entitled to special protection. Ensuring such protection is the responsibility of parents, the public sector, the voluntary sector and businesses. Schools must safeguard the privacy of children and young people during school hours, especially when children and young people are required to use digital solutions provided by the public sector. In its efforts to implement the DSA in Norway, the Government

will ban behavioural advertising to children based on personal data. The topic of children and young people's everyday digital lives will be explored in greater detail in the upcoming white paper on a safe digital childhood, scheduled for presentation in autumn 2024.

Box 3.9 **Privacy at school – Du bestemmer [You decide]**

Du bestemmer [You decide] is a collaboration between the Norwegian Directorate for Education and Training and the Norwegian Data Protection Authority. The online resource dubestemmer.no offers information about privacy and rights to children and young people between the ages of 9 and 18. The resource is intended for use in an educational context. The aim is to help students learn to better manage their personal data while respecting the data of others. There are also dedicated sites that provide teachers with knowledge and support for instruction on this topic.

The Working Environment Act and the Regulations issued pursuant to the Act currently regulate some of the issues surrounding the monitoring and control of employees.[80] Many employers are able to collect vast amounts of data about employees' digital activities via digital tools used in the work setting.[81] The use of home office and digital work have become more commonplace following the COVID-19 pandemic. This presents new challenges to privacy. The uneven balance of power can make it difficult for employees to safeguard their rights, and data collection can give rise to mistrust and uncertainty. The Government will therefore review the rules governing privacy in working life to assess whether there is a need for special regulation.

3.4.2.2 Knowledge, guidance and supervision

STATUS

It can be difficult for citizens to gain an overview of the type of personal data being processed about them, what their rights are, and how they can exercise these rights.

The public, voluntary and private sectors have all highlighted a need for more knowledge and guidance to ensure compliance with the privacy legislation. The Norwegian Data Protection Authority's regulatory sandbox for privacy-friendly innovation and digitalisation is a guidance measure that helps enterprises develop and adopt privacy-friendly and innovative solutions. Another important measure is to collaborate with industry trade groups, interest groups and others on the design and distribution of adapted guidance materials.

CHARTING THE COURSE TOWARDS 2030

The Government's aim is for citizens to be aware of their rights, and for enterprises to know and fulfil their obligations under the privacy legislation. Guidance and information from the Norwegian Data Protection Authority and other relevant authorities play an important role in relation to both citizens and enterprises. Guidance and communication on compliance with the privacy legislation must take place in close dialogue and understanding with the Norwegian Data Protection Authority. This ensures coherence between the guidance on the legislation and the criteria and standards applied by the Norwegian Data Protection Authority when supervising compliance with the privacy regulations.

Box 3.10 **Responsible innovation**

The Trondheim-based technology company Secure Practice is among those who have participated in the Norwegian Data Protection Authority's regulatory sandbox. Secure Practice has developed a service that enables enterprises to deliver targeted cybersecurity training while appropriately safeguarding employees' privacy. In 2023, Secure Practice was awarded an EU contract worth NOK 29 million to strengthen cybersecurity throughout Europe – with good privacy protection as a competitive advantage.

Knowledge of privacy protection is expected to be included in higher education where relevant, including in the fields of technology, law, teacher training and informatics. Effective privacy protection skills in related professions will benefit the population as new digital services and products are developed.

Effective guidance and enforcement of the legislation depend on a well-functioning supervisory system. The Government's ambition is for the Norwegian Data Protection Authority to be equipped to fulfil its statutory duties, meeting both current and future challenges.

Effective compliance with a complex regulatory framework requires both legal and technological competence. Data protection officers can be an important resource in the work to enhance competence regarding privacy protection in enterprises. The Norwegian Data Protection Authority is experiencing a high demand for advice and guidance, and it is important that such guidance is as practical as possible, in the form of adapted advice, templates and checklists. Guidance efforts will be strengthened by preparing templates for privacy policies in the public sector. To support effective privacy impact assessments in legislative efforts, a separate guide will be drawn up to supplement the general guide to the instructions for official studies.

3.4.3 The public sector as a trailblazer

STATUS

The public sector in Norway processes and shares vast amounts of personal data about the population. Both the central and local government sectors process data about all of us from the cradle to the grave, including sensitive data. This data is collected and shared across agencies, sectors and levels, and between central and local government, and is also used for research purposes. Most of the personal data that we as citizens share with the public sector is either a result of mandatory self-disclosure or because the data in question is required to receive services or benefits. For example, we are required to report income data for tax purposes and health data to receive healthcare.

CHARTING THE COURSE TOWARDS 2030

The vast amount of personal data processed by the public sector entails a great responsibility for citizens' privacy. Good digitalisation with effective privacy protection requires competence in technical, organisational and regulatory matters. Securing such competence is challenging.

The local government sector, in particular, has highlighted the challenges of safeguarding privacy and the need for better guidance and coordination to enable municipalities to meet privacy requirements in their digitalisation efforts. Among other things, they emphasise the need for support in safeguarding the privacy of children and young people in kindergarten and primary and secondary education and training.

Many of the measures implemented by the public sector to safeguard privacy have a considerable potential for reuse. This includes assessments of the privacy implications of digital solutions. In collaboration with the Norwegian Association of Local and Regional Authorities, the Government will therefore assess suitable measures to strengthen the sharing of skills and experience in the local government sector.

Once personal data has been collected, it may be relevant to use it for purposes other than the original purpose, such as research and quality improvement, training of algorithms for AI or audit purposes. Such reuse or data sharing can pose challenges to privacy protection. The Privacy Commission expressed concern that the public sector lacks a comprehensive approach to privacy, as no one is responsible for assessing the overall use of personal data. Even if the privacy impact of a single measure is considered minor, the sum of measures may entail a significant invasion of privacy. The Government will therefore ensure that comprehensive privacy impact assessments are carried out.

Personal data must be shared and reused in the most privacy-friendly manner. This means, among other things, that citizens must be given adequate information about how their data is shared and the opportunity to object to their data being processed as far as possible without jeopardising the purpose of the processing. Good access solutions should be facilitated, so that citizens can easily obtain an overview of what data are being processed.

The public sector is a major purchaser of various digital solutions. In its purchasing role, the public sector can set requirements and thereby create a demand for and contribute to the development of privacy-friendly services. Thereby, the public sector can also contribute to better privacy protection in other areas of society. There is a need for digital solutions and products for use in several parts of the public sector, such as teaching aids in schools and digital solutions for use in the health and care services. Privacy by design should therefore be a requirement in procurement processes.

Box 3.11 **Privacy by design**

The Personal Data Act requires digital solutions to have privacy by design. This means that privacy must be taken into account in all phases of the development process. The aim is to ensure that privacy is built-in from the ground up and that the solutions adequately safeguard users' privacy rights.

Certain areas are dominated by a few big tech companies. As there are few alternative service providers, both the public and the private sector are dependent on using services from these companies. However, several of the companies have business models and terms and conditions that may present challenges to privacy. Due to their dominance, they are largely able to dictate terms and conditions. Being a major purchaser is therefore an advantage in terms of enforcing privacy requirements. In this context, the public sector, as a major customer, can play a key role in negotiating strong privacy protection terms, such as when making purchases for the school sector.

Through its communication policy, the public sector will be able to send signals and set standards for privacy protection. Government agencies that use online analytics tools shall carry out thorough risk analyses in line with the advice of the Norwegian Data Protection Authority.[82] The Government will set relevant requirements in the Digitalisation Circular.

3.4.4 Responsible business and voluntary sectors

STATUS

Norwegian businesses and organisations are doing considerable privacy protection work and are keen to ensure that privacy is safeguarded.[83] Many are requesting more guidance, common tools and templates that will make it easier to understand the requirements and how to fulfil them in practice. Lessons learned also indicate that many people find it difficult to know what is considered good enough, as well as which privacy measures to prioritise. They want the Norwegian Data Protection Authority to provide clarity through its decisions and supervisory activities.

CHARTING THE COURSE TOWARDS 2030

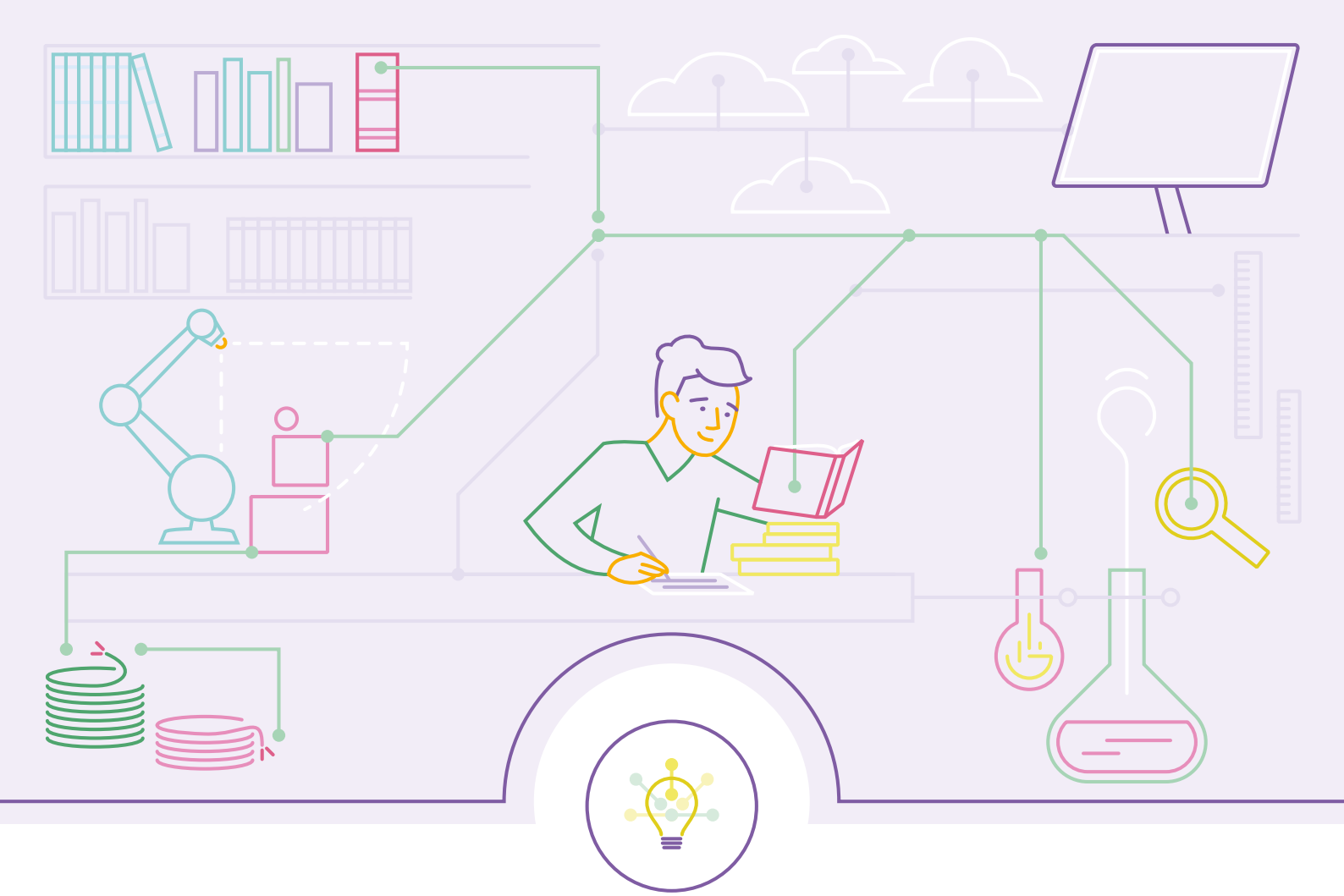
The business and voluntary sectors have a major responsibility to ensure effective privacy protection in digitalisation, both by safeguarding the privacy of their customers or members and as suppliers of digital services to the public sector. *Accountability* is also one of the basic principles of the General Data Protection Regulation (GDPR). The business or organisation that processes personal data is responsible for ensuring that it meets the requirements and safeguards the rights of the persons whose personal data is being processed (the data subjects).

It is necessary to make it easier for businesses and organisations to ensure effective privacy protection in practice. Public, private and voluntary actors must work together in order to achieve this. Tools and best practices should be shared, also between private businesses and voluntary organisations where appropriate.

The Government wants to strengthen programmes that assist Norwegian businesses in succeeding with effective privacy protection in practice. Certification and industry standards are specific and practical tools that, although not widely used today, can make a positive contribution to operationalising legislative requirements in practice. Privacy by design is a legal requirement, but also an opportunity. Building privacy into a solution from the ground up can improve the user experience and build trust, providing a competitive advantage in a world where personal data is highly valued.

THE GOVERNMENT WILL

- Investigate the establishment and organisation of a data ethics council that can assess matters of principle in the trade-off between privacy and weighty societal interests
- Ensure a more uniform regulatory framework for privacy protection
- Strengthen guidance on and enforcement of the privacy legislation
- Identify measures to strengthen the sharing of skills and experience in the local government sector in collaboration with the Norwegian Association of Local and Regional Authorities
- Encourage the development and use of privacy-friendly technology by requiring privacy-friendly solutions in public procurements
- Include a requirement in the Digitalisation Circular that government agencies using web-based analysis tools must carry out thorough privacy risk assessments
- Review and evaluate how employee privacy is safeguarded
- Encourage a greater use of industry standards, common tools, experience sharing and certification for privacy protection



3.5 Securing future-oriented digital competence

Goals

By 2030, the Government wants to ensure that Norway has access to the necessary digital competence, both as a basic skill in all relevant education programmes and as specialised skills. Technology subjects will be prioritised in education. We will ensure that the public sector and the business sector have access to the necessary skills to succeed in the green and digital transition.

STATUS

Norway will need significantly more employees with ICT skills in 2030 compared to 2019.[84] The OECD highlights digital skills in the public sector as a challenge, with Norway below the OECD average in terms of developing and retaining digital skills.[85] We need a workforce that can support the green transition, including engineers, ICT specialists, bioinformaticians and skilled workers in technology and crafts.[86] We expect a labour shortage in the health and care services and occupations that require a trade certificate. Statistics Norway has estimated that we will have a shortage of healthcare professionals of almost 70,000 full-time equivalents in 2040.[87] Digitalisation and new technologies can free up labour

for other tasks and reduce the overall demand for labour. Educational provisions in primary and lower secondary schools, upper secondary education and training, tertiary vocational colleges and higher education must support this endeavour.

Whereas it was previously common to complete an education at a young age, rapid changes in the labour market will now require skills enhancement and continuing education. The workforce must be able to handle new digital tools, ICT solutions and change processes.

The proportion of students enrolled in science and technology studies in Norwegian higher education is lower than the OECD average,[88] and the demand for labour with IT skills is greater than the supply. There is a demand in the labour market for individuals with digital skills adapted to the profession they are entering, as well as individuals with specialised technology skills. Cyber security and privacy protection should be incorporated into all ICT and technology educations. The Government's aim is for society and the labour market to have access to people with relevant digital skills.

The digital maturity of government agencies varies to a large extent.[89] Managers and employees report unmet skills needs related to digitalisation and changing working methods. There are strong indications that managers' competence, skills and expectations are key to agencies' success in adopting digital solutions.

A commission for skills reform in the labour market[90] is investigating opportunities and policy instruments for learning in the labour market, how we can stimulate more supplementary and continuing education, and how we can facilitate the development of skills adapted to the needs of the labour market. The commission will examine these issues in light of considerable variations in challenges within the labour market and between the public and private sectors. The committee will present its report in the autumn of 2024.

Applications to educational programmes have vastly exceeded their capacity. The potential for qualifying more people with ICT skills appears to be relatively high, but the capacity of the programmes represents a bottleneck.

In 2021, ICT research and development (R&D) totalled more than NOK 26 billion in Norway. This is approximately one-third of the total R&D investment. In 2011, ICT accounted for 20 per cent of the total R&D investment. This development indicates how important ICT has become in all areas of society. In the business sector alone, the share of R&D devoted to ICT is 55 per cent. Approximately 85 per cent of R&D investments in ICT are funded by the business sector, either in the form of in-house R&D or purchased services from research institutes and the university and university college sector. Most of the business sector's R&D are development activities. The majority of the research is publicly funded.

There is also research on ICT in the humanities, social sciences and law. Such research is important for understanding how ICT and organisations and people interact and influence each other. It is important to develop knowledge of how technology affects society and the legal consequences of its use.

Developments in AI research illustrate how a technological shift affects the direction of the overall research portfolio. In recent years, AI research has accounted for a growing share of ICT research funded by the Research Council of Norway. From 2019 to 2023, the annual allocation has increased from NOK 200 to 700 million.

Achieving the goals of digitalisation depends on strong, high-quality knowledge environments related to ICT, as well as R&D in areas that are important for Norway. Although much is happening internationally that we can benefit from, it is particularly important that we possess our own competence and R&D environments in certain areas; cyber security being one such area. Long-term, fundamental ICT research plays an important role in preparing for future challenges and needs. Developments in ICT have also shown that this is a field where groundbreaking changes often occur, as we have seen in recent years with the developments in AI. To be able to handle such rapid changes, fundamental research and understanding of the field at a basic level are essential. Foundational technology will often have applications beyond what was originally envisaged.

CHARTING THE COURSE TOWARDS 2030

Government agencies must develop competence related to the opportunities presented by digitalisation and AI. The local government sector has been working on this for several years. At the same time, a growing number of municipalities are finding that a lack of skills is hindering the development of their digital services.[91] Therefore, the Government will prepare a separate strategy for digital competence in the public sector, in collaboration with the Norwegian Association of Local and Regional Authorities.

