Norwegian Ministry of Local Government and Regional Development

Selected elements and main points

Official Norwegian Reports NOU 2022: 11

Your privacy – our shared responsibility

Time for a privacy policy

Norwegian Ministry of Local Government and
Regional Development

Selected elements
and main points

Official Norwegian Reports NOU 2022: 11

Your privacy – our shared responsibility

Time for a privacy policy

Translation from Norwegian. For information only.

To the Ministry of Local Government and Regional Development

The Norwegian Privacy Commission was appointed by Royal Decree on 23 June 2020 to assess the position of privacy in Norway. The Commission hereby submits its report.

Oslo, 26 September 2022

John Arne Moen
Chair

Ingvild Næss Deputy Chair	Haakon Hertzberg	Jill Walker Rettberg (until March 2021)
Tor-Aksel Busch	Marianne Høyer	Dag Wiese Schartum
Trine Skei Grande	Finn Lützow-Holm Myrstad	Helge Veum
Trude Margrethe Haugli	Toril Nag	Brita Ytre-Arne (from June 2021)
	Oddhild Aasberg	

Catharina Nes,
Head of Secretariat

Janne Loen Kummeneje

Ailo Krogh Ravna

Contents

Chapter 1
Introduction and summary

1.1 Privacy in a new light

In this report, the *Privacy Commission* paints a picture of a digitalisation process that is affecting every sector in society. It is a cross-party goal to digitalise, and this process has been, and is likely to continue to be, carried out at a high pace. Since the previous *privacy commission* presented its report, many comprehensive digitalisation processes have taken place in both the public and private sectors. As a result of this, more and more personal data is now being collected, used and reused. The societal benefits of digitalisation are often considerable, and the use of personal data is enabling efficient, high-quality services to be provided to citizens. At the same time, the *Privacy Commission* sees a general tendency for digitalisation to take place at the expense of privacy. Through its work on the report, the *Privacy Commission* has sought to obtain an overview of this development, and to identify possible ways forward to safeguard and strengthen privacy in the digital society.

1.1.1 Privacy on the agenda

Privacy is about the society we want to live in, both today and in the days that will follow. In spite of this, privacy is often considered to be an expert field or niche area. Privacy is often discussed in the context of legislation, legal interpretation and compliance. For professional operators, privacy is often associated with formal requirements, possible sanctions and complex legal assessments that get in the way of the performance of everyday tasks. Most people might associate privacy with annoying requests for consent that constantly need to be clicked, emails about updated privacy policies that no one ever reads, and other similar nuisances that distract you from what you actually want to do.

During conversations with primary school pupils, it became apparent that they are tired of talking about privacy as something that is about pointing fingers and bans.[1] They want an open and considered conversation about how personal data is collected, what it is used for, how such collection affects us, and the effects that it has on society. Such conversations require a broader discussion of what privacy means for society as a whole, and what society risks losing if privacy is not protected.

In the opinion of the *Privacy Commission*, it is high time that discussions concerning privacy are lifted out of expert circles and made a relevant and important issue in the public debate, among municipal councils and in the Storting. For this to happen, privacy must be recognised as a public good that has a fundamental value. Privacy must be understood and considered in a positive sense, as a value that helps to safeguard and build trust in society, rather than as a brake or a necessary evil to avoid sanctions.

1.1.2 Privacy as a societal value

Good privacy protection lays the foundations for freedom of expression, freedom of information and the forming of opinions. In other words, privacy is a prerequisite for an open society and a well-functioning democracy.

Privacy can contribute to a better balance of power between individuals, groups, authorities and private operators. The collection, compilation and use of personal data gives certain operators considerable influence. There is a lot of power to be gained from having a detailed knowledge of, and potentially being able to make use of information about, people's lives, thoughts and secrets. Personal data may for example be used to tailor messages, make decisions based on assumptions about individuals and groups, and develop new services. A knowledge of and the ability to control what others know about us, and how they can use

[1] Falch, C. (2022). *Rapport til Personvernkommisjonen. Intervjuer med barn og unge om personvern.*

data about us, is an important tool for limiting this power.

Privacy is not just about the rights and choices of individuals. Good privacy protection is also about protecting other people, e.g. by shielding vulnerable groups from undue intervention, or by ensuring that every citizen is afforded real protection, regardless of their competence and resources. Thus, privacy is also a collective and solidaristic value. In order for privacy to be safeguarded as a fundamental societal value in practice, politicians and other decision-makers must view privacy as a value that is desirable to safeguard. This means that techno-optimism must be accompanied – and sometimes dampened – by critical reflections on what technological advances could mean for our society. It is also about choosing technological solutions which are based on data protection by design and facilitate the safeguarding of privacy. Critical reflections require a basic understanding of both the technology and the legal issues, but ultimately it is a question of understanding and emphasising human rights in our interaction with technology.

1.1.3 Technology and privacy are policy

In many cases, technology can have the power to change, affecting how we live, how we perceive ourselves, and how we exist in interaction with others. Changes originating from technological development can appear revolutionary, for better or for worse. At the same time, these changes often occur gradually and problems often do not become apparent until later.

Privacy is often invisible, in the sense that it is not noticed until something goes wrong, and even when breaches do happen, they are rarely accompanied by physically noticeable impacts. As a result, developments that have the power to change society in fundamental ways often take place out without anyone raising critical questions regarding whether the development is even desirable, and without the development being the subject of an open, democratic debate.

It is unrealistic to think that the wider population should have in-depth knowledge and expertise concerning the technological and legal issues that are part of many discussions relating to privacy. Efforts to implement preventive measures and protect citizens from privacy breaches must be led by the authorities. Nevertheless, the power of technology to change society presupposes that most people should, as part of being a well-informed member of society, have a basic understanding of the role that privacy plays in societal development.

Technology is being developed and introduced at a rapid pace, and technology that appears controversial or remote from reality today can become normalised and widely accepted in the future. When this happens, it may result in the gradual weakening of privacy. This weakening can be difficult to spot before it is too late to counteract the negative effects. In many cases, technological development and its impacts are unpredictable, and any adverse effects may be difficult to counteract if the technology has already become widely adopted. In order to counteract any negative development, it is therefore important to have a democratic discussion regarding the encroachments on the rights and freedoms of individuals that society should be prepared to accept.

1.1.4 Technological development on society's terms

Prioritising privacy as a societal value is not necessarily either easy or frictionless. In the short term, this may entail closing the door to certain technological instruments that could prove to be both good and useful. At the same time, new doors can be opened to facilitate innovation and the development of alternative technology based on our democratic values and principles. This will be of great value for societal development in the long term.

The *Privacy Commission* also strongly believes that technology can be used consciously to improve privacy. For example, technological aids can help people to both understand their rights and exercise them. The *Privacy Commission* believes that such technological opportunities have so far not been sufficiently utilised.