Children and young people need to be able to critically handle technology and the diversity of information they encounter in everyday life in order to influence and actively participate in education, society and working life. They must be able to exercise good judgement when interacting online and when using and sharing information. Schools have an important role to play in helping students gradually develop these competencies. In line with Report to the Storting (white paper) 34 (2023-2024) *En mer praktisk skole – Bedre læring, motivasjon og trivsel på 5.–10. trinn*[92] [A more practical school – Better learning, motivation and well-being in grades 5-10], the Government is seeking a balanced and knowledge-based approach to the use of digital tools and devices in schools. This will ensure that pupils acquire the necessary digital skills, without jeopardising other basic skills such as reading. School should be an arena that promotes good choices and appropriate use of digital solutions and media, and that teaches children and young people to navigate and master the digital landscape.

Teachers' professional digital competence is a particularly important factor in strengthening the digital competence of the population. The Government will support school owners in strengthening professional digital competence in education through teacher training programmes and supplementary and continuing education schemes for teachers, managers and other school staff.

Box 3.12 **Strategy for digital competence and infrastructure in kindergartens and schools 2023–2030**

The strategy for digital competence and infrastructure in kindergartens and schools 2023-2030 has been drawn up in collaboration with the Norwegian Association of Local and Regional Authorities and describes the challenges and frameworks for work on safe and responsible digitalisation. The strategy contains a number of measures that will contribute to a more balanced, knowledge-based and responsible practice in the sector. The Government and the Norwegian Association of Local and Regional Authorities agree that we must:

- Consider the best interests of children and young people, and their rights and adopt a precautionary approach, especially in relation to younger children;
- Support the goals and core values for kindergarten and primary and secondary education and training;
- Make choices based on knowledge and a comprehensive approach;
- Involve and cooperate with the social partners and other key stakeholders, as needed;
- Facilitate innovation and testing within safe frameworks;
- Dare to ask difficult questions and tolerate nuanced answers.

In the new Education Act, the Government has placed greater emphasis on scaling upper secondary education and training in line with society's needs. Society requires skills in many areas, both now and in the future, including skills that are important for the digital and green transitions.

In tertiary vocational education, the number of IT students has increased tenfold in the past decade – from 300 to more than 3,000 students.[93] The Government will prioritise study places in technical subjects in future allocations of study places to the tertiary vocational colleges and will facilitate a dialogue with the county authorities on how they can follow up this prioritisation in their administration of the sector.

In order to strengthen society's access to specialised digital competence, the Government expects universities and university colleges to prioritise more study places in IT-related studies. This also includes supplementary and continuing education programmes. Ministry of Education and Research has commissioned

the Norwegian Directorate for Higher Education and Skills to develop a better knowledge base that national and regional authorities, universities and university colleges can use in their scaling efforts.

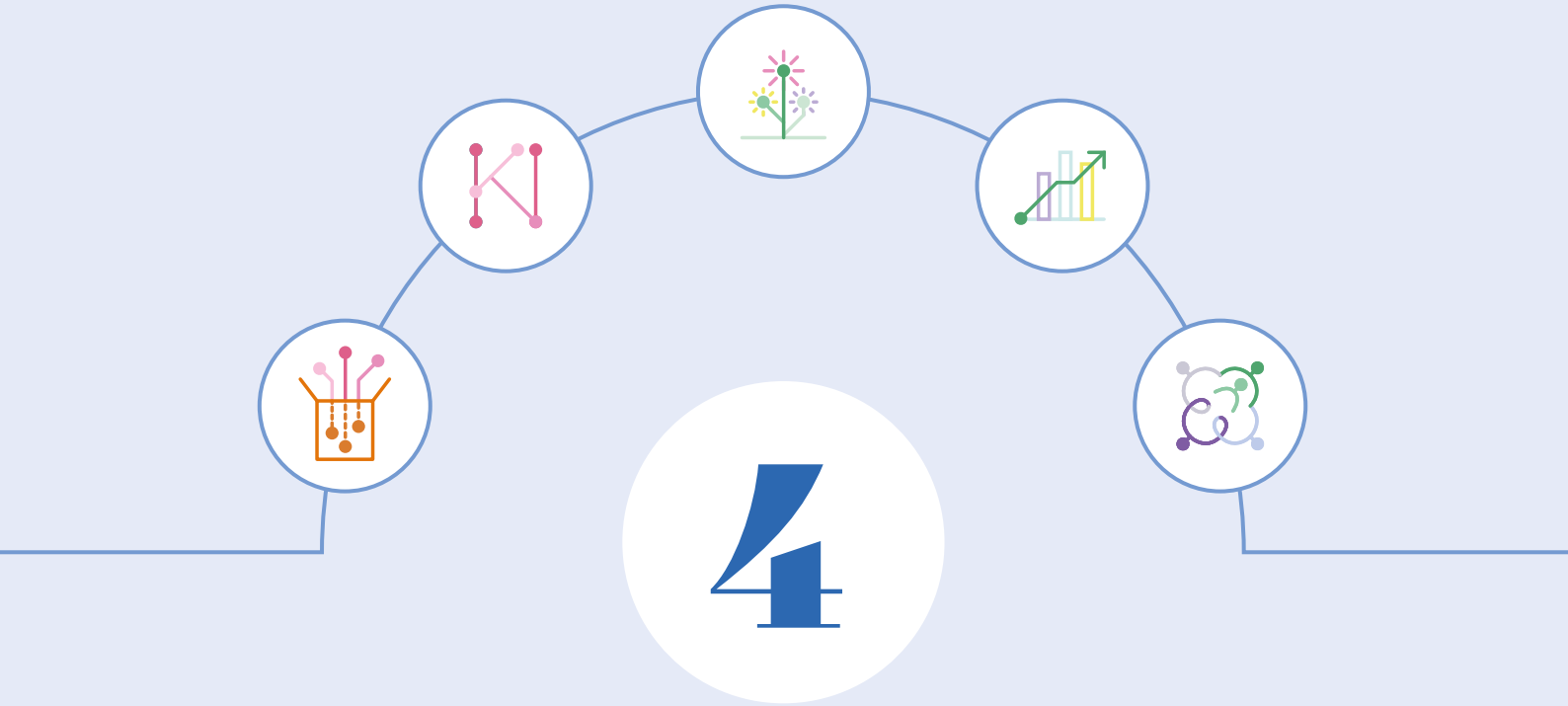
The Norwegian Committee on Skill Needs[94] has been tasked with investigating how new technologies affect skills needs. The Committee is made up of the social partners, researchers and a representative from the county authorities.

The National Qualifications Framework for Lifelong Learning describes qualifications through learning outcomes, i.e., students' skills and knowledge upon completion of studies. The Qualifications Framework was evaluated by the Norwegian Agency for Quality Assurance in Education in 2023. To improve the labour-market relevance of higher education, it will be beneficial in the follow-up of the evaluation to examine the learning outcome descriptions related to digitalisation, as announced for higher education in the Report to the Storting (white paper) 16 (2020-2021) *Utdanning for omstilling*[95] [Education for change].

Efforts will continue to ensure that Norway has good research environments in the field of ICT. It is important to conduct basic technological research and research into the societal consequences of technology, so that sound, knowledge-based decisions can be made. Strong academic environments for ICT research are crucial if Norway is to keep up with international developments in the field and be an attractive partner in research programmes, both in Europe and globally. Strong research environments are also a prerequisite for good ICT education programmes.

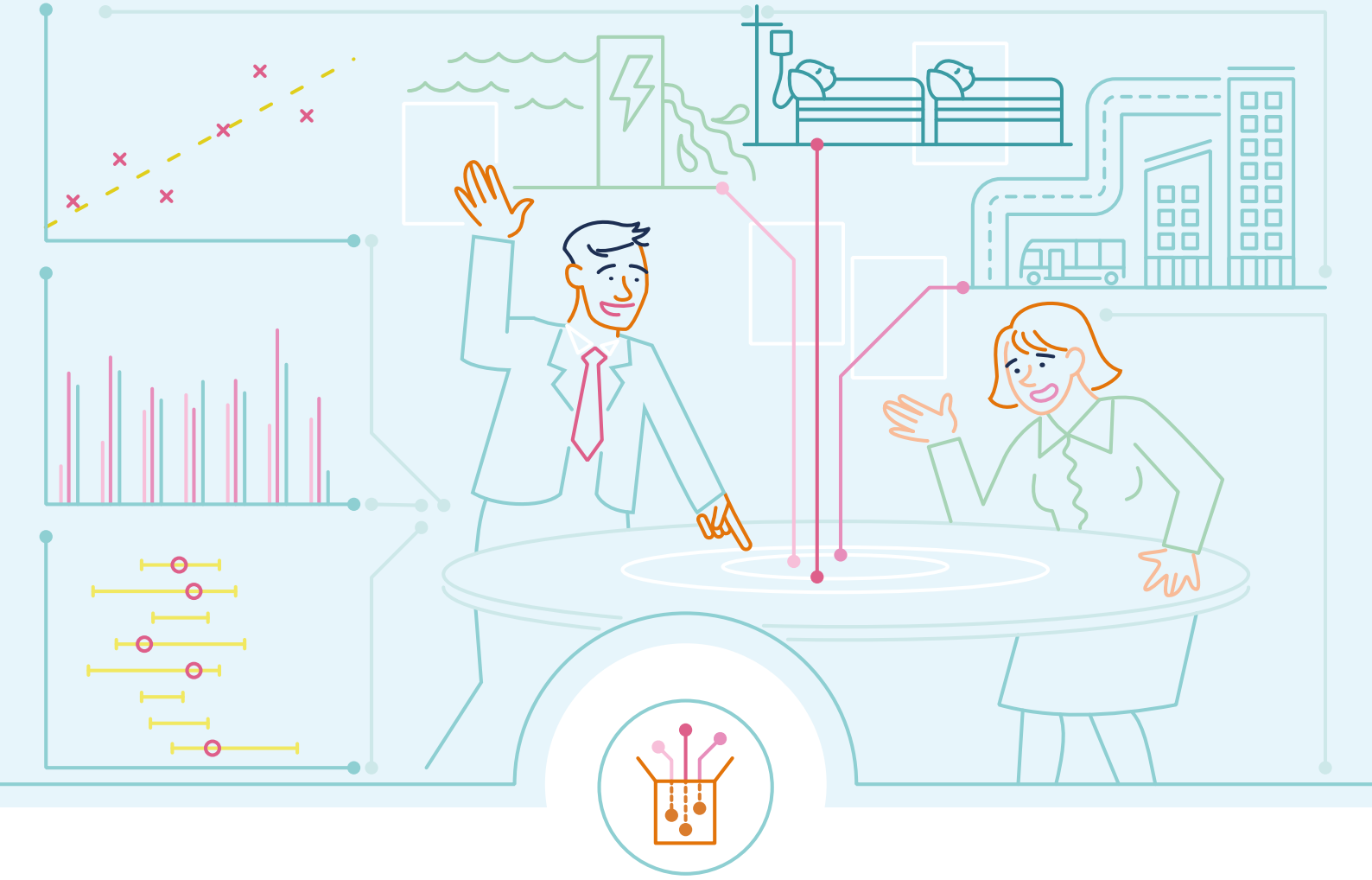
THE GOVERNMENT WILL

- Follow up on the instructions to the universities and university colleges to prioritise technology subjects in the scaling of study programmes
- Develop a competence strategy for digital transition in the public sector, in collaboration with the Norwegian Association of Local and Regional Authorities
- Follow up the measures in the strategy for digital competence and infrastructure in kindergartens and schools, in collaboration with the Norwegian Association of Local and Regional Authorities
- Prioritise study places in technical subjects when allocating study places to tertiary vocational schools, universities and university colleges
- Assess the learning outcome descriptions related to digitalisation in the National Qualifications Framework for Lifelong Learning
- Facilitate strong research environments in the field of ICT



We will increase our efforts in prioritised areas

In addition to the foundational prerequisites for the further digitalisation of society discussed in Chapter 3, the Government will prioritise five focus areas that will contribute to realising the full potential of digitalisation and achieve the goals of the strategy.



4.1 Increase data sharing and harness the opportunities in data and data-driven innovation

Goals

By 2030, the Government wants Norway to be a leader in value creation with data and in data-driven research and innovation. We will participate in the EU's data space initiatives where relevant.

STATUS

The potential for creating value with data is estimated to be huge, with data from both the business and public sectors.[96] For example, it is estimated that the economic value of public sector data in the EU will amount to EUR 194 billion in 2030.[97] This means that public data can be of great value if it is managed and shared in such a manner that it can be used for value-adding services and products in society.

Technological developments are driving fundamental changes in production, service provision and digital interaction. New technologies make it possible to extract more value out of data than ever before. Going forward, it will be important to ensure access to good datasets that can be used in the development of AI.

In Report to the Storting (white paper) 22 (2020-2021) *Data as a resource – The data-driven economy and innovation*, a national goal has been set for Norway to leverage the opportunities presented by data to increase value creation, create new jobs and develop an efficient public sector. Norway has made significant efforts to make public data accessible and to share it over a prolonged period. Various national surveys indicate extensive sharing of public data, both within the public administration and between the public and private sectors.[98] However, there is still significant untapped potential for more data sharing and accessibility.[99]

Internationally, Norway ranks among the top countries for the digitalisation of public services and the availability of open public data.[100] Public data refers to all types of information produced or collected by government agencies that is or can be digitalised and stored electronically. Open public data is data that has been made available to the general public.

Box 4.1 **Principles for sharing and use of data[101]**

- Data should be open when possible and protected when necessary.
- Data should be accessible, retrievable, usable and comparable with other data.
- Data should be shared and used in a manner that adds value to the business and public sector and society at large.
- Data shall be shared and used in a manner that ensures respect for fundamental rights and freedoms and preserves Norwegian societal values.

In its 2023 investigation of the authorities' facilitation of the sharing and reuse of data in public administration, the National Audit Office of Norway found that national governance and coordination in this area is inadequate.

Government agencies need to become even better at using their own and others' data to renew and improve public services and to ensure smarter task-solving. Furthermore, government agencies must become better at making data available so that it can be used for new purposes. Data is a prerequisite for the development of high-quality AI solutions needed by the public sector. Statistics from Statistics Norway show that only four out of ten companies in the private sector used public data in 2023.[102]

The *once-only* principle and the requirement for *order in your own house* are important policy instruments in digitalisation policy and should support the goal of an efficient and user-oriented public sector. The Digitalisation Circular requires all government agencies to have a sufficient overview of their own data, what it means and how it can be used. There is also a requirement for datasets to be registered at data.norge.no.

The Norwegian Digitalisation Agency points out that the work on order in your own house is proceeding slowly throughout the public administration.[103] Therefore,

the agency sees a need to focus this work on meeting specific needs, for example by prioritising data that is actually in demand and considered important to the public sector and society.

Data should be shared and used in a responsible and reliable manner. Good information management is an important prerequisite for each organisation to be able to decide which data can be shared and accessed, and which must be protected. According to the General Data Protection Regulation (GDPR), personal data must be used for the purpose for which it was initially collected. The ambition to share more data in the public sector must be in line with privacy legislation. The National Audit Office of Norway points out that these considerations may in some cases conflict with each other.[104]

The GDPR[105] is an important instrument to support data sharing in a safe and responsible manner and to build trust. Both public and private organisations report that they devote a lot of resources on understanding and interpreting the provisions of the GDPR. The perception of a complex regulatory framework and the fear of making mistakes and breaking the rules can therefore pose obstacles for those seeking to test out new ideas through data-driven innovation and AI. This is supported by both the Privacy Commission's report and the National Audit Office of Norway's investigation into the sharing and reuse of public data in public administration. In the National Audit Office of Norway's report, both the Norwegian Data Protection Authority and the Norwegian Digitalisation Agency state that privacy protection is often not adequately assessed or assessed early enough in development projects involving data sharing. Therefore, it is important that data protection is assessed at the same time as the legal, technical and functional possibilities are assessed in development projects.

CHARTING THE COURSE TOWARDS 2030

In 2021, the Norwegian Resource Centre for Sharing and Use of Data was established as part of the Norwegian Digitalisation Agency. In addition, the agency manages national joint solutions, frameworks and guides that contribute to the sharing and use of public data. The Ministry of Digitalisation and Public Governance will follow up in the management dialogue with the agency on how the policy instruments should be structured and further developed so that the work of realising the value of public data can be further strengthened.

SKATE (management and coordination of services in e-government) has initiated work to identify which data sources should be considered particularly important national basic data,[106] and what requirements and expectations should be placed on data managers. Furthermore, the EU sets requirements for the availability of open data from the public sector and defines particularly high-value datasets. Efforts to make particularly important datasets accessible must be prioritised.

The European Data Strategy of 2020 includes an ambition to create a single market for data and recognises that data is a significant resource for start-ups and small and medium-sized enterprises (SMEs), as well as for the development of AI. One important measure in the strategy is to establish a framework for European Data

Spaces in important areas of society where data should flow between countries and across sectors in a secure and efficient manner.[107] Currently, Norway contributes funding to the data spaces through the DIGITAL programme. To date, the greatest efforts have been made in the health field (The European Health Data Space, EHDS). There is considerable overlap between the data spaces mentioned in the white paper *Data as a resource* and the EU's priorities. The Government will promote Norwegian interests and facilitate national actors in leveraging the opportunities presented by the EU's efforts in common European data spaces.