To facilitate responsible technological development and innovation, privacy must be safeguarded through specific actions by authorities and entities that process personal data. In this report, the *Privacy Commission* presents a number of measures to contribute to action and improvement. Some of these measures can be implemented through political and commercial measures, while others will require cultural and competence building over time. Common to the measures is that they will help to raise awareness of the issue of privacy.

It is the *Privacy Commission*'s wish and hope that this report will stimulate a broader public debate concerning privacy. This will entail not only the abovementioned discussion concerning what encroachments on privacy society should be

prepared to accept, but also an examination of the issues from a political perspective. In this way, these fundamental democratic questions can be lifted out of purely legal or technological discussions and viewed from a broad societal, political and human rights perspective.

1.2 A national privacy policy

The *Privacy Commission* calls for a national privacy policy that sets out guidelines for the digitalisation of society, in addition to that which follows from the legislation. This policy must cover the processing of personal data by both the public and private sectors, and ensure that privacy is safeguarded during the formulation of legislation.

The government should draw up a national privacy policy which looks at the status of privacy in Norway, both today and in the future. Privacy is a shared responsibility. The privacy policy must therefore help to open up a public discussion about privacy, and make it an inclusive and important debate about fundamental values, society and democracy.

Below, the *Privacy Commission* summarises the *overriding considerations* that must be taken into account in a national privacy policy. These points are supplemented by examples of specific recommendations from the *Commission*, taken from the various sub-chapters of the report.

A national privacy policy must have the overriding goal of ensuring the genuine protection of privacy. The policy must provide guidance across sectors, with the aim of safeguarding the privacy of citizens. This will require the formulation of overarching principles regarding how society can safeguard privacy as a natural part of the digitalisation process. Policy development must take place in open public debates concerning fundamental issues relating to how much interference in their privacy citizens should have to accept, e.g. in order to meet the need for effective public administration and crime prevention. The *Privacy Commission* recommends that the *precautionary principle* be applied in cases where the use of technology entails a particularly high risk to privacy.

A national privacy policy must view privacy from a holistic perspective. Norway currently has no public body that has overarching responsibility for assessing the general use of personal data in the public administration or its significance as regards privacy. Assessments linked to the use of personal data are largely carried out on a sector-by-sector basis, often with little parliamentary oversight or open debate. As long as data protection assessments take place in silos, or on a piecemeal or individual basis, it will be very difficult to assess the overall impact of potentially intrusive services, measures or legislative changes. The government should pay particular attention to the data protection impacts of more extensive sharing and further processing of personal data, and how this should be assessed in relation to other important considerations, such as efficiency and the rule of law. In order to draw attention to the importance of safeguarding privacy in the digitalisation of society, the *Privacy Commission* believes that the government should present an annual privacy policy report to the Storting, rooted in the current privacy policy.

A national privacy policy must entail thorough risk assessments. It will not be sufficient to consider data protection impacts solely in connection with the individual specific processing of personal data. Possible data protection impacts must also be examined in connection with the formulation of regulations, during the development of services and during the preparation of budgets, procedures and organisational measures. Privacy-friendly technological and organisational alternatives must always be considered before it is assumed that there is a conflict between privacy on the one hand and, for example, societal security, crime prevention and efficiency, on the other.

A national privacy policy must pay particular attention to vulnerable groups, including children and young people in particular. Vulnerable groups may be less able to safeguard their own privacy and exercise their rights. The incorrect use of personal data can contribute to the creation or reinforcement of unfair biases which disproportionately affect vulnerable individuals and groups.

Children and young people are a particularly vulnerable group, because they are shaped by their surroundings to a greater extent than adults, and are exploring their identity. As a result, it is important that personal data about them is not used to «put them in a box» or used against them later in life. The *Privacy Commission* therefore recommends that the government work to introduce a ban on behavioural advertising aimed at children. The school and kindergarten sector must take the lead in seeking to ensure that privacy is safeguarded. It is unacceptable for children's personal data to be commercially exploited.

A national privacy policy must include a clear foreign policy role. Norway should take an active role in the formulation of new international regu-

lations, as well as in the development of international standards and common solutions that can promote privacy. This will entail representatives of the Norwegian authorities working actively and systematically in relation to European legal processes which will have impacts on privacy.

A national privacy policy must make use of national discretion as regards regulation. In many cases, there are limitations on Norway's discretion concerning the formulation of rules and procedures which impact on privacy. International authorities, with the EU as the focal point, largely set out guidelines regarding what can be implemented at national level. Nevertheless, there is considerable scope, in relative terms at least, as regards nationally adapted provisions. The Norwegian authorities must pursue an active national legislative policy in order to promote data protection. It should always be an ambition to utilise the national discretion provided for by EU legislation to *supplement* the European rules to both *support* and *strengthen* current EU legislation which the Norwegian authorities regard as being of particular importance. Where appropriate, the Norwegian authorities should adopt *deviating Norwegian rules* if there is access and sufficient reason to do so.

A national privacy policy must promote privacy-friendly innovation. Technological development should take place in a way that safeguards and promotes privacy. The *Privacy Commission* believes that robust standards and codes should be developed to clarify how innovation can take place within an ethical and justifiable framework. The national privacy policy should also strengthen research and development in the field of privacy, in order to contribute to privacy-friendly innovation and digitalisation. Research in the field of privacy may have a major impact on our ability to understand the overall impacts of digitalisation on the fundamental rights and freedoms of citizens.

A national privacy policy must entail the public sector taking the lead. Public authorities have a responsibility to maintain high standards, including as regards privacy. This means that government agencies must carry out thorough data protection assessments and utilise tools that respect the privacy of citizens. The *Privacy Commission* recommends that the public sector uses its purchasing power to stimulate the emergence of privacy-friendly products and services. Guidelines should be issued concerning how privacy should be weighted in procurements.

A national privacy policy presupposes a solid knowledge and competence base. Decisions and assessments that impact on privacy must be based on legal, technological and social science expertise. The *Privacy Commission* therefore believes that the public sector must prioritise the strengthening of privacy competence among its employees. The privacy policy must also include measures which ensure that citizens receive basic training regarding privacy. The *Privacy Commission* therefore recommends that privacy be included in primary and lower secondary education, and that privacy education be strengthened at all levels, including higher education.

A national privacy policy requires transparency surrounding the processing of personal data. Transparency surrounding the use of personal data is necessary to safeguard and build up trust in the authorities and service providers among citizens. This means not only transparency regarding which personal data is processed and used concerning individuals, but also transparency regarding how personal data is aggregated/compiled and reused. As far as possible, the information should be made available to citizens, without any need to actively request access.

A national privacy policy requires effective enforcement. To ensure compliance with regulations that are intended to protect the privacy of citizens, it will be necessary to ensure that the Norwegian Data Protection Authority has sufficient resources to enforce the law. In addition to effective controls and sanctions, the *Privacy Commission* believes that the Norwegian Data Protection Authority must have the resources it needs to provide guidance operators who need it. As privacy continues to cover more and larger areas, supervision must be strengthened in line with these actual needs. The *Commission* furthermore believes that supervisory authorities other than the Norwegian Data Protection Authority should also provide guidance regarding privacy issues directly linked to their particular area of authority.

1.3 Summary

The following sections present a summary of the key points in each chapter of the report. The *Privacy Commission* stands united behind the assessments and recommendations, with the exception of one recommendation in Chapter 9 relating to exploring the possibility of a general ban on behavioural advertising. With regard to this, the *Commission* has split into *a majority* that supports the recommendation and a *minority* that does not support the measure.

1.3.1 Part I – What are privacy, legal frameworks and technological driving forces?

In *Chapter 3*, the *Privacy Commission* presents an account of different perceptions of what privacy means, and discusses why privacy is important both for the individual and for society at large.

Privacy is a fundamental right for the individual and an important premise for freedom of expression. Yet privacy has a collective aspect. If privacy is disregarded, vulnerable groups or society at large could be affected, e.g. through groups reining themselves in and curbing their active participation in society. Thus, responsibility for privacy cannot be left solely to individual choices and preferences. This discussion forms the backdrop to the rest of the report.

In *Chapter 4*, the *Privacy Commission* reviews the legal regulation of privacy. A general overview is presented of the key provisions of the General Data Protection Regulation, along with a review of the regulation of privacy both as a human right and in the Constitution. The *Commission* also provides a brief account of how privacy is affected and regulated in various sectoral legislation. In addition, the *Privacy Commission* reviews the specific regulation of children's privacy, including the Constitution and the Convention on the Rights of the Child. The principle of the best interests of the child is briefly presented. At the end of this chapter, the *Commission* discusses current and forthcoming European privacy legislation. A discussion of other regulations and a more detailed regulatory review can be found in the respective chapters.

In *Chapter 5,* the *Privacy Commission* presents a brief overview of fundamental features of technological development in society, and identifies certain key areas where technology can create particular privacy challenges. This description forms the basis for further discussions in subsequent chapters.

The development of powerful tracking and sensor technology, data transfer infrastructure, storage technology, as well as ever-increasing processing power, have made it possible to collect, transfer, store and process data on a large scale. As a result, ever larger amounts of personal data can be collected and analysed, a development that puts privacy under pressure. This rapid and complicated technological development has meant that decision-makers and legislators often «fall behind». In order to counteract any unfortunate development, it is therefore important to have a principled and knowledge-based approach to how technology impacts on society, and how society can influence technological development. The discussion regarding technological development must also include certain red lines – technologies or technology applications that are *unacceptable* in a democratic society.

The *Privacy Commission* advocates that the precautionary principle must be applied before technology is introduced which could have serious impacts on both individuals and society at large. Against this backdrop, the *Commission* recommends the introduction of a ban on the use of remote biometric identification in public spaces. This is technology that is used to identify individuals in real-time, which in the opinion of the *Privacy Commission* is so intrusive that the technology is incompatible with fundamental societal values and human rights.

1.3.2 Part II – The position and challenges of privacy in selected sectors

The mandate of the *Privacy Commission* highlights a number of specific areas/sectors where privacy challenges are both numerous and difficult to overcome. In its mandate, the *Commission* is asked to focus in particular on issues relating to privacy in the public sector, privacy in the justice sector, the privacy of consumers, and the privacy of children and young people. Part II of the report presents the *Privacy Commission's* assessments and proposals for measures in the abovementioned areas.

As mentioned above, the *Privacy Commission* recommends that the government establish a privacy policy that is viewed in the context of digitalisation policy. In the privacy policy, the government should pay particular attention to the data protection impacts of more extensive sharing and further processing of personal data, and how such sharing and further processing should be assessed in relation to other important considerations, such as efficiency and the rule of law. Every year, the government should present a report on privacy policy to the Storting, rooted in current data protection policy.

In *Chapter 6,* the *Privacy Commission* discusses digitalisation of the public administration and assesses the privacy implications of developments. The public sector has a particular responsibility to ensure that the privacy of citizens is safeguarded, and must therefore facilitate both thorough impact assessments and due process guarantees. If the public administration is unable

to adequately safeguard the privacy of citizens, this could have serious impacts on individuals and potentially undermine trust in the authorities.

The aim of the digital administration is to offer efficient and user-friendly services. As part of this objective, many administrative tasks are being fully or partially automated, including the use of automated systems in case processing. This often entails systems analysing large quantities of information concerning citizens in order to derive recommendations regarding decisions. Although the use of such systems in the public administration entails a number of advantages, challenges relating to privacy may arise if the systems do not facilitate comprehensible and transparent case processing. In particular, the *Privacy Commission* discusses challenges relating to the use of automated systems for control purposes. Extensive or disproportionate use of profiling for control purposes can have serious negative effects for both individuals and society at large, e.g. in the form of unlawful discrimination or chilling effects. The *Privacy Commission* therefore recommends that the public administration should apply the precautionary principle in connection with the use of profiling for control purposes.

There are also privacy challenges associated with the formulation of regulations in the public sector. If the data protection impacts are not adequately evaluated as part of the regulatory process, there is a risk of disproportionately large intrusions into privacy. The *Privacy Commission* therefore recommends that systematic data protection assessments be carried out in legislative processes.

In this chapter, the *Privacy Commission* also presents an overview of the legal framework for the processing of personal data in the public administration. The *Commission* then goes on to present the various requirements regarding the basis for processing. An overview is presented of the basis for processing, processing purposes and the legal framework for the further processing of personal data. The *Privacy Commission* particularly stresses the importance of creating a secure and clear legal framework for the further processing of personal data. The *Privacy Commission* is of the opinion that impact assessments in legislative processes should include an assessment of whether existing regulations are sufficient and whether use should be made of national discretion. If national provisions are laid down, this could contribute to clearer and more comprehensive legislation, and thus provide greater predictability for citizens. It would also provide a better basis for assessing whether or not specific processing of personal data is lawful.

The *Privacy Commission* highlights a number of challenges relating to the sharing and use of personal data in the public administration. The formulation of legal bases, the use of artificial intelligence and the sharing of personal data between administrative bodies are some of the challenges that are reviewed. One challenge in connection with the sharing of personal data across bodies is that it leads to uncertainty regarding the *division of responsibility* between cooperating bodies. The *Privacy Commission* therefore recommends that the division of responsibility should be laid down in law or regulations to a greater extent in cases where the sharing of personal data forms part of a wider collaboration between administrative bodies and where ambiguity could lead to serious data protection impacts.

The *Privacy Commission* believes that there is a need for an advisory body that has a comprehensive overview of the use of personal data in Norway. Such a body could help to ensure that the privacy policy in force at any given time is implemented and carried out effectively, and provide advice regarding how privacy considerations should be weighed against other considerations, as well as what ethical assessments should be made in connection with the use of personal data.

In *Chapter 7,* the *Privacy Commission* looks at privacy challenges in the justice sector, with a particular focus on the processing and use of personal data by the police. Within the area of justice, the right to privacy must in many cases be weighed against the need to ensure effective crime prevention, which in turn means that privacy is placed under pressure. Privacy is challenged both when there is a desire to implement new methods, and when legislative measures are implemented in order to facilitate crime prevention.