The Government recognises the need to strengthen its efforts to make societally important public data available. Therefore, we will establish a national prioritisation council for data sharing, where key stakeholders are represented. The council will help identify and advise the Government on which national data should be prioritised to maximise the value of public data. A similar board already exists in Ireland, called the Open Data Governance Board.[108]

The Ministry of Digitalisation and Public Governance is preparing the implementation of the EU's many regulations that will promote the sharing and use of data. These are the Open Data Directive, the Data Governance Act and the Data Act.[109] The Government-appointed Commission on Data Sharing has proposed that the sharing of public information (data) should be subject to more comprehensive regulation. The Commission submitted its report, Norwegian Official Report (NOU) 2024: 14 *Med lov skal data deles Ny lovgivning om viderebruk av offentlige data*[110] [Data sharing pursuant to law: New Act relating to the sharing of public data] of 26 June 2024. The Government will follow up the report.

Authorities' contribution to cross-sectoral collaboration on standards and formats for data sharing is important for the business sector. This is also an important prerequisite for the development of AI solutions. Furthermore, there is a need for policy instruments to digitalise entire value chains. Open APIs and good standards for data sharing, processes and data structures are needed. The business sector also needs public data and research results to be shared and made available in common formats. In addition, the industry trade groups must take greater responsibility for facilitating collaboration on the digitalisation of value chains and data sharing.

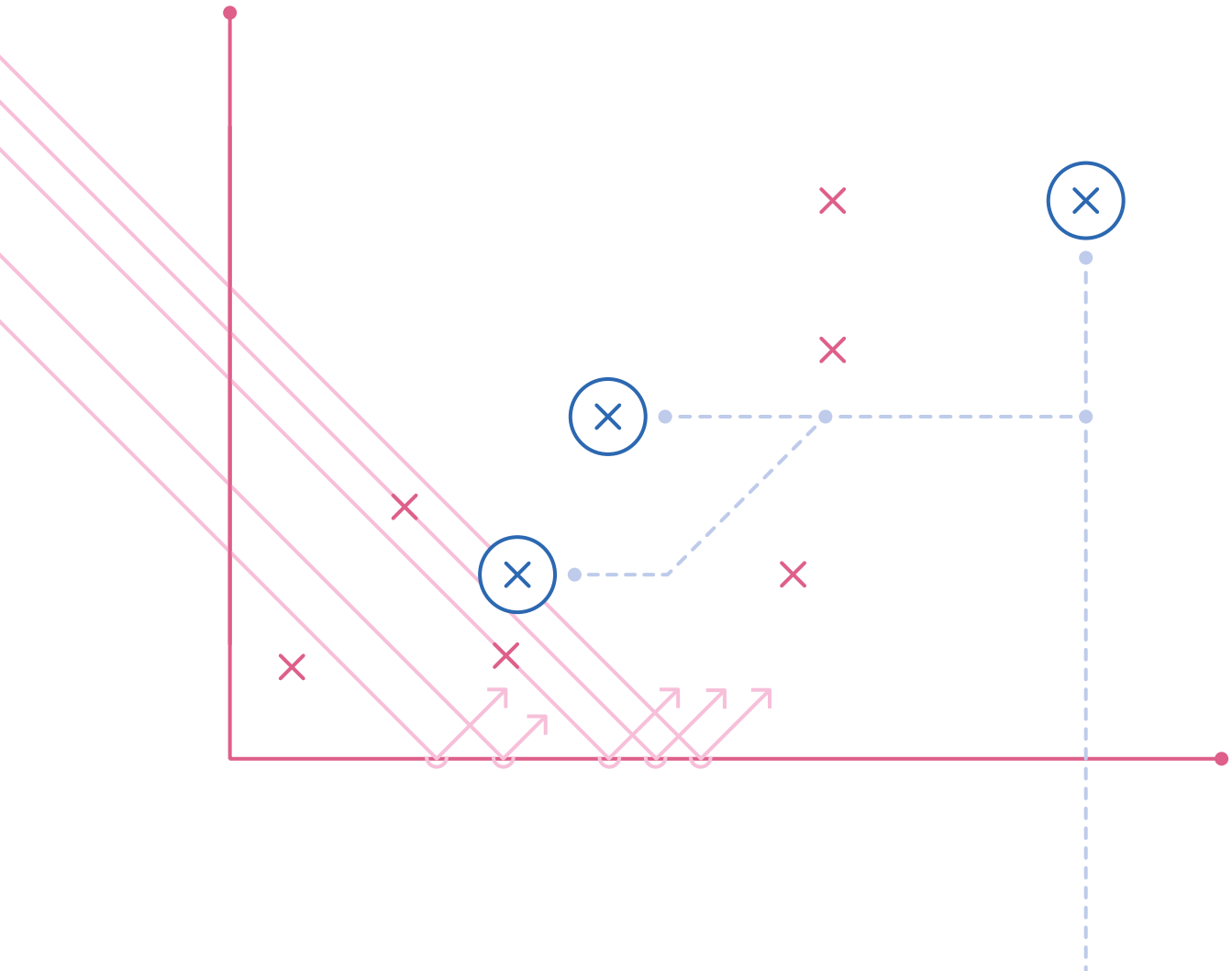
Personal data is an important resource, and using it correctly can benefit both individuals and society at large. At the same time, privacy is a human right. It is important that the use of personal data takes place within the framework of legislation and what is ethically justifiable.

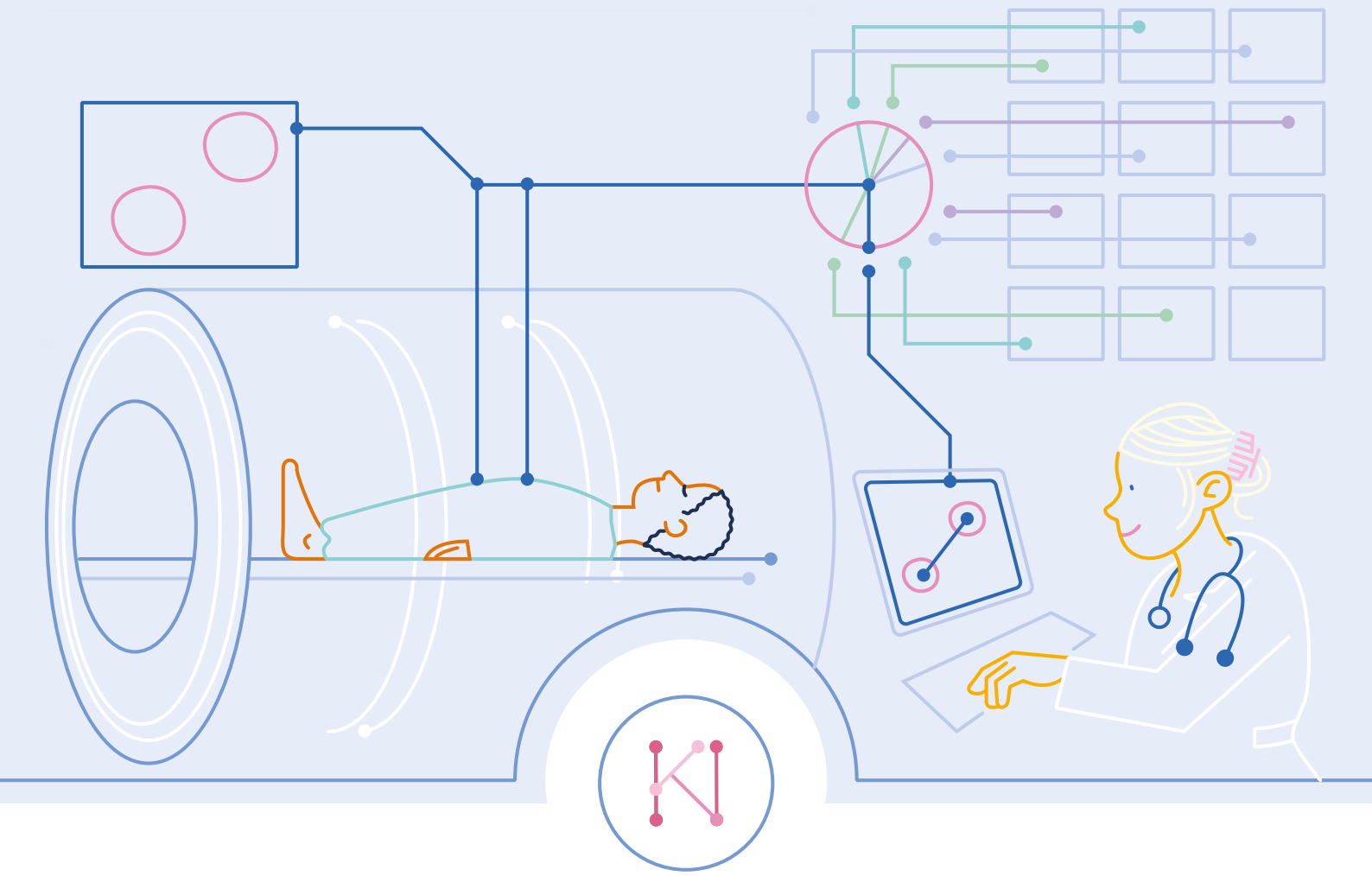
We must leverage the GDPR's scope of action so that it does not unnecessarily inhibit innovation, business development and streamlining of the public sector. The Norwegian Data Protection Authority's regulatory sandbox is an important tool designed to stimulate privacy-friendly innovation and digitalisation. The Norwegian Data Protection Authority must also provide good guidance beyond the sandbox.

The Norwegian Data Protection Authority is responsible for providing national guidance on privacy protection, and the Norwegian Digitalisation Agency provides general guidance on the sharing and use of data in public administration, as well as to private actors seeking to use data for new purposes. The demand for guidance on the use of personal data is high, and neither the Norwegian Digitalisation Agency nor the Norwegian Data Protection Authority currently have the sufficient capacity to meet this demand. The Government will consider schemes that contribute to more targeted and coordinated guidance.

THE GOVERNMENT WILL

- Propose a new data sharing act based on Norwegian Official Report (NOU) 2024: 14 *Med lov skal data deles Ny lovgivning om viderebruk av offentlige data* [Data sharing pursuant to law: New Act relating to the sharing of public data]
- Establish a national prioritisation council for data sharing
- Coordinate and strengthen guidance on sharing and use of data, and the work on order in one's own house
- Prioritise the work of making available national datasets that are important to the public sector and society
- Facilitate cross-sectoral collaboration on standards and formats for data exchange for the digitalisation of entire value chains
- Leverage the opportunities presented by the EU's common European data spaces (European Data Spaces)





4.2 Harness the opportunities of AI

Goals

Towards 2030, the Government will establish a national infrastructure for artificial intelligence (AI), placing Norway at the vanguard of ethical and safe AI use. The business sector shall have favourable framework conditions for developing and using AI. The public sector shall utilise AI to develop better services and solve tasks more efficiently.

STATUS

AI is a ground-breaking technology that has the potential to solve major societal challenges, increase productivity and improve the welfare state. The use of AI can also make important contributions to the green transition. AI can be a game changer for many industries, and the targeted use of this technology can give us a major advantage in sectors including health, energy, aquaculture and other maritime industries.

At the same time, the use of AI raises a number of ethical questions. Using AI to anticipate needs and adapt public services to individual users can challenge privacy. If data and algorithms contain biases, there may also be a risk of discrimination.

Additionally, there is a risk that the development and use of AI could violate human rights and undermine human autonomy. Furthermore, bad faith actors can use the technology to challenge our democracy through disinformation and attacks on important national infrastructure.

The 2020 National Strategy for Artificial Intelligence established seven ethical principles for responsible and trustworthy AI.[111] These principles still apply, and form the basis for the Norwegian Digitalisation Agency's guidance on AI.[112]

Box 4.2 **Ethical principles for responsible and trustworthy AI**

1. AI-based solutions must respect human autonomy and control;
2. AI-based systems must be safe and technically robust;
3. AI must take privacy and data protection into account;
4. AI-based systems must be transparent;
5. AI systems must facilitate inclusion, diversity and equal treatment;
6. AI must benefit society and the environment;
7. Accountability.

The principle of accountability complements the other principles and entails the introduction of mechanisms to ensure accountability for solutions based on AI and their outcomes. All AI systems must be auditable.

The Confederation of Norwegian Enterprise's Skills Barometer for 2023[113] shows that one in five member enterprises of the Confederation have adopted AI tools. Nearly half of the member enterprises have made no use of AI, one important reason being a lack of skills.

Developing and adopting AI requires good communication infrastructure, quality data and access to sufficient computing power. Several industries are working on structures for sharing industry data in value chains. These efforts should be intensified.

The need for supercomputers and associated high-performance computing infrastructure is growing rapidly in connection with the development of AI and is being met through the use of both national and international high-performance computing resources. Not only large enterprises but also start-ups and SMEs need access to high-performance computing resources.

AI can make working life more efficient, interesting and safer. With fewer people available to perform the work, new technology can help maintain and increase productivity and efficiency.

The introduction and use of AI must be in accordance with the rules governing the labour market. Incorporating AI into the labour market can lead to a need for major restructuring. Many jobs will be lost and new ones will be created. This can lead to

a need for employees to enrol in continuing education to acquire new skills. Good collaboration between the social partners is the key to succeeding with the necessary changes.

The aim is to achieve a good balance between the use of digital and analogue teaching aids in schools. AI tools can contribute to more personalised learning and offer suitable aids to pupils and students with disabilities or other challenges. At the same time, the use of such tools raises questions regarding ethics, privacy, cheating and plagiarism. The Norwegian Directorate for Education and Training will strengthen the knowledge base and create guidelines for the use of AI so that school owners have sound advice to follow.

In the healthcare sector, AI can contribute to faster and more precise diagnostics, better decision-making support for personnel, simplified logistics and automation of administrative tasks. In addition, it can improve citizens' monitoring of their own health.[114] Using AI to analyse radiological and other types of imagery can, among other things, reduce the workload for personnel, reduce the radiation doses to which patients are exposed and shorten the time required for examinations. The use of AI can also help streamline writing and structuring tasks, logistics and resource allocation. AI and other labour-saving technologies will help to maintain and improve the quality of healthcare in the years to come and are already reducing wait times in places where they are in use today.

The healthcare sector is by far the area of the public sector[115] with the most AI projects. Many of these are research projects. The Health Research Act has largely remained unchanged since it entered into force in 2009 despite major medical, technological and organisational changes. The Health Research Act and other relevant legislation will be reviewed to assess changes that can ensure that the regulatory framework is better adapted to current needs.

The potential applications of AI in the transport sector are substantial, with the capacity to impact a wide range of important areas for achieving a sustainable, efficient, and safe transportation system. For example, AI is important for the development of more automated vehicles. In road traffic, AI can be used to analyse traffic data and predict traffic flows and driving patterns, which in turn can help optimise traffic flow and contribute to emissions reductions in both passenger and freight transport. In rail and public transport, historical and real-time data can be leveraged to improve travel planning for both operators and travellers.

CHARTING THE COURSE TOWARDS 2030

Norwegian enterprises should harness the power of AI to realise the potential for improving efficiency, quality and innovation. In the public sector, there is great potential to use AI to develop new working methods and better and more adapted services for citizens. The Government wants 80 per cent of government agencies to have adopted AI in 2025, and 100 per cent by 2030.

The Norwegian Board of Technology has presented a report[116] in which it recommends several measures for the safe and appropriate use and development of AI

in Norway. There is a need to establish a national infrastructure for AI that includes access to computing power and language models that are adapted to Norwegian and Sámi languages and Norwegian social conditions.

Supercomputers constitute a necessary infrastructure for the development of Norwegian AI. Immense computing power is required to train foundational models that the business or public sector can then further develop to create and use AI tools for more efficient services and production.

The state-owned limited company Sigma2 AS is responsible for investing in and operating our largest national supercomputers. They do so in collaboration with the Research Council of Norway and universities in Bergen, Oslo, Tromsø and the Norwegian University of Science and Technology in Trondheim. In addition, Norway has access to supercomputers through the European High Performance Computing Joint Undertaking (Euro-HPC). In order to establish and train national models in the future, we need more specialised computing power in the form of supercomputers with graphics processors. On behalf of the Ministry of Education and Research, the Research Council of Norway has assessed the national need for this type of computing power and concluded that the need for computing power is vastly outpacing the supply. Therefore, the Government has commissioned the Research Council of Norway to investigate how much computing power Norway will need in the coming years, both that which must be established nationally and that which Norwegian enterprises can access through European cooperation.

Quantum computing technology offers new opportunities but also poses challenges for national and cyber security. The US Department of Homeland Security estimates that the first quantum computers will be able to crack current encryption technology in 2030. The potential of quantum technology has led several countries to establish national strategies for such technology. Therefore, the Government wants Norway to invest in R&D in this field.

Box 4.3 **Foundational models and major language models**

Foundational models consist of large neural networks trained on extensive general datasets, which can include text, images, sound, and more. These models serve as foundational elements for a variety of solutions.

Generative AI encompasses solutions that primarily generate, or produce, new material, such as text or images.

Large language models, such as the well-known GPT models, are a type of foundational model trained on vast amounts of text to predict the next word or syllable based on the given context. Language models do not store the text on which they were trained. They do not “know” anything about the world, nor do they review websites to find facts. They only know languages. However, one could easily be led to believe that these models think or possess knowledge, given how adept they are at generating text that humans perceive as meaningful.

The Norwegian public sector has vast amounts of data and text that can be useful for training Norwegian language models. Language models, and services based on these models, reflect the material they are trained on. To obtain models that work in the Norwegian language variants of Bokmål and Nynorsk, as well as the Sámi languages and Norwegian dialects, the models need to be trained on vast amounts of high-quality data. The models must also be adapted to Norwegian social conditions. Therefore, we need data from different domains reflecting the breadth of knowledge and experience in Norwegian society. It is necessary to investigate how these models can be used in a manner that safeguards security and privacy, and whether there are important datasets that are currently difficult to access that can be released for training purposes.