When drafting regulations, data protection impacts are often only assessed to a limited extent, or not at all. This may lead to the introduction of a number of apparently less intrusive legal provisions, which can collectively lead to a surveillance burden on the population. If disproportionately intrusive measures are implemented in the name of crime prevention, it could both erode trust in key societal institutions and lead to chilling effects which could challenge fundamental democratic values.

In the opinion of the *Privacy Commission*, it is therefore crucial that the data protection impacts of crime prevention measures are assessed from a

holistic perspective and subjected to public debate. The starting point must be that, as a fundamental right, privacy must also be safeguarded in the face of the need to ensure effective crime prevention.

Transparency helps to create trust. A lack of information and transparency regarding the use of technology, combined with the steady development of powerful data collection and analysis tools for use in the justice sector, can compromise privacy. One possible impact of this is that the public's confidence in the justice sector is weakened. Limited information is available regarding the tools and methods that are used by the police in Norway and how privacy is safeguarded in practice. The *Privacy Commission* therefore recommends that a committee be appointed to study the use of methods in the justice sector. The committee should particularly consider the data protection impacts of policing methods, especially in relation to the principles of purpose and proportionality.

In the opinion of the *Privacy Commission,* it is crucial that systems and solutions are constructed in a way that safeguards privacy. For example, if the legislature considers extensive mass data collection to be essential in order to combat serious crime, systems for storing such data must be kept apart from other systems to ensure that the data cannot be used for purposes other than collection.

Furthermore, the *Privacy Commission* considers it to be crucial that the Norwegian Data Protection Authority carries out regular checks in the field of justice.

As in other sectors, there is also a general need for a competence lift relating to privacy in the justice sector. This entails the training of personnel, appropriate procedures, systems and tools for handling personal data, as well as a management-based understanding of privacy as a fundamental human right. The *Privacy Commission* believes it is particularly important that senior police officers have a high level of awareness of the risk of slippage of purpose, and that the risk of such slippage is reduced through the establishment of appropriate procedures and technical measures. The *Privacy Commission* furthermore recommends that better systems be established for handing over documents to lawyers, and that an assessment be carried out to determine how information covered by prohibitions against seizure can be sorted out in connection with the review of mobile phones.

In *Chapter 8*, the *Privacy Commission* discusses how the digitalisation of the school and kindergarten sector has taken place at the expense of children's privacy. Schools and municipalities have largely implemented extensive changes in order to digitalise school life, but have not had either the expertise or resources to ensure that privacy is safeguarded as part of the digitalisation process.

Teachers, parents, students and school management make use of a wide range of digital services as part of their teaching on a daily basis. Many of these services, from learning resources to administrative tools, process large amounts of personal data concerning students, who are also exposed to extensive advertising, despite the ban on advertising in schools. In many cases, a detailed technological and legal knowledge is needed in order to obtain an overview of how personal data is processed and used in these systems, and the data protection impacts that such processing and use could have. Most municipalities have neither the resources nor the expertise to carry out thorough assessments on their own, which in turn means that there is currently a limited overview of how the privacy of Norwegian pupils is being safeguarded. There is a need for the professionalisation and centralisation of risk assessments and testing of digital solutions that are being considered for use in schools and kindergartens.

The *Privacy Commission* recommends that a national competence and testing environment be established to assist municipalities in dealing with challenges relating to data protection. A national service catalogue for digital learning resources should be established, which also contains data protection assessments that municipalities and schools can use as a basis when choosing digital services. In addition, the *Privacy Commission* wants to see immediate measures be introduced to limit the commercial exploitation of personal data relating to pupils and reduce the advertising pressure in services that are used by schools in their teaching.

Major global technology companies have gained access to classrooms across the country by offering affordable, user-friendly services. Individual municipalities, schools and teachers do not possess the necessary expertise, nor have any influence or bargaining power in their meetings with these operators, and there is therefore a considerable risk that the digitalisation of schools will take place on terms stipulated by the technology giants. It is difficult to obtain an overview of how the privacy of pupils is safeguarded when commercial solutions are used, and it can also be prob-

lematic that individual pupils develop an early consumer relationship with the companies concerned through school.

The *Privacy Commission* believes that it should not be up to each municipality to negotiate agreements with technology giants, and that the national authorities should come on board. There is also a need for a wider debate about the role of major technology companies in Norwegian schools. Insofar as the solutions that are available on the market do not adequately safeguard privacy, the *Privacy Commission* believes that Norwegian authorities must invest in the development of new solutions that safeguard privacy in a satisfactory manner.

In *Chapter 9*, the *Privacy Commission* discusses challenges which particularly relate to consumer privacy and the use of social media and digital platforms in a broad sense. The collection and use of personal data for commercial purposes has become a pivotal part of digital consumer life and led to the development of many new services. This development has also created significant privacy challenges and it is now almost impossible to prevent commercial operators collecting information about who you are, what you like and where you move around.

The commercialisation of personal data has created strong financial incentives to collect as much information as possible. Everything from who you communicate with, what news you read, what you buy, who you love and where you are, is recorded and subject to analysis and commercial exploitation. Among other things, personal data is used to develop new products and services, to be resold or to create detailed profiles that can be used to target behavioural advertising and other messages.

The challenges are all the greater as regards the commercial use of children's personal data. Children are entitled to special protection. Yet they are frequent users of digital services, and personal data concerning children is often collected on the same scale as that of adults. It is impossible to obtain an overview of how the information is used or what future impacts its use could have. At the same time, children have rights and a right to protection against surveillance, including surveillance by their own parents. The rights of children are coming under pressure from digital products and services which allow parents to monitor their children's movements and activities. The legislation protecting children is fragmented and partially overlapping, and the *Privacy Commission* therefore recommends that the legislation be reviewed and reworked to ensure that children's rights are safeguarded.

The *Privacy Commission* recommends, inter alia, that the Norwegian authorities take an active role in relation to the EU as regards consumer privacy, especially in relation to ongoing legislative processes. The *Privacy Commission* shares the government's view that behavioural advertising aimed at children should be banned. The *Commission* also supports the prohibition of the use of special categories of personal data for marketing purposes.

The *Privacy Commission* split into a majority and a minority regarding the question of whether a *general ban* on behavioural advertising should be evaluated. The *majority of the Commission* believes that an evaluation should be carried out to determine whether or not a *general ban* is necessary to protect Norwegian and European consumers. *A minority in the Commission* believe that, as long as behavioural advertising is done responsibly, a general ban would be disproportionate.

Privacy is not currently a competitive advantage for commercial operators, both because it is normally impossible for consumers to obtain an overview of any data protection impacts, and because punishments for breaking the law are inadequate. The *Privacy Commission* believes that the authorities have a role to play in stimulating the development and use of privacy-friendly technology, both through procurement schemes and procurements, and by cracking down harder on operators who fail to protect privacy. It is particularly crucial that regulations are enforced with respect to the global technology companies, which have a dominant position in the data-driven economy. In this regard, consideration should also be given to whether or not the competition legislation could be used more actively to prevent negative data protection impacts in connection with mergers and acquisitions, and to limit the market power of the giants in order to ensure a level playing field.

As an investor, Norway also has a unique opportunity to influence global technology companies through the Norwegian Government Pension Fund Global (also known as the Oil Fund), which owns significant shares in the technology giants. The *Privacy Commission* believes that the Oil Fund should use its power as an investor, e.g. by formulating privacy requirements as part of its investment strategy. This could make the inadequate protection of privacy a significant invest-

ment risk, which in turn could create financial incentives to develop privacy-friendly solutions.

1.3.3 Part III – Other areas in which the Commission has worked

In *Chapter 10,* the *Privacy Commission* describes the legal complexity of the privacy regulations and discusses the national discretion that follows from the Regulation.

Privacy is regulated by the Personal Data Act and the General Data Protection Regulation, which are both cross-sectoral regulations. In addition, there are also national, sector-specific rules concerning the processing of personal data. The Regulation is formulated in such a way that it creates a number of difficult interpretative choices. In many cases, the legislation also requires broad discretionary considerations. Difficulties in understanding the interaction between the GDPR and national legislation are not uncommon. This can create challenges for both controllers and data subjects. The *Privacy Commission* therefore recommends that ongoing efforts be made to make the legal rules as clear and comprehensible as possible.

Although the General Data Protection Regulation applies equally across all EU and EEA countries, there is in certain contexts both a right and an obligation to issue national provisions. There may also be a need for national regulations that bridge the gap between national legislation and the Regulation.

The *Privacy Commission* recommends, inter alia, that the government pursue an active legislative policy to promote privacy, both by making use of the national discretion and by working actively with the EU to strengthen pan-European legislation. The *Commission* also submits a number of concrete proposals regarding how the national discretion can be utilised.

In *Chapter 11*, the *Privacy Commission* discusses how technology can be used to better protect privacy. It is a question of how technology can not only threaten privacy, but also help to protect privacy. Among other things, technological tools can better equip citizens to safeguard and exercise their privacy rights, and help controllers to fulfil their obligations. The *Commission* describes what data protection by design can look like in practice, through a «rights platform», where citizens have access to the information that public operators hold about them, and where they can get support to exercise their rights, such as access, rectification and erasure.

The *Privacy Commission* recommends that the Norwegian authorities stimulate the development of privacy technology, e.g. through the imposition of procurement requirements and the introduction of financial incentive schemes.

In *Chapter 12,* the *Commission* discusses transparency as a prerequisite for satisfactory democratic participation, privacy and the rule of law.

Data protection impacts many different aspects of freedom of expression and information, and these rights can sometimes come into conflict with each other. For example, the right to privacy could restrict access to personal data, which in turn could limit freedom of information. Yet privacy can also be an important prerequisite for individuals choosing to express their opinions concerning controversial topics. Good privacy can thus counteract chilling effects on the voice climate.

The *Privacy Commission* believes that it is essential that the results of automated processes that have a direct bearing on citizens' duties, rights, freedoms and opportunities can be explained. If, for example, administrative decisions are made, applications for loans decided or prison sentences determined using entirely or partially automated systems, the people that the decisions concern must be given a clear explanation of why the output from the machine was as it was.

Transparency also means the opportunity to gain access to your own personal data, and knowledge about who has accessed the data and how it has been used. The *Privacy Commission* believes that it should be a goal that citizens have access to information about the specific personal data that has been registered about them. By making this information available, the individual does not have to apply for access. Provision must also be made to ensure that the information is clear and comprehensible to those affected, including those who lack basic digital skills. The *Privacy Commission* endorses key conclusions in the Norwegian Digitalisation Agency's report on how transparency and disclosure of information concerning the processing of personal data should be implemented in practice.

The *Privacy Commission* also recommends that data subjects be involved to a greater extent in the development of services. There is a need for genuine participation in the development of solutions that process personal data.

In *Chapter 13*, the *Privacy Commission* presents the role of the Norwegian Data Protection

Authority as a supervisory authority, guidance body and social actor. The Norwegian Data Protection Authority currently has cross-sectoral responsibility and a substantial workload, which presents challenges relating to resources in connection with the performance of its statutory tasks.

The *Privacy Commission* believes that the Norwegian Data Protection Authority must be strengthened by being given more resources. However, it is not true that privacy can only be ensured through a strong central supervisory authority. In order to strengthen privacy, it will be necessary to secure access to expertise relating to privacy in all areas of society, including those of public bodies other than the Norwegian Data Protection Authority.

Because the privacy regulations are difficult to apply, it is problematic that many controllers do not have sufficient access to guidance. This can lead to the regulations being misinterpreted, leading to breaches of privacy.

The *Privacy Commission* recommends that guidance provided for controllers be strengthened. At the same time, sectoral supervision should to a greater extent regard the safeguarding of data protection as a task within its remit. This can contribute to better guidance and more effective enforcement.

Chapter 2
The Commission's mandate, composition and work

2.1 Mandate of the Privacy Commission

The *Privacy Commission* was appointed by Royal Decree on 23 June 2020.

The *Commission* was given the following mandate:

«On its political platform (the Granavolden platform), the government has decided that it will: «Set up a privacy commission to assess the position of privacy in Norway. This commission will, inter alia, look at privacy in the justice sector and how privacy can be safeguarded in connection with the greater use of digital solutions, including the rights of social media users.» It also follows from the platform that «The government presupposes that privacy is enshrined in the Constitution, that everyone has the right to privacy, and that the state has a responsibility to ensure the protection of personal integrity. The pressure on privacy is intensifying as a result of the increasing use of digital solutions and the internet. The government will establish strict requirements regarding the secure storage and processing of personal data from both private and public operators.»

It also follows from request decision 588 (2017–2018) that: «The Storting asks the government to ensure that the mandate of the *Privacy Commission* includes a special assignment to assess the status of the privacy of children and to propose measures to strengthen this.»

In 2012, the EU began work on a new general regulatory framework for the protection of personal data, with the General Data Protection Regulation (GDPR) subsequently entering into force in EU Member States in May 2018. This Regulation was implemented in Norway through the Personal Data Act on 15 June 2018. An important consideration in the new privacy legislation is the harmonisation of legislation throughout the EEA, so that businesses are ensured a level playing field, regardless of which Member State they operate in. At the same time, residents throughout the EEA will enjoy the same strong privacy protection, regardless of which Member State they live in.

In 2014, the Storting decided to strengthen the protection of personal integrity by incorporating a provision concerning privacy in the Constitution. The right to privacy also follows from Article 8 of the European Convention on Human Rights (ECHR) and the Council of Europe's Convention on Data Protection in connection with electronic data processing of personal data, ETS no. 108.