Since 2010, the National Library of Norway has been tasked with developing and offering basic resources for language technology in Norwegian via *Språkbanken* (the Norwegian Language Bank). The Sámi language technology centre *Divvun* works with Sámi language resources in collaboration with the Sámi Parliament of Norway. These resources will be used to ensure that people in Norway have access to high-quality AI tools based on Norwegian and Sámi languages and Norwegian social conditions.

It is important that the rights of creators of intellectual property and other protected works are respected and that general awareness of such rights is raised. This applies, for example, when training language models. Copyright law restricts the types of material that can be used to train such models. The implementation of the Digital Markets Act (DMA) will help clarify what constitutes lawful use of works in the training of language models.

Legislation and court rulings are unique to each country. The Norwegian judicial information site Lovdata will therefore be key to a number of Norwegian AI applications, not least in the public sector. AI based on Lovdata can be important for law enforcement and for decision-making support when issuing individual decisions.

If we are to realise the potential of AI, it is important that both the public and business sectors dare to test and adopt AI quickly. This requires access to relevant data, the right skills, leadership and a willingness to take risks. Good knowledge of the legislation governing the use of AI is also important. Regulatory sandboxes, such as the Norwegian Data Protection Authority's sandbox for privacy-friendly innovation and digitalisation, and the digital innovation hubs Nemonoor and Oceanopolis, enable experimentation with new AI solutions.

The Government is increasing grants for AI research by NOK 200 million each year for the next five years.[117] These funds are in addition to the approximately NOK 850 million allocated to research on AI and robotics through the Research Council of Norway. Such an investment is important because it helps to put Norway in a position to play a role in AI. The research must be connected to practical development work to ensure it impacts various areas of application.

The health and care services sector has a great deal of information that can be useful for developing AI, such as registry data, medical imagery and patient records. It must become easier for relevant actors to access health data to use it with AI. Improved and easier access to health data is important for the further development of our common health service, and for research and business development, but national security interests must be protected.[118]

The principles for ethical and responsible AI may appear general, and it can be difficult for individual enterprises to apply them in practice in their own projects. The Norwegian Digitalisation Agency has prepared a guide for the ethical and responsible use of AI. The Agency's guidance efforts will be further developed and strengthened in the future. The Government will set a requirement in the Digitalisation Circular for all government agencies to adhere to principles for ethical and responsible AI when adopting AI solutions.

In 2024, the EU adopted a regulation on AI (the AI Act). The Act is EEA-relevant. It is first and foremost a product liability act designed to ensure that products and systems utilising AI are safe to use. The AI Act classifies AI systems according to the risk they pose to society and individuals. Most AI systems in use today are not regulated by the AI Act, but must nevertheless be in accordance with other legislation. The Act requires Member States to have administrative and supervisory structures in place to enforce the Act. Although the majority of AI systems in use today are not high-risk according to the Act, several future systems may be classified as high-risk AI. Thus, the Act will provide the main framework for the future development of AI in Norway. This means that anyone seeking to develop and utilise AI will need comprehensive guidance.

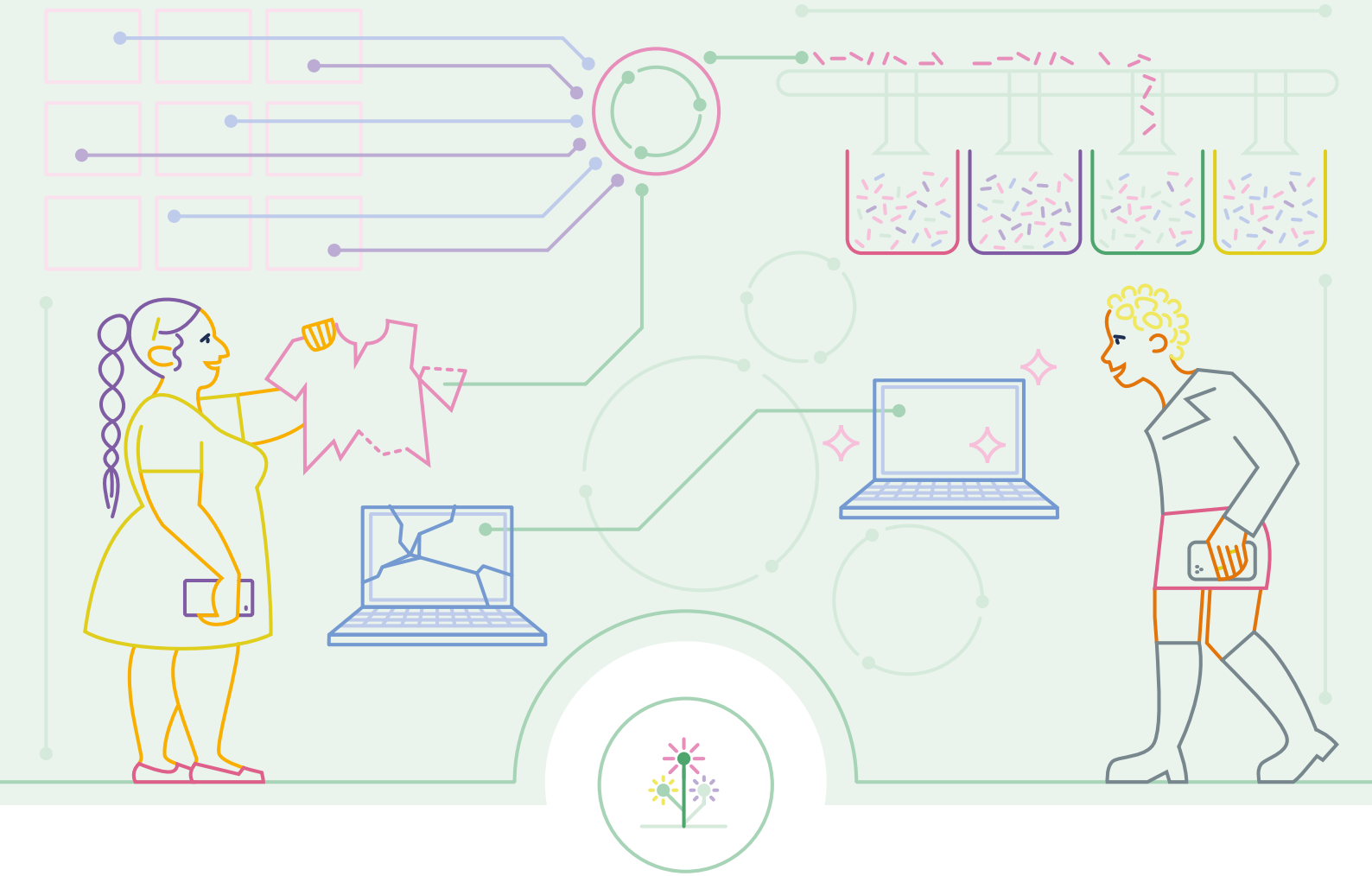
The Government will work to ensure that the AI Act is incorporated into the EEA Agreement as quickly as possible. In the national implementation of the Act, we will prioritise establishing a national supervisory and administrative structure.

We must also continuously assess whether changes are needed in the sectoral legislation as AI becomes more widespread in society.

Norway will take an active role in important international efforts on the ethical and responsible development and use of AI. Norway works with the EU, the Nordic Council of Ministers, the UN, the OECD and the Council of Europe to ensure that our values influence international developments in this important area.

THE GOVERNMENT WILL

- Ensure that 80 per cent of government agencies have adopted AI in 2025, and 100 per cent by 2030
- Work to further develop a national infrastructure for AI that will provide access to foundational models based on Norwegian and Sámi languages and social conditions
- Investigate the need for high-performance computing based on known needs in the research sector, public and business sectors
- Implement the AI Act into Norwegian law
- Establish a national supervisory and administrative structure for AI
- Implement changes to sectoral legislation due to the widespread adoption of AI in society
- Investigate how to use data and text from government agencies for ethical and safe training of national language models
- Clarify what constitutes the lawful use of copyright and other protected works in text and data mining processes
- Investigate whether the data basis in Lovdata can be made available, including for the training of language models
- Strengthen the guidance work for the responsible development and use of AI, including through regulatory sandboxes
- Ensure responsible development and use of AI in the public sector
- Contribute to better and easier access to health data and the use of AI for the further development of our common health service, research and business development
- Facilitate innovation based on AI in the business sector through the business-oriented policy instrument system
- Ensure that Norway takes an active role internationally to influence the development of legislation in the field of AI especially in terms of the ethical and safe use of AI
- Establish research centres for the development and use of AI in society
- Strengthen quantum technology research



4.3 Accelerating the green and digital transitions

Goals

In the lead-up to 2030, the Government will facilitate the green and digital transitions of the business sector.

STATUS

The green transition is the greatest challenge of our time. The global climate, pollution and environmental crises must be addressed with changes in all parts of society. The consumption of resources exceeds global capacity. Continued economic development presupposes that resource consumption is kept within the planet's tolerance levels. Europe is in the process of transitioning to a more circular economy with lower resource consumption and increased sustainability in all parts of the economy. This transition requires extensive digitalisation.

Norway's climate goals for 2030 under the Paris Agreement is to reduce our greenhouse gas emissions by at least 55 per cent compared to 1990 levels. This is enshrined in the Climate Change Act. Climate policy shall be regularly presented in climate reports to the Storting, and presented annually at the same time as the National Budget in the climate status and plan (green book).[119]

In 2022, the states parties to the Convention on Biological Diversity agreed on a new global framework for nature. The framework sets concrete global goals to protect nature, achieve sustainable management and combat the causes of degradation and destruction of ecosystems. To follow up on the new framework, the Government will present an action plan for nature to the Storting in 2024, which will include Norway's contribution to the global nature goals.

AI, and the training and use of large generative models, consume a lot of energy. It is possible to make such models more sustainable and climate-friendly, for example by designing more compact and energy-efficient architectures, using data centres powered by renewable energy, and not making the models larger than necessary for their purpose. The Government will emphasise the development and use of the most climate-friendly AI possible, and support research into climate-friendly AI models through the Research Council of Norway.

Box 4.4 **Examples of how AI can contribute to a green transition**

- Energy consumption and efficiency: AI can optimise energy consumption in buildings, factories and data centres.
- Environmental monitoring and protection: AI can assist in environmental monitoring, such as tracking air and water quality.
- Sustainable transport: AI can be used to optimise traffic flow, reduce congestion and thereby minimise emissions. In many cases, autonomous (self-driving) vehicles equipped with AI will be more energy efficient than traditional vehicles.
- Agriculture and food security: AI can improve crop monitoring, optimise irrigation and reduce the use of pesticides.
- Circular economy: AI can improve the recognition of recyclable materials and optimise waste management.
- Climate modelling and forecasting: AI can help us understand climate change and predict extreme weather events. AI can also contribute to the development of sustainable solutions to address climate challenges.

Digitalisation can contribute to the green transition. In order to transition to a more circular economy involving more resource-efficient and sustainable production and consumption patterns, we need to accelerate both the green and digital[120] transitions. In this context, investing in research, development and innovation in the business and public sectors, as well as society as a whole is key.

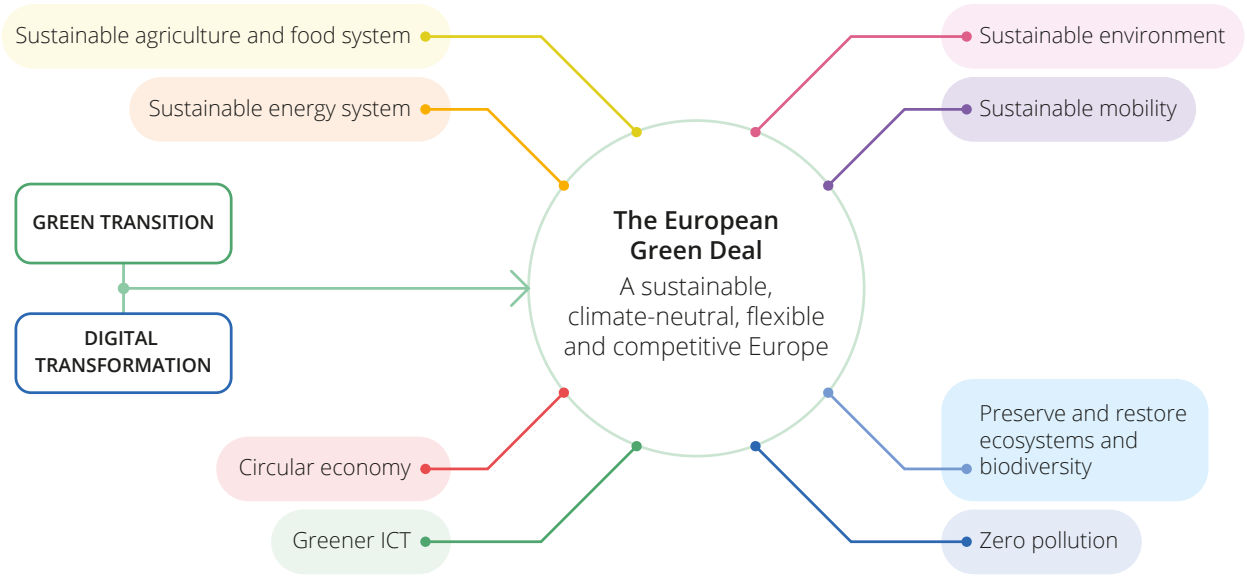
However, it is a dilemma that IT equipment, data centres and digital networks already account for around ten per cent of global energy consumption, and that the production of energy is the largest source of emissions, globally. Energy consumption for information and communication technology is growing eight times faster than global energy production.[121] The widespread use of technology and digital services and the frequent replacement of equipment reinforce this trend.

The generation of electrical and electronic waste (EE waste) is a challenge for Norway. Since 2016, Norway has unfortunately ranked as the leading OECD country in terms of EE waste generation per capita. Although a return scheme for electrical and electronic (EE) products has been established, Norway remains one of the Nordic countries that generate the most EE waste per capita while recycling too little.[122]

CHARTING THE COURSE TOWARDS 2030

The EU's February 2020 digitalisation strategy highlights the need for the digital and green transitions to mutually reinforce each other. One of the most important ways to promote both transitions is to move to a circular economy. Digitalisation and the use of new technology, with better utilisation of data, are key to achieving the goal of a climate-neutral Europe by 2050. The EU will create a separate data space[123] for the European Green Deal (see Figure 4.1.). This data space will harness the potential of data that supports the goals of EU climate policy. This encompasses the shift to a circular economy, achieving net-zero emissions, conserving biodiversity, curbing deforestation, and tracking the progress of implemented measures.

Figure 4.1 **The green and digital transitions as part of the same transformation**[124]



The transition to a circular economy is highly prioritised, and in 2024, the Government presented an action plan for a circular economy.[125] As stated in the action plan, the European regulatory framework is undergoing an extensive period of reform to transition to a circular economy as a means of achieving the objectives of the European Green Deal. A strengthened product framework is one of the most important measures in this regard. The framework contains two key and complementary measures.

One is the *Ecodesign for Sustainable Products Regulation*. With few exceptions, all products in the internal market must fulfil new and stricter requirements

for sustainable characteristics that make the products best suited to a circular economy. For example, the new proposal for a regulation on batteries sets extensive requirements for documentation of, among other things, production conditions, quality, utilisation properties and waste management that must accompany the battery in the form of a *Digital Product Passport*.

The second key measure is a *value chain-based approach to a circular economy* in seven main product categories. The overarching goal is to reduce the overall pressure on the natural resource base. In order to be able to implement a new regulatory framework in this area, the Government has submitted a proposal for a Sustainable Products Act to the Storting.[126] In addition, Norway will actively participate in the further development of EEA-relevant joint European solutions for regulation and control.

Box 4.5 **Information and product passport requirements**

The proposal for a new Ecodesign for Sustainable Products Regulation includes a requirement for the mandatory adoption of Digital Product Passports for products regulated in delegated acts under the Regulation. This will enable actors throughout the product value chain, as well as consumers, to make more informed choices. In addition, the work of supervisory authorities is simplified. Digital Product Passports will facilitate easier repairs, reuse and material recycling. In conjunction with border control regulations and digital information exchange tools, product passports will represent a key policy instrument for ensuring compliance with environmental requirements.

Digitalisation enables a more sustainable society. In collaboration with the Ministry of Digitalisation and Public Governance, the Norwegian Communications Authority is conducting a comprehensive analysis of how digital network infrastructure impacts climate and nature. The analysis, which is due in early 2025, will include the current status and expected developments towards 2030 and 2050 and could form the basis for an annual sustainability index. The analysis and an annual index will provide a common, knowledge-based reference for goals and possible measures, policy instruments and industry agreements to reduce the footprint of digital network infrastructure and improve sustainability in other sectors.

The public sector procures products and services worth approximately NOK 740 billion a year [127] An investigation by the National Audit Office of Norway[128] has revealed that the public sector does not make sufficient use of its purchasing power to minimise environmental impact and promote innovation and climate-friendly solutions. Green and innovative procurement will be adopted as a strategic tool to facilitate the green transition of the business sector. Climate and the environment shall be weighted at least 30 per cent in public procurement processes.

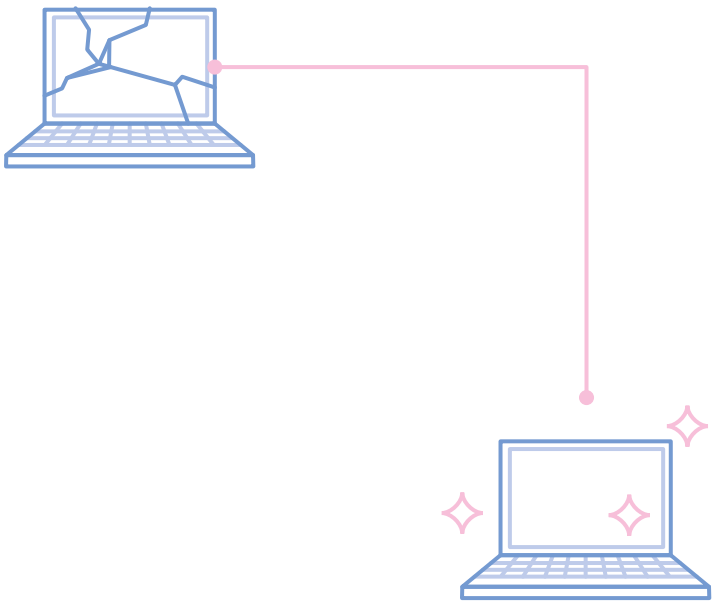
Through the roadmap for a green industrial boost,[129] the Government will aid the Norwegian business sector's transition to a low-emission society, create attractive

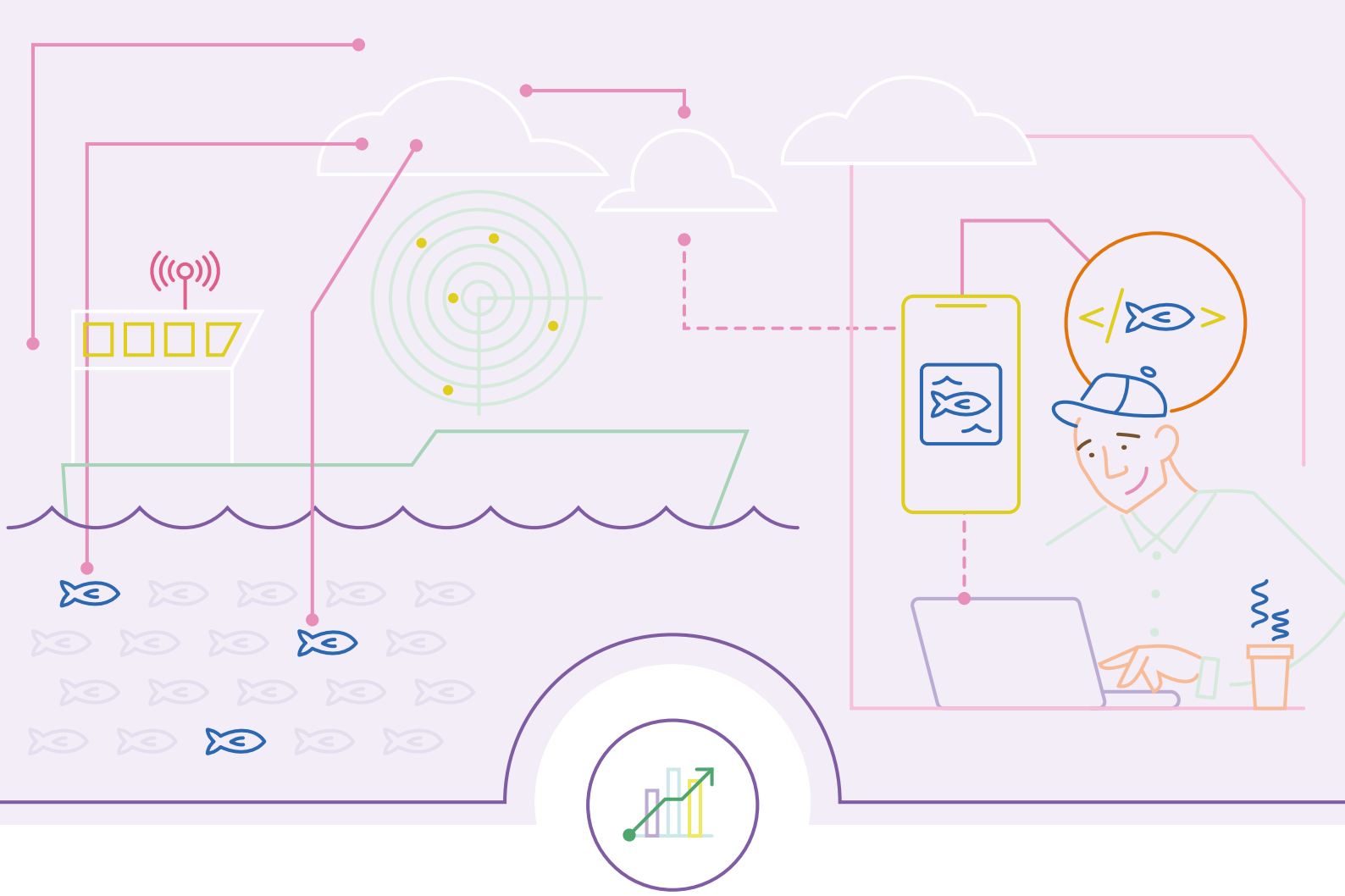
jobs for the future, increase exports from the mainland and reduce the vulnerability of key supply chains for the green transition. Norway and the EU have established a Green Alliance.[130] One result of this alliance is an industrial partnership on sustainable value chains for batteries and land-based raw materials that was signed on 21 March 2024.

Data on nature, climate and the cultural environment is the cornerstone of knowledge-based and comprehensive land-use management. The digital transition includes improving access to and utilisation of such data. Among other things, this will help us achieve the goals of preventing incidents related to extreme weather events, better land-use planning and rehabilitation of water and wastewater solutions. Strengthened public-private collaboration on the sharing of relevant data will be important in this regard.

THE GOVERNMENT WILL

- Ensure that Norway participates in the development of EEA-relevant common European solutions for regulation and control for the transition to a circular economy
- Increase the use of green and innovative procurement where digital solutions contribute to sustainable products and services
- Follow up on measures in the Roadmap for the green industrial initiative
- Strengthen public-private collaboration on sharing and making available data related to climate and the environment
- Develop a strategy for the green and digital transition in Norway





4.4 Promote an adaptable and innovative business sector

Goals

In the run-up to 2030, the Government will facilitate the strengthening of the business sector's competitiveness through the innovative use of data and digitalisation. The conditions for start-up enterprises shall be favourable. We shall ensure that digitalisation and the use of data reinforce our advantages in key industries, such as health, energy, aquaculture and other maritime industries.

We shall prioritise lifelong learning offerings in areas that are necessary for the future business sector.

STATUS

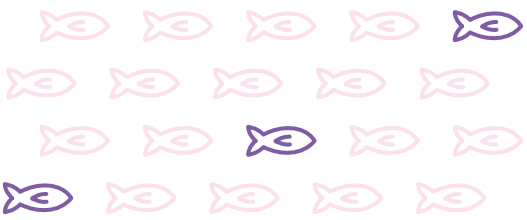
Productivity in Norway is high, but productivity growth has declined over time.[131] Harnessing the potential of innovation and digitalisation is crucial to realising opportunities for increased productivity and value creation, developing new business opportunities and gaining access to new markets. Access to relevant skills and uncertainty regarding future economic benefits are examples of the challenges the business sector is facing.

The Norwegian Directorate for Higher Education and Skills has noted that there will be a significant need for education and skills related to ICT and digitalisation in the future.[132] This is also supported by surveys from interest organisations such as Abelia and the Confederation of Norwegian Enterprise.

Report to the Storting No. 14 (2022-2023) *Outlook on the skills needs in Norway* highlights the labour market's skills needs in the short and long term. Necessary skills for a highly productive and competitive business sector is one of the Government's priority areas for education and skills policy going forward. The Government wants to ensure that the education authorities maintain a good and continuous dialogue with the business sector regarding the need for ICT skills at both the national and regional levels.

Some of the Government's policy instruments for skills development are described in section 3.5 of the strategy. In the work on developing a skills policy, the Government is collaborating extensively with the social partners, including via the Skills Policy Council, the Committee on Future Skills Needs and the Committee on Skills Reform in the Labour Market (Skills Reform Committee). The report *Outlook on the skills needs in Norway* notes that employees in SMEs are less involved in skills development measures than employees in larger enterprises. The Norwegian business sector is characterised by many SMEs, which means that Norway has different challenges and opportunities than many other countries. The Skills Reform Committee will examine opportunities and policy instruments for learning in working life in Norway, based on the prevailing conditions in the Norwegian business sector.

In May 2022, the Expert Group on Industrial Data Sharing submitted its report on data sharing between Norwegian industry actors.[133] The Ministry of Digitalisation and Public Governance has commissioned Digital Norway to better facilitate the sharing of industrial data.



Box 4.6 **Digital Norway**

Toppindustrisenteret AS – Digital Norway is a member organisation established in 2017 by 15 industry actors. Digital Norway is a non-profit organisation, and its funding is largely based on membership fees from a few larger companies, support from the public sector, as well as project funding. Digital Norway's purpose is to promote the digitalisation of the Norwegian business sector and industry, with an emphasis on SMEs. Digital Norway works to ensure that enterprises and employees have access to the knowledge and networks they need in a digital world by offering free courses, learning expeditions, webinars and digital meeting places.

Digital Norway and Microsoft Norway are collaborating with the Norwegian Confederation of Trade Unions and the Confederation of Norwegian Enterprise on a nationwide "AI tour" with the course "AI ABC", where Norwegian enterprises receive a primer on AI and how it can be utilised. Digital Norway also works with information and courses in a number of areas, including sustainability, cyber security, data and privacy.

The Ministry of Digitalisation and Public Governance is a strategic member of Digital Norway through a separate cooperation agreement. In addition, Digital Norway receives a grant from the Ministry to increase the understanding and speed of sharing and use of industrial data among enterprises in different industries and sectors. Digital Norway also participates in the secretariat of the 5G Industry Forum.

Norway participates in the EU's Digital Europe (DIGITAL) programme 2021-2027 [134] The DIGITAL programme represents a joint effort to increase the competitiveness of European enterprises, ensure better and more efficient solutions for the public sector, provide the basis for a green transition and ensure Europe's digital security and sovereignty.

One of the measures in the DIGITAL programme is the establishment of the European Digital Innovation Hubs Network (EDIHs). The Government considers this to be a key initiative for the future competitiveness of Norwegian enterprises and has therefore set aside funds to co-finance the two Norwegian innovation hubs. The national co-financing triggers a corresponding amount from the DIGITAL programme. Thus, the opportunities offered by the programme are leveraged to generate far greater activity than would have been possible without Norway's participation.

Box 4.7 **Digital Innovation Hubs (EDIHs) in Norway**

Nemonoor and *Oceanopolis* are national digital innovation hubs in the European Digital Innovation Hubs Network (EDIHs). They will aid enterprises in upgrading their business models, processes, products and services using innovative digital technologies. The aim is to boost the productivity and competitiveness of the enterprises. With the "Test before you invest" service, enterprises can trial new technologies risk-free. In addition, the hubs offer mentorship and technical expertise, financial guidance, training and skills development, which are all essential tools for a successful digital transition.

AI and machine learning can help increase productivity in the business sector by automating working methods and processes that were previously regarded as "knowledge work".[135] According to figures from Statistics Norway's survey *ICT usage in enterprises* (2023), access to skills is the most significant barrier to the use of AI in the business sector.[136] Figures from Economics Norway in report 23/2023[137] support this finding, showing that only a quarter of Norwegian enterprises used AI in 2023 and just under half of these had a strategic approach to its use.

The Government has presented a strategy to encourage the business sector to invest more in R&D.[138] The business sector is key to the success of the digital and green transitions. It is in the business sector, in close collaboration with the research environments, that the new sustainable and value-creating solutions will be developed and adopted nationwide. More R&D in the business sector can result in new technology and new solutions. In addition, it promotes society's ability to adopt and benefit from new technology. There is considerable potential in utilising and making public data available for both R&D and business development purposes. This is also important in the EU, where health data and the European Health Data Space are good examples of how public data can be made available for use in the business sector.

Deep technologies (deep tech) are technologies such as AI, autonomous systems, robotics and quantum systems. They represent opportunities for innovation for both society and the business sector. A report prepared by Economics Norway for the Confederation of Norwegian Enterprise (NHO) and others [139] emphasises that rapid implementation of advanced technology, including AI, can result in a significant increase in business value creation.

The technology industry has called for a separate business-oriented plan for actors working with deep tech, i.e., technologies that are based on scientific breakthroughs and groundbreaking innovations. The technology-based business sector consists of enterprises that utilise advanced technology in the production, distribution or organisation of their own business or business model. These are enterprises that stand to achieve significant gains through a successful transformation based on leveraging new and enabling technologies, but they also risk becoming competitively vulnerable if they fail to successfully navigate the technological shift.

CHARTING THE COURSE TOWARDS 2030

The Norwegian business sector has significant potential for business development through the use of digitalisation and technology.[140] Strong industries such as healthcare, energy, aquaculture and other maritime industries possess significant amounts of data that are of a high enough quality to form the basis for major new export opportunities. This presupposes that enterprises have the capacity and ability to utilise the potential. However, many enterprises, particularly in the SME segment, have limited resources to do so.

The business sector has clearly expressed the importance of recruiting skilled labour and specialists, including those from outside the EEA, to meet the need for ICT skills. The skilled worker quota was introduced in 2002 and determines the number of work permits that can be granted each year following a simplified procedure. It ensures that employers can quickly and easily recruit necessary expertise from countries outside the EEA. The need to adjust the quota is continuously assessed.

The enabling and deep technologies represent a technological shift that creates many opportunities for both society and the business sector. Through a roadmap, the Government is seeking to help the business sector better utilise these opportunities.[141] The roadmap will provide a good understanding of what the industry needs in terms of framework conditions and skills in order to utilise advanced technology.

Currently, data constitutes an increasingly large share of value creation across most Norwegian industries and sectors. However, the business sector must improve its ability to leverage data and enhance data sharing between actors.[142] The Government's ambition is to enhance data sharing both within the business sector and between the public and private sectors. Improved leveraging of data is crucial for Norway to succeed in the transition to a more sustainable society, a highly productive industry and a greener economy.

It is first and foremost the responsibility of enterprises to leverage the opportunities and manage the challenges arising from technological development and the green transition. However, the scale of the effort required is such that the central government must also become more involved through an active and ambitious industrial and business policy in collaboration with enterprises.[143]

The Government wants to provide the business sector, entrepreneurs and start-ups with better framework conditions and conditions for growth. This involves taking measures to simplify and identify good digital solutions between enterprises and the public sector. The Government will present the first white paper on entrepreneurs and start-ups. The report will present the Government's overall entrepreneurial policy.

To realise the green industrial initiative, Norwegian industrial enterprises must adopt new technology and data. In the *Roadmap for the green industrial initiative*,

which the Government launched in 2022, one of the measures is to facilitate greater value creation with data by stimulating increased sharing and use of data in and across sectors, industries and trades.

Although digitalisation is widespread among Norwegian enterprises, the level of investment in digitalisation is insufficient compared to other countries.[144] In Innovation Norway's experience, start-ups with digital business models find it difficult to raise private capital because they are often considered to have low collateral security.[145] To stimulate digital innovation in the business sector, especially for start-ups, it should be considered whether loan and grant schemes can increasingly be geared towards risk mitigation.

Box 4.8 **Seed funding – Investinor**

A seed fund is an active ownership fund consisting of both central government and private capital that invests in innovative enterprises with high-value creation potential nationwide. The funds have significant financial leverage and will contribute to the long-term development of the enterprises.

Investinor invests venture capital in some of the most promising enterprises in its market. Investinor can make direct investments in enterprises, invest in seed and venture funds, co-invest with private investors in seed and venture stage companies and make pre-seed investments in funds or via matching. Investinor manages the central government's interests in the seed fund and pre-seed scheme.

The business-oriented policy instrument system consists of institutions and schemes that directly and indirectly stimulate increased value creation in the business sector through capital, research, infrastructure and skills measures. Work is underway to strengthen the policy instrument system through *Virkemiddelapparatet 2.0* [Policy Instrument System 2.0]. The purpose of this work is to make the policy instrument system more accessible, simpler and more user-friendly. Public authorities facilitate both research and innovation through grants, loans, guarantees, advice and skills measures that are managed by the overall national and regional policy instrument system.

Norwegian actors must be able to make the best possible use of the link between national and international instruments. This applies both to the value chain from basic knowledge to commercial activities within each individual field and to interfaces between national initiatives and the international initiatives in which Norway participates. This requires sufficient information, active and broad mobilisation and targeted coordination at the ministry and agency level.

Tripartite industry programmes for skills development[146] develop short and flexible continuing education courses that people can take alongside their jobs. Industry programmes exist in five industries, and it is the social partners who identify the

type of skills needed by the industries. In 2023, a separate industry programme for information security and ICT was established to ensure that employees in the industry have up-to-date knowledge. The industry programme for skills development will be further developed.

Large sums are allocated annually to research, development and piloting related to ICT and digitalisation at both the national and European levels. For investments to pay off, it is important that the results can lead to testing, implementation and scaling. This requires sufficient infrastructure and capacity, both nationally and through international cooperation.

The EU's Digital Decade policy programme 2030[147] establishes concrete goals for a successful digital transformation. Among other things, three out of four enterprises are to utilise cloud services, big data and AI by 2030. More than 90 per cent of SMEs are to adopt foundational digital technologies, and the number of *unicorn companies* in the EU (start-ups with a valuation of USD 1 billion or more) will be doubled.