The challenges

Norway is a country with a high level of digital maturity, both among the population in general and in the business sector in particular.[1] Digitalisation is helping to improve welfare, increase productivity and boost economic growth in virtually every sector of society and industry. New industries are being created, and the needs and habits of consumers are changing rapidly. The digitalisation of services means that far more personal data about individual citizens is being generated, registered and processed than ever before. This is information about geographical patterns of movement, contact networks, health, finances, interests and other information about the individual's activities. The information can be compiled and analysed. Profiles can be built up about each individual, which in turn can provide a lot of information about us. Service providers with whom we do not feel we have a close relationship can also analyse us in this way, using information shared between operators in the digital economy. This has increased the pressure on privacy. However, the introduction of the General Data Protection

[1] OECD. (2019). *Measuring the Digital Transformation*.

Regulation has also contributed to a significant strengthening of privacy in many areas of society.

Personal data collected as a result of the greater use of digital services also offers unique potential for analysis and service development. Both public and private entities can become more efficient and provide better services. Where do those searching for information about the flu vaccine or the treatment of vomiting bugs live? Analyses of such searches online can help the health authorities to understand the population's health situation both faster and better. Data traffic analyses are important in enabling providers of electronic communication to plan the digital infrastructure on which we depend. Based on the simultaneous movements of many cars, each driver can get recommendations on travel routes which were previously impossible to get in real-time. Transport companies can analyse travel patterns in order to plan public transport capacity. Financial institutions can also analyse their customers' shopping patterns and use of different means of payment to develop and improve their services. Authorities can compile and use data for the benefit of citizens. Personal data can also be used for service development and optimisation within individual entities, meaning that it has significant market value.

The potential of and pressure on the commercial use of personal data is considerable. Services are offered without any user payment based on the resale of information about users. The value of personal data may depend on who is buying or selling and what the information will be used for.

2.1 Reuse of data for control purposes, including in the justice sector

The prevention, detection, investigation and prosecution of crime is vital in states governed by the rule of law. Crime is changing. The perpetrators are using new methods, including new technology. In much of the justice sector's work, the compilation and analysis of electronic traces and other information about the activities of citizens is therefore both important and useful. To facilitate this work, access is in many cases given to disclose information, both between bodies within the justice sector and between the justice sector and the public administration in general.

While information sharing and analysis are important for combating crime and preventing abuse and encroachment on the legal sphere of those who fall victim to crime, it may also mean that personal data is used for purposes other than those for which it was originally collected. Such reuse of personal data has increased in recent years.

Other areas of the public administration and the private sector are also increasingly reusing personal data for various control purposes. Customs, taxes and insurance are examples of this. Personal data is being reused in some contexts without the data subjects being made aware of the relevant processing of personal data. In some contexts, it is essential that such processing is not publicly known if the purpose is to be achieved, e.g. to uncover tax evasion or insurance fraud.

2.2 Privacy in digital solutions

Both the public and private sectors are increasingly using digital solutions. We submit tax returns digitally and use Altinn for various reports. We have road toll tags and electronic tickets on buses, trains, boats and planes. We use online banking and read newspapers digitally. This, and many other tasks where digital solutions are used, mean that we leave electronic traces on a completely different scale than in the case of paper-based solutions.

Public authorities are increasingly seeking to compile information about citizens across sectors in order to improve and streamline their services. Services are being personalised and automated. The technology enables information to be analysed and used for research purposes. This, in turn, is facilitating the development of good public services. Yet privacy considerations must also be safeguarded. The secondary use of personal data, e.g. for research purposes, may have data protection impacts. It is a question of the extent to which the authorities can compile, analyse and reuse information about individuals, without adversely affecting the individual's trust in the authorities. It can be challenging for individuals to obtain information and obtain an overview of the processing of their own personal data. It is important to create solutions that enable large amounts of data to be used, while ensuring the fewest possible privacy disadvantages for individuals.

Digital services in the private sector also require the processing of personal data to varying degrees. Some only process absolutely essential information in order to be able to execute an agreement, while others collect data to a far greater extent than is necessary to actually provide the service concerned. Everyday life as a digital consumer increasingly involves having to disclose personal data in order to participate in society. The advantages and disadvantages of new technological solutions must be balanced against each other in an appropriate way. Yet Norwegian enterprises must also be competitive in an international perspective.

The Report to the Storting on consumer policy (Report to the Storting no. 25 (2018–2019) «Consumer of the future – green, smart and digital»[2]), which was presented in summer 2019, identified a series of new consumer challenges in the digital world in which we live. One of the challenges discussed in the report concerns consumer rights, privacy and security with regard to digital products and services. Digital services collect large amounts of personal data about consumers, which is reinforced by the development of connected products in the Internet of Things. Companies use this personal data for targeted marketing aimed at consumers.

In 2015, the Norwegian Data Protection Authority published the report entitled «Det store datakappløpet» (The big data race).[3] In 2020, the Norwegian Consumer Council presented an analysis of the processing of personal data in the digital advertising industry.[4] The reports describe the trading of person-based analyses and the poor transparency and, in particular, incomprehensibility of this. The analyses are used to send us advertisements and select news which is presented to us in online newspapers and social media. The advertising and selected news can influence the choices that we make. The ability not only to influence what we buy, but also – covertly – to influence democratic processes is significant. Covert influencing can challenge democracy. It is therefore necessary to increase our insight into, and awareness of, how information about us can be used to influence the choices we make.

We use digital media for social contact on a daily basis. In the 2016 report entitled «App-fail», the Norwegian Consumer Council reviewed 20 apps to determine the extent to which consumer and privacy rights were being safeguarded. The use of personal data by services is more extensive than many people realise, which makes it difficult to maintain control over your own personal data. Information concerning how consumers' personal data is processed is often hidden in long, complicated and, in many cases, unbalanced, contractual terms and conditions.

2.3 Special considerations concerning children's privacy

Article 104 of the Norwegian Constitution gives children an individual right to protection of their personal integrity. Article 16 of the Convention on the Rights of the Child states that no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation, and the child has the right to the protection of the law against such interference or attacks. The Personal Data Act and the General Data Protection Regulation also set out special rules concerning children, inter alia. Section 5 of the Personal Data Act contains a special age limit of 13 years for children's consent to the use of information society services.

Kindergartens and schools register and store personal data about children and young people. In addition to traditional information such as general orderliness, conduct, grades and development, data is collected when students use new digital learning resources and in connection with communication between the school and the pupil's parents or guardians. This can challenge the privacy of children and young people in a new way.

Half of the data breaches notified to the Norwegian Data Protection Authority in 2019 regarding children occurred in the school sector. Schools are using more and more types of digital solutions. This is presenting a range of challenges relating to privacy. Learning platforms and tablets are a very useful resource in a teaching context, but unnecessary data, such as data concerning location and when

---

2 Report to the Storting no. 25 (2018–2019) *Consumer of the future – green, smart and digital*. Ministry of Children and Families.