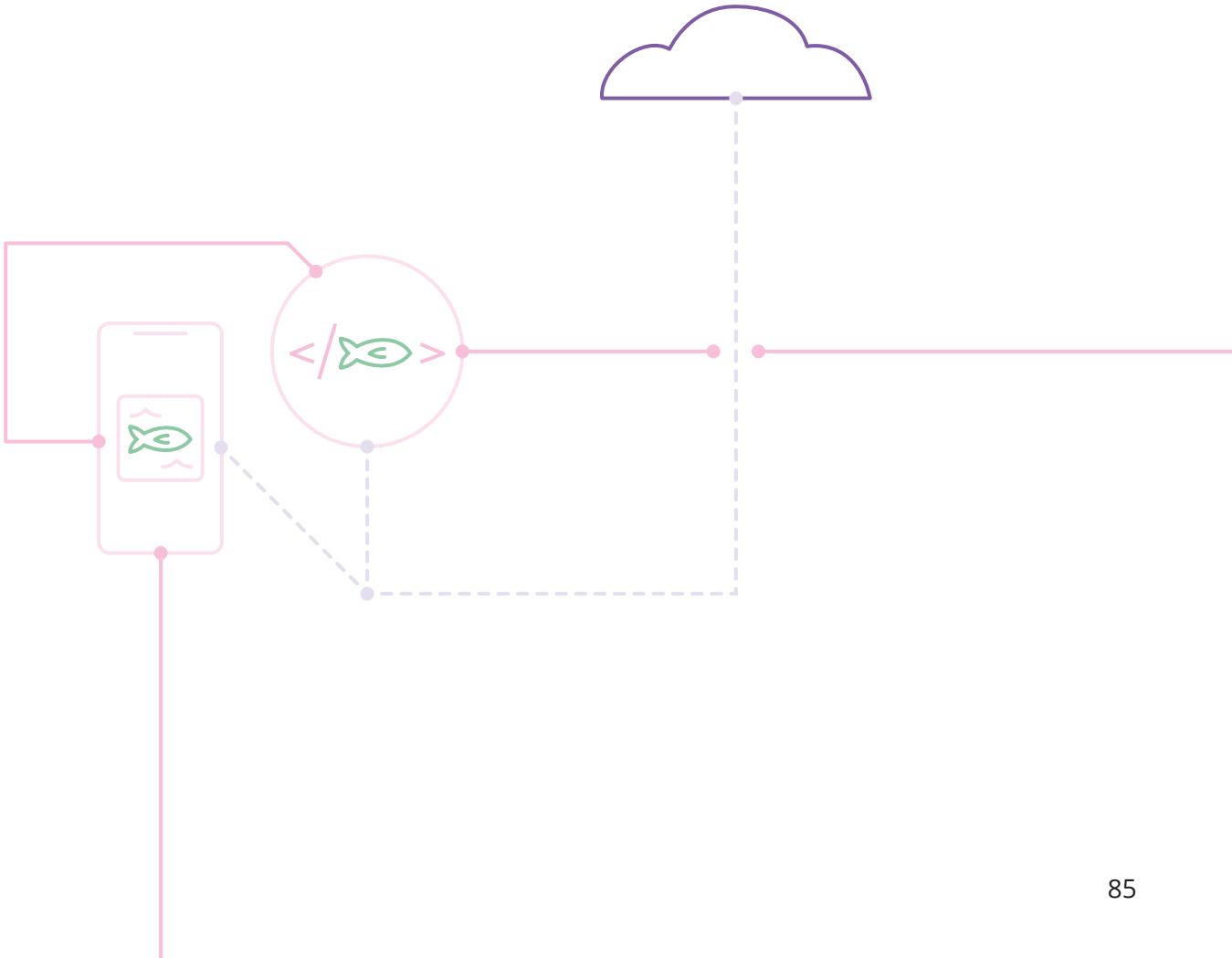
In the strategy for Norwegian participation in DIGITAL[148], the Government wants the programme to be a tool for implementing the digital transition we are currently facing. Norway must accomplish this by utilising opportunities for financial support, access to knowledge, professional networks and access to capacity and infrastructure. We must utilise the opportunities for synergies between the EU's digital policy and developments in Norway to digitally transform enterprises, utilise enabling technologies and increase business development.

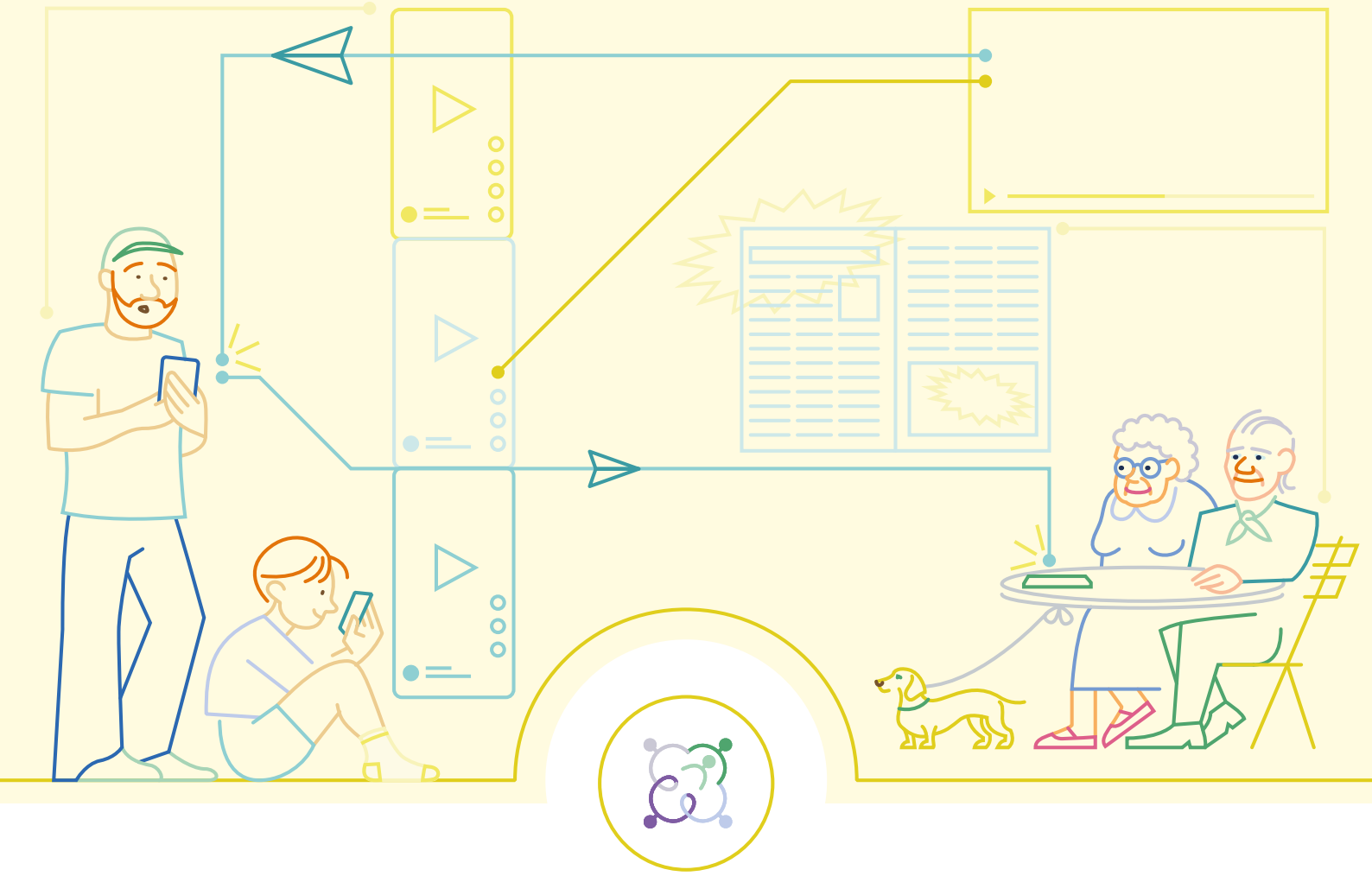
The fourth industrial revolution (Industry 4.0) involves the increased digitalisation of industrial systems. Advanced algorithms, machine learning and AI are used to increase productivity, raise quality and improve the adaptability of industrial systems. Industry 5.0 advances this concept by incorporating climate and environmental considerations into industrial automation and including employees' skills and work situations as prerequisites for realising the benefits of advanced digital technologies.

Through business networks, SMEs can establish targeted, commercial and market-oriented collaborations to strengthen their innovative capacity and competitiveness. The goal is to achieve growth and value creation in the participating enterprises through the realisation of new market opportunities. The work of the business networks should be structured in such a manner that they contribute to increased innovation with the use of ICT in SMEs.

THE GOVERNMENT WILL

- Fulfil the business sector's need for digital competence through stronger collaboration between relevant educational institutions, the business sector, policy instrument actors and the social partners
- Present a roadmap for the technology-based business sector
- Present a white paper on entrepreneurs and start-ups
- Consider whether loan and grant schemes can be geared more towards risk mitigation to stimulate digital innovation in the business sector, especially for start-ups
- Further develop tripartite industry programmes for skills development
- Facilitate increased participation by the business sector in EU programmes for research, innovation, development and implementation related to ICT
- Continue co-funding for the Digital Innovation Hubs Network (EDIH) under the DIGITAL programme
- Assess whether the policy instruments are appropriately structured to support the digital transition of the business sector
- Hold the business sector's industry trade groups accountable to ensure that they better facilitate collaboration on the digitalisation of value chains and data sharing





4.5 Maintaining trust, strengthening inclusion, and safeguarding considerations for children and young people

Goals

Towards 2030, the Government will ensure that everyone can take part in digitalisation. We will strengthen our efforts to increase the digital competence of those groups experiencing digital barriers and digital exclusion. We shall make sure that everyone is offered an electronic identity. We shall strengthen the population's resilience to digital disinformation. Children and young people shall be ensured a safe digital upbringing. We shall ensure a good digital-analogue balance in kindergartens, schools and in the leisure time of children and young people.

4.5.1 Maintaining a strong and inclusive democracy with a high level of trust

STATUS

In Norway, citizens have a high level of trust in one another, the authorities and democracy. This high level of trust enables simple, fast and smooth processes and minimises conflict. It can also be an advantage in the digitalisation of society and the public sector. For public trust to remain high, digital solutions must be accessible, user-friendly and of high quality.

The highest possible level of trust is not an end in itself, and healthy scepticism is beneficial for any democracy. For example, it is important to build critical media literacy and develop a critical attitude toward information at a time when it can be more difficult to distinguish between true and false information.

Openness in the public administration is an important means of building citizens' trust. Norway is one of 70 member countries in the *Open Government Partnership* (OGP). The purpose of the partnership is to create a more open, well-functioning and user-friendly public administration.[149]

The Freedom of Expression Commission's report[150] describes how misinformation and disinformation can pose a threat to democracy and trust in society, and how the free formation of opinion requires access to reliable information. It is easier than ever to spread misleading or false information to a larger audience.

The amount of information from different sources places even greater demands on the public's ability to critically assess whether they believe and trust the information they receive online. If people can no longer distinguish between fact and fiction, this poses a serious threat to freedom of expression. The Freedom of Expression Commission concluded that Norway is relatively well-equipped to handle these challenges. The political culture is not particularly polarised, we have a robust and trusted media system, and the population's critical understanding of the media is at a high level. However, the extent of disinformation that has been uncovered in several countries and the rapid technological developments give cause for concern and increased vigilance.

Internationally, there have been several examples of digital influence campaigns in connection with elections. The Government has established an inter-ministerial working group to strengthen resilience against unwanted actions in Norwegian elections. Ahead of each election, the working group has presented its action plans for how society can build resilience against unwanted influence in connection with elections. As part of this effort, an assessment is made to determine whether there are attempts at unwanted foreign influence related to the election. To date, the assessments have not revealed any signs that foreign actors have attempted to influence Norwegian elections.[151] The Norwegian National Election Studies[152] provide a basis for understanding how resilience to disinformation and unwanted influence during elections and election campaigns can be strengthened.

Spreading disinformation and influencing elections on social media can pose a threat to public discourse and trust in society. The Digital Services Act (DSA)[153] imposes requirements on major social media platforms to implement measures that limit the risk of election influence and the spread of disinformation and harmful content aimed at children. These measures are to be weighed against freedom of expression.

CHARTING THE COURSE TOWARDS 2030

Digitalisation in Norway must take place within a secure framework to preserve trust in our democracy.

The Government wants to ensure that people are aware when content has been generated by AI. The AI Act includes rules on the labelling of AI-generated content. The Act stipulates that if AI is used to generate content that can be perceived as being an existing person, place or event, this must be clearly labelled.

The Freedom of Expression Commission notes that social media algorithms amplify the spread of engaging content, which will often be favourable to those seeking to disseminate false information. It is expected that AI will accelerate this development. The volume of information also places greater demands on the public's ability to critically assess the information they receive online.

As part of the follow-up to the Freedom of Expression Commission, the Government will present a strategy to strengthen resilience against disinformation in the spring of 2025.[154] Among other things, the strategy will address how we can safeguard and strengthen the editor-controlled media's important social mission, how we can enhance the population's critical understanding of the media, how we can ensure vigorous follow-up of the big tech companies and their influence on Norwegian discourse, and how we can obtain and share knowledge about disinformation and influence in Norway.

The Government has started work on a national strategy for an open and informed public discourse.[155] The strategy will account for the Government's efforts to fulfil the *infrastructure requirement*, including how to facilitate a well-functioning space for expression, a good culture of expression, and emergency preparedness for expression among citizens. The work will be based on the Freedom of Expression Commission's report and the subsequent extensive public consultation.

Knowledge of democracy and citizenship and critical media literacy are particularly important for children and young people. Children are less able to evaluate content and are more likely to consume media that lacks editorial oversight. The Norwegian Association of Local and Regional Authorities is working on initiatives aimed at young people aged 16-19. In cooperation with the Norwegian Association of Local and Regional Authorities, the Government will contribute to enhancing knowledge about democracy and citizenship among young people.

The Government has established a fast-working expert group tasked with assessing the consequences of AI for secure and democratic elections.[156] The expert group will gather experiences from the 2024 elections, with a particular focus on how AI changes the existing challenges and will provide a knowledge status and present concrete proposals to the Government on possible measures that can be implemented before the 2025 parliamentary elections.

New technology, including AI, also provides new opportunities. In the coming years, it will be important to learn more about how the new technology can be used to strengthen democracy. For example, it will be important to learn more about whether authorities and politicians can use AI to make better decisions, whether AI can be used in citizen participation, and how it can help citizens receive better-adapted information about elections and democracy, rights, obligations and opportunities.

THE GOVERNMENT WILL

- Develop a strategy to strengthen resilience to disinformation
- Develop a strategy for an open and informed public discourse
- Strengthen young people's knowledge of democracy and citizenship, in cooperation with the Norwegian Association of Local and Regional Authorities
- Work to strengthen resilience against unwanted influence in connection with elections
- Consider recommendations from the expert group assessing the impact of AI on secure and democratic elections
- Increase citizen participation and provide a better basis for political decisions by utilising new technology

4.5.2 Include everyone in a digitalised society

STATUS

Norway has a digitally mature population. Most are online and have experience using digital services. However, some are unable to use digital services or do not want to use digital services, for various reasons. Based on existing figures, it is estimated that around 20 per cent of the adult population is vulnerable when using public digital services.[157]

A lack of digital competence, administrative skills, trust, and confidence are among the individual challenges that create barriers to the use of digital solutions. In addition, factors related to the solutions themselves, such as a lack of universal design, poor user interface, complexity, or a lack of cohesion, can hinder citizens from using them.[158]

The Norwegian Labour and Welfare Administration has investigated which services should be digitalised and how this should be carried out.[159] The report from the investigation notes that public services have different characteristics that may impact how well they are suited to digital solutions. Determining the extent of

digitalising public services and deciding what alternatives to provide those who are unable or unwilling to use digital services are dilemmas that necessitate further discussion and policy deliberations.

Box 4.9 **Key figures about digital users**

- 99 per cent of the population between the ages of 16 and 79 are online *(Statistics Norway)*.
- More than 90 per cent use email and online banking and read online newspapers *(Statistics Norway)*.
- 70 per cent have a positive view on using public digital services *(Norwegian Digitalisation Agency)*.
- 63 per cent have considerable experience using private and public digital services *(Norwegian Digitalisation Agency)*.
- 11 per cent (660,000 people) of those over the age of 16 have poor digital skills.
- 67 per cent need more digital skills in their daily and working lives (*Norwegian Directorate for Higher Education and Skills*).

In June 2023, the Government launched an *Action plan for increased inclusion in a digital society*.[160] The action plan aims to ensure that all citizens receive equal public services, regardless of background, language skills or age. The action plan primarily targets those groups that experience digital barriers and digital exclusion.

Box 4.10 **Digihjelpen**

Grants aimed at establishing *Digihjelpen* programmes in municipalities have been announced for several years. The Digihjelpen programme is a collaboration between the government and the Norwegian Association of Local and Regional Authorities. More than 100 municipalities have received financial support to establish a Digihjelpen programme. The Norwegian Association of Local and Regional Authorities offers advice and assistance to municipalities seeking to develop and establish a guidance service on basic digital competence for their citizens. This allows the persons responsible in the municipalities to find tips and advice on how to develop and establish a municipal guidance service: *www.digihjelpen.no*.

Box 4.11 **The libraries**

Libraries are part of society's digital resilience. Libraries provide guidance on online sources, real and fake news and how to distinguish between good and bad sources of knowledge. In addition to making knowledge sources accessible, libraries contribute to the active dissemination of research, knowledge and culture.

Public libraries contribute to promoting digital inclusion, including through guidance and training in basic digital skills for citizens with low digital competence.

Users must be included to a greater extent in the development of digital services. This also applies to services aimed at children and young people. A collaborative forum for digital inclusion has been established and is managed by the Norwegian Digitalisation Agency. The forum consists of representatives from the public sector, voluntary organisations and the business sector and works to facilitate equal public services, irrespective of digital skills.