3 Norwegian Data Protection Authority. (2015). *Det store datakappløpet*.

4 Norwegian Consumer Council. (2020). *Out of control*.

homework is actually done, may also be processed.

The use of «free» apps by schools for teaching purposes means that others will gain access to extensive information about the pupils. In practice, neither the pupils themselves nor their parents/guardians have much opportunity to influence the collection and processing of personal data when using such apps, and consent to the use of the app will not necessarily be genuine.

Children are active users of social media. They communicate independently on social media from a relatively young age. The sharing of photographs and video is a natural part of the communication that takes place between children. We know very little about the scope of this or how its use affects children's privacy. Service providers that disseminate advertising based on user information, sharing, choices and preferences also target children. Such marketing can be particularly challenging for children and young people, who find it more difficult than adults to identify and understand advertising. Therefore, the Marketing Control Act also stipulates strict requirements regarding advertising that is aimed at children. Studies of marketing aimed at children also show that children[5] are exposed to direct marketing, which can be regrettable. Furthermore, the Norwegian Consumer Council has discovered that internet-connected toys and products aimed at children are able to «monitor» the children who use them.

3. The assignment

Against this backdrop, the *Commission* will:

- Review the situation regarding privacy in Norway and identify the key challenges and developments.
- Review the public sector's processing of personal data for purposes other than that for which the data was collected, and present an assessment of the negative data protection impacts of this in relation to the benefits.
- Consider the development of privacy in the justice sector and determine the extent to which the overall scope of measures creates challenges as regards privacy.
- Review the genuine opportunities open to consumers to safeguard their own privacy when using digital solutions and services, and assess whether industry standards, labelling schemes and certification mechanisms could be better used; see Chapter IV, Section 5 of the General Data Protection Regulation.
- Examine the impacts of using social media for the collection, analysis and further use of personal data, and propose measures to safeguard privacy, including the ability of individual citizens to safeguard their own privacy.
- Review how children and young people's privacy is safeguarded in Norway, including the safeguarding of children's privacy in the kindergarten and school sectors and the use of «free» apps by schools where payments are made in the form of children's personal data. In its work, the *Commission* must take into account the follow-up to NOU 2019: 23 New Education Act.
- Propose measures that enhance the digital consumer competence of children and young people, especially that relating to the digital collection of personal data and marketing in social media. The *Commission* shall not propose measures that entail changes to the Knowledge Promotion 2020 curriculum.
- Review how extensive use of and exposure in social media, including user-generated content, affects the privacy of children and young people and suggest possible measures to improve privacy. The *Commission* may, inter alia, map the data protection impacts of profiling children and consider possible regulations relating to the use of personal data for direct marketing to children, and examine the ability of children to give consent within the area of privacy.
- Discuss other topics that prove to be particularly relevant in order to provide a holistic picture of the overall situation regarding privacy. In its work, the *Commission* shall also seek out information in our neighbouring countries and give an account of relevant measures that have been implemented to safeguard privacy.»

---

[5] Rosenberg, T. Grav., Steinnes, K. K., Storm-Mathisen, A. (2018). *Markedsføring og personvern i sosiale medier – en flermetodisk undersøkelse med barn som medforskere*. Forbruksforskingsinstituttet SIFO, OsloMet Steinnes, K.K., Teigen, H.F. & Bugge, A.B. (2019). *Photophop, fillers og falske glansbilder? En studie blant ungdom om kjønn, kropp og markedsføring i sosiale medier*. Forbruksforskningsinstituttet SIFO, OsloMet.

The *Privacy Commission* was originally due to submit its report in the form of an NOU to the Ministry of Local Government and Modernisation by 1 December 2021. In a letter from the Ministry of Local Government and Modernisation dated 11 December 2020, the *Commission* was given an extended deadline of 1 June 2022. To allow time for proofreading and printing, the date for submission of the report was subsequently set to 26 September 2022.

2.2 The Privacy Commission's interpretation and delimitation of the mandate

The *Privacy Commission*'s mandate is broad. It has therefore been necessary to establish priorities with regard to the issues that the *Commission* should address in more detail. This has been done on the basis of the *Commission's* overall assessment of the challenges in light of the existing knowledge base. As a result, there are issues and topics that the *Commission* has not discussed in more detail.

The *Privacy Commission* has also delimited the mandate in relation to other ongoing work and processes. The Freedom of Expression Commission, the Expert Group for Digital Learning Analysis and the Media Harmfulness Committee have all worked in parallel with the *Privacy Commission* to some extent. During the course of its work, the *Privacy Commission* has been in dialogue and had meetings with these committees.

The *Commission* has considered challenges relating to privacy in the four main areas outlined in the mandate: the public sector/administration, the justice sector, the school and kindergarten sector, and the consumer sector.

The *Commission* based its work on key driving forces and developments that impact privacy, with an emphasis on technology, regulations and general societal characteristics. The *Commission* has discussed privacy as a fundamental human right and assessed privacy as an essential right for individuals, an important collective societal value, and a prerequisite for a well-functioning democracy and the rule of law.

The mandate highlights issues relating to the public sector's re-use of personal data and the processing of personal data for purposes other than that for which the data was collected. The *Commission* emphasises these challenges, but also notes other challenges, and has therefore opted to take a broader look at the status of privacy in the public sector, including expertise and legislative work. Throughout the report, the *Privacy Commission* will use the term *further processing* to refer to the use of personal data for purposes other than that for which the data was collected. Such further processing may be either compatible or incompatible with the purpose of collection; see Article 6 (4) of the General Data Protection Regulation.

The *Commission* has delimited the report's chapter on the justice sector so as to exclude sectors such as the security industry and the Norwegian Customs Service. Processing of personal data and examples from these areas are only used where they shed light on the situation. The principal discussion presented in the chapter relates to the police. It has not been possible to go into all the different issues relating to specific police tasks, and the *Commission* therefore discusses topical issues at an aggregated level.

The mandate emphasises children in a number of the points. For this reason, the *Privacy Commission* wished to involve children in the work of the *Commission* and hear their opinions. In order to include children's perspectives on privacy in the report, the *Commission* decided to commission an external study where children were interviewed about their thoughts and knowledge concerning the topic.

The *Commission* believes that the involvement of children in the report has strengthened the knowledge base and given the *Commission* a better insight into the measures that will be both relevant and effective for this target group. In addition, the *Commission* believes that it is important that children can have a greater influence over societal development within the area of privacy.

The *Commission* has opted not to separate out children's privacy as a separate chapter, and has instead considered the topic in Chapter 4 on legal regulation, Chapter 8 on privacy in schools and kindergartens, and Chapter 9 on children as consumers and in familial relationships.

The mandate states that the *Privacy Commission* is tasked with mapping the protection of children's privacy in the school and kindergarten sector. The *Commission* has limited the scope of this mapping to the work of the Expert Committee on Digital Learning Analysis, and has therefore not discussed the use of digital learning analysis tools.