AI may pose challenges for equality and non-discrimination, but can also be used to promote inclusion, for example through text reading, speech-to-text and audio description of images, and in programmes that support persons with dyslexia with writing. Good speech-to-text models, such as the National Library of Norway's NB-Whisper, can be used for subtitling videos.[161] Thereby, persons with disabilities or developmental challenges, or persons who otherwise require assistance with reading or writing, can receive effective assistance. In the future, AI will also be able to assist persons who do not speak Norwegian through written and oral translations from other languages.

CHARTING THE COURSE TOWARDS 2030

The public sector is making progress in digital inclusion; however, the efforts are not sufficiently coordinated. Strategies and action plans for inclusion and participation contain measures that cut across sectors and administrative levels. Efforts must be coordinated when implementing such measures.

Services should be developed based on standards for universal design, privacy by design and non-discrimination by design. It is also important to use more inclusive design and clear language in the development of digital services.

Good services with proximity to people are important for the Government. Therefore, we have invited municipalities with service centres or citizen service centres, and municipalities where citizens have to travel far to access user-facing government services, to apply to participate in a pilot for local service centres. The pilot will also include measures where the municipality assists citizens in using

digital public services. This involves assistance in navigating and using the digital services provided by e.g., the Norwegian Tax Administration and the Norwegian Labour and Welfare Administration.

All citizens must be able to use their eID safely and securely to participate in the digital society. Digital exclusion is exacerbated by technological barriers, such as the fact that not everyone has an eID, a lack of digital authorisation solutions and the fact that not all digital solutions are universally designed. The latter makes it difficult or impossible for persons with disabilities to participate in society, even if they possess good digital competence. Digital services must be universally designed in order to be accessible to all. In recent years, the Norwegian Authority for Universal Design of ICT has established a data-driven digital supervisory authority to effectively enforce the legislation. To ensure effective compliance and increased digital participation, the Norwegian Authority for Universal Design of ICT must be equipped to be future-oriented and data-driven.

In December 2022, a Declaration on Digital Rights and Principles was signed in the EU.[162] These digital rights and principles are intended to guide decision-makers, public authorities and enterprises when working with or developing new technology. To ensure that digital development continues in line with our societal values and for the benefit of citizens and enterprises in Norway, the Government will consider whether these or similar rights and principles should form the basis for digitalisation in Norway.

THE GOVERNMENT WILL

- Follow up on the action plan for increased inclusion in a digital society
- Strengthen efforts to increase the digital competence of older adults
- Strengthen the work on quality of use, clear language and universal design in public digital services
- Strengthen citizens' digital competence through the piloting of local service centres
- Ensure increased user involvement in the development of digital services
- Strengthen the Norwegian Authority for Universal Design of ICT

4.5.3 Ensure a safe digital upbringing for children and young people

STATUS

Children and young people's everyday lives are largely characterised by school, leisure and family life, entertainment, play, expression and learning through the use of the internet and digital tools. For children and young people, digital solutions can enhance their ability to express themselves and be heard, communicate with others, learn and explore the world and their individual identity. At the same time, they can challenge children's personal and consumer protection, mental and physical health, and the right to be protected from harmful content and abuse.

Children and young people are in a special legal position, both because they are generally dependent on caregivers making decisions on their behalf, and because children and young people have a special right to protection. Digitalisation efforts must therefore take into account that children face different challenges than adults on digital platforms. When following up on personal and consumer protection, it is also important to be aware of children's special legal position (Article 104 of the Constitution of Norway and the Convention on the Rights of the Child), and that they have different needs to adults.

We have little updated knowledge about children and young people's digital competence. A Consumption Research Norway study[163] has taken a closer look at how a sample of children and young people perceive their own digital competence and the need to develop it. Norway participates in the international comparative study *IEA International Computer and Information Literacy Study* (ICILS), which assesses pupils' digital competence. Data collection was completed in 2023, and the final report will be published in 2025.

Box 4.12 **Key figures on children and young people's digital use[164]**

- 93 per cent of 9–11-year-olds have a mobile phone. By the age of 12–14, nearly everyone has their own mobile phone.
- 64 per cent of 9–18-year-olds have their own PC or computer at home.
- 90 per cent of 9–18-year-olds are on social media (one or more).
- 7 out of 10 children and young people think they are exposed to too much advertising on social media.
- Approximately one in three social media users between the ages of 9 and 18 have regretted something they have shared on social media.
- More than 8 out of 10 children between the ages of 9 and 18 state that their parents are well aware of the social media they use.

The digitalised society is reflected in the challenges that today's children and young people face in their everyday lives, both in the physical and the digital world. The threat actors are not only people they know but also strangers who intend to exploit children and young people.

Together with the Norwegian Association of Local and Regional Authorities, the Government has drawn up a strategy for digital competence and infrastructure in kindergartens and schools.[165] The strategy aims to ensure that digitalisation in the sector is responsible, rooted in a sound knowledge base and that it is based on the best interests of children and young people, their rights and the precautionary principle. The strategy contains a number of measures, divided between central and local government, to be implemented towards 2030, including support for the local government sector to manage new technologies, digital tools in education and increased pressure on privacy.

CHARTING THE COURSE TOWARDS 2030

The Government is working on a white paper on safe digital upbringing. The report will contribute to a more comprehensive policy in the field and will cover both opportunities and challenges in the digital lives of children and young people. Online, children and young people can express themselves, actively participate in public debate, engage in creative expression and have social networks.

The report will address the risks faced by children and young people, such as exposure to harmful content, children and young people's digital competence, as well as the role of parents and caregivers in children's digital lives. It will also cover public services for children and young people online and the business sector's responsibility for the rights of the child. Furthermore, the report will cover the authorities' design of a comprehensive, knowledge-based policy for the digital upbringing of children and young people.

The Government has initiated a comprehensive review of children's consumer protection in digital media. The purpose is to assess cross-sectoral measures to strengthen children's consumer protection. In its report, the Privacy Commission identified particular challenges to children's privacy, which will be considered in the work on the white paper on safe digital upbringing.

The Government has appointed a committee to obtain more knowledge about how children and young people's screen use in kindergarten, school and leisure time affects their health, quality of life, learning and upbringing. Where the committee finds that particular challenges have been adequately documented, it will provide input for policy development and advise on measures. The committee's final recommendations will be submitted to the Ministry of Education and Research in the autumn of 2024.[166]

THE GOVERNMENT WILL

- Present a white paper on safe digital upbringing
- Follow up on the recommendations of the Screen Use Committee
- Take children and young people's rights into account when designing digital public services
- Consider age limits for social media

5

Economic and administrative consequences

The measures in the strategy will contribute to a sustainable welfare society that ensures a safe and simple everyday life for citizens and the voluntary sector, a competitive business sector and an improved public sector. In order to meet the challenges of the future, we need to leverage the opportunities presented by technology in a responsible manner.

The financial and administrative consequences of the measures in the strategy need to be assessed in greater detail. The starting point is that measures that may have economic consequences for the central government shall be covered within the prevailing budget frameworks of the affected ministries. Measures that require investigation shall be investigated in accordance with the Instructions for Official Studies of Central Government Measures and Circular R-109/21[167] on socioeconomic analyses. The economic consequences of the goals and measures in the strategy must be managed within the ordinary budget processes.

Increasing digitalisation in the public sector is occurring across sectors and administrative levels and in collaboration with the business sector. Therefore, the strategy particularly addresses cross-cutting issues. If we are to succeed with the strategy, all ministries must take an active role and responsibility for realising the stated ambitions. The strategy must be implemented in close collaboration with the business sector, the Norwegian Association of Local and Regional Authorities and the voluntary sector.

The strategy will be followed up through sectoral and thematic action plans to ensure good implementation. The progress and effect of the measures shall be measured. To achieve the vision, it will be necessary to update and concretise measures throughout the strategy period in line with developments in society.

Endnotes

1 Report to the Storting (white paper) No. 31 (2023 -2024). *Long-term Perspectives on the Norwegian Economy 2024*. Ministry of Finance.

2 OECD. *OECD Digital Government Index*.

3 Norwegian Communications Authority. *Brebåndsdekning* [Broadband coverage].

4 Statistics Norway. *Actions taken as a part of internal control for information security*

5 Statistics Norway. *Actions taken as a part of internal control for information security*

6 Norwegian Agency for Public and Financial Management. *The Norwegian Citizen Survey – Digitalisering i offentlig sektor* [Digitalisation of the public sector].

7 Statistics Norway. *Digitalisation and ICT in the public sector*

8 Nordic Institute for Studies in Innovation, Research and Education. (2023). *NHO's kompetansebarometer 2023* [The Confederation of Norwegian Enterprise Skills Barometer 2023]. nho.no

9 National Audit Office of Norway. 2024. *Document 3:18 (2023-2024) Use of Artificial Intelligence in the Central Government*.

10 Statistics Norway. *Use of ICT in the business sector*

11 OECD. (2024). *«Innovation» OECD Going Digital Toolkit.*

12 OECD. (2024). *ICT Access and Usage Databases*

13 OECD. *Unmanaged e-waste per capita*

14 BankID. *Om oss* [About us]

15 Norwegian Directorate for Higher Education and Skills. (2021). *Befolkningens digitale kompetanse og deltakelse* [Population digital competence and participation]

16 OECD. (2024). *Digital Government Index 2023*.

17 OECD. (2024). *Going Digital: Shaping Norway's Digital Future.* Regjeringen.no

18 The Norwegian Digitalisation Agency. (2023). *Noreg i verda* [Norway in the world]. Digdir.no

19 National Audit Office of Norway. (2023). *Document 3:8 (2023-2024) The National Audit Office of Norway's investigation of the authorities' facilitation of the sharing and reuse of data in public administration*. Riksrevisjonen.no

20 National Audit Office of Norway. (2023). *Document 3:8 (2023-2024) The National Audit Office of Norway's investigation of the authorities' facilitation of the sharing and reuse of data in public administration, Appendix Mapping of the development and use of artificial intelligence in the public administration and state-owned enterprises.* Riksrevisjonen.no

21 Rambøll Management Consulting AS. (2023). *IT i praksis for 2023* [IT in practice for 2023]. Digdir.no

22 Rambøll Management Consulting AS. (2023). *IT i praksis for 2023* [IT in practice for 2023]. Digdir.no

23 Norwegian Agency for Public and Financial Management. (2024). *The Norwegian Citizen Survey 2024*. Dfo.no

24 Norwegian National Security Authority. (2023). *Nasjonalt digitalt risikobilde 2023* [National Digital Risk Situation 2023]. Nsm.no

25 OECD. (2024). *The Digital Transformation of Norway's Public Sector*. Oecd.org

26 OECD. (2024). *Going Digital: Shaping Norway's Digital Future.* Regjeringen.no.

27 The Norwegian Digitalisation Agency. (2023). *Drivkrefter og teknologiske trender mot 2030* [Drivers and technological trends towards 2030]. Digdir.no

28 Ministry of Digitalisation and Public Governance. (2024). *Digitalisation Circular*. Regjeringen.no

29 Norwegian Official Report (NOU) 2023: No. 9 *System of Generalist Municipalities*. Ministry of Local Government and Regional Development

30 DSOP. *Digital Samhandling Offentlig Privat (DSOP)* [Public–Private Digital Cooperation (PPDC)]. Bits.no

31 National Audit Office of Norway. (2023). *Document 3:8 (2023-2024) The National Audit Office of Norway's investigation of the authorities' facilitation of the sharing and reuse of data in public administration*. Riksrevisjonen.no

32 Ministry of Finance. (2023). *Statsbudsjettet 2024 - Direktoratet for forvaltning og økonomistyring - tildelingsbrev* [National Budget 2024 – Norwegian Agency for Public and Financial Management – Letter of Allocation]. Dfo.no

[33] Kommunesektorens organisasjon [Norwegian Association of Local and Regional Authorities]. (2022). *Samstyringsstrukturen for digitaliseringsområdet* [The joint governance structure for digitalisation]. KS.no

[34] Analyses from the Ministry of Local Government and Regional Development (2023) based on figures from Rybalka, M., et al. (2023). *Digitalisering i kommunene. Utviklingen fra 2018 til 2022* [Digitalisation in the municipalities: Developments from 2018 to 2022]. Reports, Statistics Norway. 27: 1-39.

[35] The Norwegian Digitalisation Agency. (2021). *Samarbeid – ikke stafett* [Collaboration, not a relay race]. Digdir.no

[36] European Commission. *Europe's Digital Decade: digital targets for 2030*.

[37] Ministry of Digitalisation and Public Governance. (2024). *Strategi for norsk deltakelse i Programmet for et digitalt Europa – DIGITAL* [Strategy for Norwegian participation in the Digital Europe Programme (DIGITAL)]. Regjeringen.no

[38] Nordic Council of Ministers. *https://www.norden.org/no/digitalisering-og-innovasjon*.

[39] Norwegian Official Report (NOU) 2024: No. 7 *Norway and the EEA: Development and experiences. Ministry of Foreign Affairs*

[40] Norwegian Agency for Public and Financial Management. (2024). *The Norwegian Citizen Survey 2024: Nedgang i tillit og tilfredshet* [Decline in trust and satisfaction]. dfo.no

[41] Norwegian Agency for Public and Financial Management. (2024). *DFØ-rapport 2024:4 Oppleves offentlige tjenester som sammenhengende?* [Norwegian Agency for Public and Financial Management Report 2024:4 Are public services perceived as seamless?]. Dfo.no

[42] Ministry of Local Government and Modernisation. (2019). *One digital public sector: Digital strategy for the public sector 2019–2025*. Regjeringen.no

[43] Ministry of Digitalisation and Public Governance. (2024). *Digitalisation Circular 2024*, section 3.1.1. Regjeringen.no

[44] Ministry of Digitalisation and Public Governance. *Tillitsreformen* [The Trust Reform]. Regjeringen.no

[45] Report to the Storting (white paper) 6 (2023-2024). *Et forbedret pensjonssystem med en styrket sosial profil* [An improved pension system with a strengthened social profile]. Ministry of Labour and Social Inclusion.

[46] Ministry of Digitalisation and Public Governance. (2021). *Central Government Communication Policy*. Regjeringen.no

[47] Norwegian Directorate of Health et al. *Alvorlig sykt barn – Sluttrapport Stimulab 2021 m/vedlegg – vedlegg 4 Resultat av nullpunktsmålinger* [Seriously ill child – Final report Stimulab 2021 w/appendices – Appendix 4 Results of baseline measurements].

[48] Ministry of Local Government and Modernisation. (2019). *One digital public sector: Digital strategy for the public sector 2019–2025*. Regjeringen.no

[49] The Norwegian Digitalisation Agency and the Norwegian Agency for Public and Financial Management. (2024). *Oppdatert veileder om sammenhengende tjenester* [Updated guidance on seamless services]. Digdir.no

[50] Regulations *(EU) 2018/1724 of 2 October 2018 and (EU) 2020/1121 of 29 July 2020*.

[51] European Union. *Your Europe*. Europa.eu

[52] Report to the Storting (white paper) 9 (2023-2024). *Nasjonal helse- og samhandlingsplan 2024–2027 – Vår felles helsetjeneste* [National Health and Cooperation Plan 2024-2027 – Our Common Healthcare Service]. Ministry of Health and Care Services.

[53] The Norwegian Directorate of Health. (2023). *Status og forslag til videre arbeid med kunstig intelligens (KI) i helse- og omsorgstjenesten* [Status and proposals for further work on artificial intelligence (AI) in the health and care services]. Helsedirektoratet.no

[54] The Norwegian Directorate of Health. (2024). *Enklere tilgang på informasjon* [Easier access to information]. Procurement.no

[55] The National Program for Supplier Development *LUP sørger for at bedrifter og offentlig virksomheter sammen løser fremtidens utfordringer* [The National Program for Supplier Development ensures that companies and government agencies cooperate to solve the challenges of the future]. Innovativeanskaffelser.no

[56] The Financial Supervisory Authority of Norway. *Fraud and fraud statistics*. Finanstilsynet.no

[57] The Norwegian Police Service. *Beskytt deg mot svindel og ID-tyveri* [Protection yourself against fraud and identity theft]. Politiet.no

[58] The Norwegian Digitalisation Agency. *Felles økosystem* [Shared Ecosystem]. Digdir.no

[59] The Norwegian Digitalisation Agency. *Fellesløysningar* [Joint solutions]. Digdir.no

[60] Ministry of Local Government and Regional Development. (2023). *Nasjonal strategi for eID i offentlig sektor* [National strategy for eID in the Public Sector]. Regjeringen.no

[61] The Norwegian Digitalisation Agency. *Handlingsplan for nasjonal strategi for eID i offentlig sektor* [Action Plan for a National Strategy for eID in the Public Sector]. Digdir.no

[62] Act relating to electronic trust services. Act of 15 June 2018 relating to the implementation of the EU Regulation on electronic identification and trust services for electronic transactions in the internal market. *https://lovdata.no/dokument/NL/lov/2018-06-15-44*

[63] Proposition to the Storting (Prop.) 87 (Resolution) (2023 -2024). *The Norwegian Defence Pledge. Long-term Defence Plan 2025-2036*. Regjeringen.no

[64] Report to the Storting (white paper) 9 (2022-2023) *National control and cyber resilience to safeguard national security – As open as possible, as secure as necessary*.

[65] Norwegian National Security Authority. (2023). *National Digital Risk Situation 2023*. nsm.no

[66] Kripos. (2023). *Generativ kunstig intelligens og cyberkriminalitet – Temarapport* [Generative Artificial Intelligence and Cybercrime - Thematic Report]. Politiet.no

[67] Nachiappan, A. (2023, 18 September). *WormGPT: AI tool designed to help cybercriminals will let hackers develop attacks on large scale*. Sky News.

[68] The County Governor. (2023). *Totalforsvaret* [Total defence]. Statsforvalteren.no

[69] Norwegian National Security Authority. (2020). *Grunnprinsipper for IKT-sikkerhet versjon 2.0* [Basic Principles of ICT Security version 2.0]. nsm.no

[70] The Norwegian Digitalisation Agency. *Stifinneren* [Pathfinder]. Digdir.no

[71] *"Digitale seksuelle overgrep og krenkelser mot barn og unge – gjerningspersoner, fornærmede og arenaer" [Digital sexual abuse and offences against children and young people – perpetrators, victims and arenas] (NKVTS 2023) and "Seksuell utnyttelse av barn over internett: Rapport om analyse av teknologiske faktorer som påvirker produksjon og deling av materiale som seksuelt utnytter barn over internett"* [Sexual exploitation of children over the internet: Report on the analysis of technological factors that affect the production and sharing of material that sexually exploits children over the internet] (NTNU 2023).

[72] The Norwegian Police Service. *Delbart.no*. Politiet.no

[73] The Norwegian Police Service. *DELE=DELTA: Om deling av voldsvideoer* [Sharing=Participating: About the sharing of videos depicting violence]. Politiet.no

[74] NOU 2022:11. *Your privacy – our shared responsibility*. Regjeringen.no

[75] A chilling effect occurs when people refrain from expressing themselves for fear of the consequences.

[76] An echo chamber is a meeting place where people with the same/similar opinions convene so that opinions are repeated and often reinforced/polarised.

[77] Nudging refers to small measures aimed at influencing people's actions or behaviour in a certain direction.

[78] The Data Ethics Council. *Dataetiskraad.dk*.

[79] NOU 2022: 11 *Your privacy – our shared responsibility*. NOU 2022: 11 - Regjeringen.no

[80] Chapter 9 of the Working Environment Act contains provisions on control and monitoring. There are also separate regulations relating to working from home, access to employee emails and other electronically stored material and video surveillance in working life.

[81] The Norwegian Data Protection Authority. (2022). *Sjefen ser deg? Overvåking og kontroll av arbeidstakeres digitale aktiviteter* [Is your boss watching you? Monitoring and control of employees' digital activities]. Datatilsynet.no

[82] The Norwegian Data Protection Authority. (2023). *Råd for analyse og sporing på nettsted* [Advice for analysing and tracking on websites]. Datatilsynet.no

[83] In the spring of 2023, the Norwegian Data Protection Authority organised input meetings where it received input from more than 160 businesses and organisations on their experiences working with data protection.

[84] Economics Norway. (2021). *Norges behov for IKT-kompetanse i dag og framover Rapport 1-2021* [Norway's need for ICT skills today and in the future Report 1-2021]. IKT-norge.no

[85] OECD. (2023). *2023 OECD Digital Government Index* and OECD. (2024). *The Digital Transformation of Norway's Public Sector*. Oecd.org

[86] Norwegian Committee on Skill Needs. (2023). *Fremtidige kompetansebehov: Utfordringer for grønn omstilling i arbeidslivet, Temarapport 1/2023* [Future skills needs: Challenges for green transition in working life, Thematic report 1/2023]. Kompetansbehovsutvalget.no

[87] Norwegian Official Report (NOU) 2023: 4 *Tid for handling – Personellet i en bærekraftig helse- og omsorgstjeneste* [Time for action - A sustainable health and care services workforce]. Ministry of Health and Care Services.

[88] OECD. (2024). *Going Digital: Shaping Norway's Digital Future.* Regjeringen.no

[89] Nordic Institute for Studies of Innovation, Research and Education (NIFU). (2019). *NIFU-rapport 2019/30: Statens kompetansebehov i den digitale fremtiden – Utfordringer og tiltak* [NIFU Report 2019/30: Central government skills needs in the digital future - Challenges and measures]. Nifu.no

[90] Ministry of Education and Research. *Partssammensatt utvalg for å utrede en kompetansereform for arbeidslivet* [Tripartite Commission for the investigation of skills reform in the labour market]. Regjeringen.no

[91] Rybalka, M., Brevik, R. & Denisova, E. (2023). *Digitalisering i kommunene. Utviklingen fra 2018 til 2022* (Reports, Issue 2023/27) [Digitalisation in the municipalities: Developments from 2018 to 2022]. Statistics Norway. SSB.

[92] Report to the Storting (white paper) 34 (2023-2024). *En mer praktisk skole – Bedre læring, motivasjon og trivsel på 5.–10. trinn* [A more practical school - Better learning, motivation and well-being in grades 5-10].

[93] Excerpt from the Database for Statistics on Higher Education's tertiary vocational college statistics.

[94] Norwegian Committee on Skill Needs. *Kompetansebehovsutvalget.no*

[95] Report to the Storting (white paper) 16 (2020-2021) *Utdanning for omstilling – Økt arbeidslivsrelevans i høyere utdanning* [Education for change – Improved labour market relevance in higher education]. Ministry of Education and Research.

[96] COM (2020) 66 final, *A European Strategy for Data*. Eur-lex.europa.eu

[97] Deloitte. (2018). *Study to support the review of Directive 2003/98/EC on the re-use of public sector information*. Op.europa.eu

[98] National Audit Office of Norway. (2023). *Document 3:8 (2023-2024) The National Audit Office of Norway's investigation of the authorities' facilitation of the sharing and reuse of data in public administration.* Riksrevisjonen.no; Norwegian Digitalisation Agency. (2023). *Rikets digitale tilstand 2024* [Digital State of the Realm], Goal 4. Digdir.no.; Report to the Storting (white paper) 22 (2020-2021). *Data as resource. Data-driven economy and innovation*, Chapter 5. Ministry of Local Government and Modernisation.

[99] The Norwegian Digitalisation Agency. (2024). *Samlet vurdering av måloppnåelse i Rikets digitale tilstand 2024.* [Overall assessment of goal attainment in the Digital State of the Realm 2024.] Digdir.no

[100] OECD. (2023). *2023 OECD Digital Government Index.oecd.org*; OECD. (2023). *2023 OECD Open, Useful and Re-usable data (OURdata) Index 2023*. oecd.org

[101] Source: Report to the Storting (white paper) 22 (2020-2021) *Data as a resource – The data-driven economy and innovation*

[102] Statistics Norway. (2023). *ICT usage in enterprises*. ssb.no.

[103] The Norwegian Digitalisation Agency. (2024). *New report on "Order in your own house"*. Digdir.no

[104] National Audit Office of Norway. (2023). *Document 3:8 (2023-2024) The National Audit Office of Norway's investigation of the authorities' facilitation of the sharing and reuse of data in public administration, section 7.2.1*. Riksrevisjonen.no

[105] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *https://lovdata.no/static/NLX3/32016r0679.pdf*

[106] SKATE (management and coordination of services in e-government) (2024). *SKATE's experience report 2023*. Digdir.no

[107] European Commission. (2024). *Common European Data Spaces*. Digital-strategy.ec.europa.eu

[108] Open Data Governance Board of Ireland. *Open Data Governance Board*. Data.gov.ie

[109] Requires incorporation into the EEA Agreement

[110] Norwegian Official Report (NOU) 2024: 14 *Med lov skal data deles: Ny lovgivning om viderebruk av offentlige data* [Data sharing pursuant to law: New Act relating to the sharing of public data]. Ministry of Digitalisation and Public Governance.

[111] Ministry of Local Government and Modernisation. (2020). *National Strategy for Artificial Intelligence*. Regjeringen.no

[112] The Norwegian Digitalisation Agency. *Kunstig intelligens* [Artificial intelligence]. Digdir.no

[113] Nordic Institute for Studies in Innovation, Research and Education. (2023). *NHO's kompetansebarometer 2023* [The Confederation of Norwegian Enterprise Skills Barometer 2023]. Nho.no

[114] Report to the Storting (white paper) 9 (2023-2024). *Nasjonal helse- og samhandlingsplan 2024–2027 – Vår felles helsetjeneste* [National Health and Cooperation Plan 2024-2027 – Our Common Healthcare Service]. Ministry of Health and Care Services.

[115] The Norwegian Digitalisation Agency. *Kunstig intelligens – oversikt over prosjekter i offentlig sektor* [AI – overview of projects in the public sector]. Data.norge.no

[116] The Norwegian Board of Technology. (2024). *Generativ kunstig intelligens i Norge* [Generative AI in Norway]. Teknologiradet.no

[117] The Ministry of Education and Research and the Office of the Prime Minister. (2023). *Regjeringen med milliardsatsing på kunstig intelligens* [Government investing billions in AI]. Regjeringen.no

[118] Report to the Storting (white paper) 9 (2023-2024). *Nasjonal helse- og samhandlingsplan 2024–2027 – Vår felles helsetjeneste* [National Health and Cooperation Plan 2024-2027 – Our Common Healthcare Service]. Ministry of Health and Care Services.

[119] Separate appendix to Prop. 1 (Resolution) (2023 -2024). *The Government's climate status and plan*. Ministry of Climate and Environment.

[120] Twin transition refers to the inherent opportunities in technology and digitalisation to realise the Sustainable Development Goals.

[121] The Norwegian Digitalisation Agency. *Klima – Vinduet for omstilling smalner* [Climate - The window for change is narrowing]. Digdir.no

[122] OECD. *Going Digital Toolkit*.

[123] See the discussion on data spaces in section 4.1.

[124] Report to the Storting (white paper) 22 (2020-2021). *Data as resource. Data-driven economy and innovation - Figure 3.3*. Ministry of Local Government and Modernisation.

[125] The Ministry of Climate and Environment and the Ministry of Trade, Industry and Fisheries. (2024). *Handlingsplan for en sirkulær økonomi 2024–2025* [Action plan for a circular economy 2024-2025]. Regjeringen.no

[126] Proposition to the Storting (Prop.) 69 (Draft bill and Resolution) (2023-2024). *Lov om bærekraftige produkter og verdikjeder (bærekraftige produkter loven)* [Act relating to sustainable products and value chains (Sustainable Products Act)]. Ministry of Climate and Environment. Regjeringen.no

[127] Statistics Norway (2023). *General government revenue and expenditure*.

[128] National Audit Office of Norway. (2022). Document 3:5 (2021-2022) *Riksrevisjonens undersøkelse av grønne offentlige anskaffelser* [The National Audit Office of Norway's investigation of green public procurement]. Riksrevisjonen.no

[129] Ministry of Trade, Industry and Fisheries. (2023). *Roadmap 2.0. The green industrial initiative*. Regjeringen.no

[130] Ministry of Trade, Industry and Fisheries. (2023). *Nye tiltak for raskere omstilling til grønn industri* [New measures for a faster transition to green industry]. Regjeringen.no

[131] Report to the Storting (white paper) 31 (2023-2024). *Long-term Perspectives on the Norwegian Economy 2024*. Ministry of Finance.

[132] The Norwegian Directorate for Higher Education and Skills. (2021). *Rapport nr. 01/2021 Behovet for ikt kompetanse i Norge, En vurdering av kunnskapsgrunnlaget* [Report No. 01/2021 The need for ICT skills in Norway, An assessment of the knowledge base].

[133] The Expert Group on Industrial Data Sharing. (2022). *Deling av industridata* [Industrial data sharing]. Ministry of Local Government and Regional Development. Regjeringen.no

[134] The Norwegian Digitalisation Agency. *DIGITAL Europe Programme (Digital Europe Programme)*. Digdir.no

[135] Confederation of Norwegian Enterprise. *Bedriftscaser* [Business Cases]. Nho.no

[136] Statistics Norway. (2023). *Use of ICT in enterprises – Obstacles to the use of artificial intelligence technology*. Ssb.no

[137] Economics Norway. (2023). *Kunstig intelligens i Norge – nytte, muligheter og barrierer, Rapport 35-2023* [Artificial intelligence in Norway - benefits, opportunities and barriers, Report 35-2023]. Nho.no

[138] The Ministry of Trade, Industry and Fisheries and the Ministry of Education and Research. (2024). *Strategi for å øke næringslivets investeringer i forskning og utvikling.* [Strategy to increase business investment in research and development] Regjeringen.no

[139] Economics Norway. (2023). *Kunstig intelligens i Norge – nytte, muligheter og barrierer, Rapport 35-2023* [Artificial intelligence in Norway - benefits, opportunities and barriers, Report 35-2023]. Nho.no

[140] OECD. (2024). *Going Digital: Shaping Norway's Digital Future.* Regjeringen.no

[141] The Ministry of Trade, Industry and Fisheries and the Ministry of Digitalisation and Public Governance. (2024). *Nytt veikart skal hjelpe teknologinæringen med å peke retning for innovasjon og verdiskaping* [New roadmap to help the technology industry chart the course for innovation and value creation]. Regjeringen.no

[142] Report to the Storting (white paper) 22 (2020-2021). *Data as resource. Data-driven economy and innovation*. Ministry of Local Government and Modernisation.

[143] Ministry of Trade, Industry and Fisheries. (2022). *Roadmap: The green industrial initiative*. Regjeringen.no

[144] OECD. (2024). *Going Digital: Shaping Norway's Digital Future.* Regjeringen.no

[145] Innovation Norway. (2023). *Ny nasjonal digitaliseringsstrategi – innspill fra Innovasjon Norge* [New national digitalisation strategy - input from Innovation Norway]. Regjeringen.no

[146] The Norwegian Directorate for Higher Education and Skills. *Treparts bransjeprogram for kompetanseutvikling* [Tripartite industry programme for competence development]. Hk.dir.no

[147] European Commission. *Europe's Digital Decade: digital targets for 2030*. Commission.europa.eu

[148] Ministry of Digitalisation and Public Governance. (2024). *Strategi for norsk deltakelse i Programmet for et digitalt Europa – DIGITAL* [Strategy for Norwegian participation in the Digital Europe Programme (DIGITAL)]. Regjeringen.no

[149] The Norwegian Digitalisation Agency. (2023). *EU eGovernment Benchmark 2023*. Digdir.no.

[150] NOU 2022: 9. (2022). *The Norwegian Commission for Freedom of Expression Report*. Ministry of Culture and Equality.

[151] Norwegian Defence Research Establishment Report 2023. *Kartlegging av utenlandsk informasjons-påvirkning på sosiale medier før, under og etter kommunestyre- og fylkestingsvalget 2023* [Assessment of foreign information influence on social media before, during and after the 2023 local government elections].

[152] Norwegian Institute for Social Research. (2022). *Valgforskning.no – ny nettside fra Valgforskningsprogrammet med velgerprofiler og viktige valgsaker over tid* [Valgforskning.no - new website from the Norwegian National Election Studies with voter profiles and important election issues over time]. Samfunnsforskning.no

[153] European Commission. *DSA: Very large online platforms and search engines*. Digital-strategy.ec.europa.eu

[154] Ministry of Culture and Equality. (2024). *Om arbeidet med strategi for å styrke motstandskraften mot desinformasjon* [About the work on a strategy to strengthen resilience to disinformation]. Regjeringen.no

[155] Ministry of Culture and Equality. (2024). *Nasjonal strategi for en åpen og opplyst offentlig samtale* [National strategy for an open and informed public discourse].

[156] Ministry of Local Government and Regional Development. (2024). *Expert group to look at the significance of artificial intelligence for secure and democratic elections*. Regjeringen.no

[157] The Norwegian Digitalisation Agency. *Kor mange opplever digitalt utanforskap?* [How many people experience digital exclusion?]. Digdir.no

[158] The Norwegian Digitalisation Agency. (2023). *Rikets digitale tilstand 2023 Tema: Digitalt utanforskap* [Digital State of the Realm 2023. Theme: Digital Exclusion]. Digdir.no

[159] University of Agder et al. (2024). *Hvilke tjenester bør digitaliseres, og hvordan? En analyse fra brukerperspektiv av hvilke offentlige tjenester som egner seg for digitalisering – Prosjektrapport* [Which services should be digitalised and how? An analysis from a user perspective of which public services are suitable for digitalisation – Project report]. Nav.no

[160] Ministry of Local Government and Regional Development. (2023). *Handlingsplan for auka inkludering i eit digitalt samfunn* [Action plan for increased inclusion in a digital society]. Regjeringen.no.

[161] National Library of Norway. *Demos - Whisper*. Ai.nb.no

[162] European Commission. (2022). *European Declaration on Digital Rights and Principles*. Digital-strategy.ec.europa.eu

[163] Consumption Research Norway. (2022). *Barn og unges digitale kompetanse: Unges erfaringer og perspektiver som utgangspunkt for en utvidet digital kompetanseforståelse* [Children and young people's digital skills: Young people's experiences and perspectives as a starting point for an expanded understanding of digital competence].

[164] Norwegian Media Authority (2022): *Barn og medier 2022 – en undersøkelse om 9–18 åringers medievaner* [Children and media 2022 – a survey of 9-18-year olds' media habits]. Medietilsynet.no

[165] Ministry of Education and Research. (2023). *Strategy for digital competence and infrastructure in kindergartens and schools 2023-2030*. Regjeringen.no

[166] Screen Use Committee. *Om utvalget* [About the Committee]. Skjermbrukutvalget.no

[167] Ministry of Finance. (2021). *Circular R109-21 Prinsipper og krav ved utarbeidelse av samfunnsøkonomiske analyser* [Principles and requirements for socioeconomic analyses]. Regjeringen.no

Published by: Norwegian Ministry of Digitalisation and Public Governance

Publications are available on:
www.government.no

Publication number: D-2006 E
Design: Melkeveien Designkontor AS
Print: Norwegian Government Security and Service Organisation 10/2024 – Impression 50

SVANEMERKET
Trykksak
2041 0446