The mandate notes that the *Commission* is to look at the genuine scope that consumers have open to them to safeguard their own privacy when using digital solutions and services. Through its

work, the *Commission* has concluded that consumers today have very limited opportunities to safeguard their own privacy because of the considerable scope of practices by commercial operators which invade the privacy of consumers. The *Commission* has therefore opted to discuss how consumer privacy is being put under pressure, and how this development can be counteracted through legislation, enforcement and altered practices among commercial enterprises.

The mandate states that the *Commission* must also discuss other topics that are particularly relevant to the overall situation regarding privacy. Practical measures to protect and promote privacy require an effective and applicable regulatory framework, as well as robust enforcement and guidance mechanisms. The *Commission* has therefore opted to discuss the national discretion as regards legislation relating to privacy, and assessed the scope and role of the Norwegian Data Protection Authority as a supervisory and guiding authority.

In the view of the *Privacy Commission*, transparency and the practical application of rights are cornerstones for the safeguarding of privacy. Therefore, the *Commission* has discussed how technology can be used to promote privacy, considered measures to promote transparency, and discussed the ability of individuals to exercise their rights.

2.3 Composition of the Commission

The *Commission* was as composed as follows:
- John Arne Moen, CEO, Steinkjer (Chair)
- Ingvild Næss, Chief Privacy and Data Trends Officer, Oslo (Deputy Chair)
- Tor-Aksel Busch, retired Attorney General, Askim
- Trine Skei Grande, Director of Sustainability, Oslo
- Trude Haugli, Professor of Law, Tromsø
- Haakon Hertzberg, Deputy Director General, Drammen
- Marianne Høyer, Board Chair, Trondheim
- Finn Lützow-Holm Myrstad, Senior Adviser, Oslo
- Toril Nag, CEO, Sandnes
- Jill Walker Rettberg, Professor of Digital Culture, Bergen
- Helge Veum, Business Manager, Ålesund
- Dag Wiese Schartum, Professor of Management Informatics, Oslo
- Oddhild Aasberg, Senior Legal Advisor, Brønnøysund.
- Brita Ytre-Arne, Professor of Media Studies, Bergen
- Jill Rettberg, resigned as a Commission member on 15 March 2021.
- Brita Ytre-Arne took up her position as Commission member on 13 June 2021.
- The Commission's secretariat has been placed under the Ministry of Local Government and Regional Development, with the following secretariat members:
- Hege B. Sæveraas, Senior Adviser (Head of Secretariat from June 2020 to November 2020 and December 2021 to January 2022)
- Dana Irina Jaedicke, Senior Adviser (Head of Secretariat from December 2020 to November 2021)
- Catharina Nes, Director (Head of Secretariat from January 2022 inclusive)
- Janne Loen Kummeneje, Adviser
- Christiane Engelmann Helgar, Adviser (from January 2021 to March 2022)
- Ailo Krogh Ravna, Senior Advisor (from February 2022 inclusive)

2.4 The work of the Commission

The first plenary session of the *Privacy Commission* took place on 30 September 2020. The *Commission* has held a total of 18 plenary meetings, including 12 two-day meetings. During the first plenary meeting, the *Commission* decided to split into three working groups, each responsible for different aspects of the mandate. The groups have held separate meetings throughout the *Commission's* work. The *Privacy Commission* concluded its work on 18 July 2022. The report has not been updated with any regulatory changes or other circumstances of relevance which occurred after this date.

The *Commission*'s website (www.personvernkommisjon.no) has been live since May 2021 and, among other things, includes a presentation of the members of the *Privacy Commission*, a public relations page, as well as a page on which documents published by the Commission are made available to the public. In addition, the *Commission* has held several input seminars. These input seminars were recorded and published on the website. The members of the *Privacy Commission* have also given talks and lectures. The Commission members and the secretariat have participated in con-

ferences, meetings and lectures relevant to the work.

The *Commission* have held a total of three input seminars on privacy in schools, technological trends and privacy in the municipal sector.

The following people, organisations and businesses spoke at the input seminars:

Privacy in schools

- Edvard Botterli Udnæs, Leader of the Student Organisation
- Asle Sandnes, Senior Adviser, Parents' Committee (FUG)
- Kjersti Botnan Larsen, Senior Adviser, Ombudsman for Children
- Sara Eline Grønvold, Special Adviser, Save the Children
- Line Gaare Paulsen, Director of Competence and Public Affairs, ICT Norway
- Simen Sommerfeldt, CTO Bouvet Øst, Bouvet Norge

Technological trends

- Tore Tennøe, Director, Norwegian Board of Technology
- Øyvind Husby, CEO, ICT Norway
- Simen Sommerfeldt, CTO Bouvet Øst, Bouvet Norge
- Erik Lehne, Managing Partner, Gartner

Privacy in the municipal sector

- Morten Haug Frøyen, Data Protection Officer, City of Oslo
- Arnstein Eek, Data Protection Officer, Utsira Municipality
- Connie Bjørseth, Data Protection Officer for the municipalities of Stor-Elvdal, Åmot, Trysil and Engerdal
- Inger Cock-Olsen, Data Protection Officer, Østre Toten Municipality
- Harald Torbjørnsen, Foreningen kommunal informasjonssikkerhet (KINS)
- Jan Sandtrø, Lawyer

The Commission has invited professionals to open the Commission's meetings. These were:

- Adele Matheson Mestad, Director of the Norwegian National Human Rights Institution
- Inga Bejer Engh, Ombudsman for Children, and Kjersti Botnan Larsen, Senior Adviser, Ombudsman for Children
- Elisabeth Staksrud, Professor, Department of Media and Communication, University of Oslo
- Kristinn Hegna, Professor, Department of Education, University of Oslo
- Leif Ole Topnes, Assistant Chief Constable and Head, Joint Unit for Immigration and Public Administration (FUF), Norwegian National Criminal Investigation Service (Kripos)
- Rune Reitan, Superintendent, Department of Joint Operational Services, Norwegian National Criminal Investigation Service (Kripos)
- Merethe Smith, Secretary General, and Marius Dietrichson, Lawyer, Norwegian Bar Association
- Bjørn Erik Thon, Director-General, Norwegian Data Protection Authority
- Åsmund Mæhle, Adviser and CTO Bouvet Øst, Bouvet Norge
- Anders Lund, Head of Section, Sigrid Lian, Adviser and Aksel Morris Bjørnø, Adviser, Sikt – Norwegian Agency for Shared Services in Education and Research
- Kristine Meek, Director of Communication, Advisory Services and Analysis and Thea Grav Rosenberg, Senior Advisor, Critical Media Understanding, Norwegian Media Authority
- Asbjørn Tolo, Senior Adviser, Parents' Committee (FUG)
- Christian Sørbye Larsen, Project Manager SkoleSec, Lene Karin Wiberg, Special Advisor, Steinar Hjelset, Project Employee SkoleSec and Asbjørn Finstad, Deputy Director General, Strategic ICT and Digitalisation, SkoleSec, Norwegian Association of Local and Regional Authorities (KS)
- Runar Karlsen, Sector Director for Security and Emergency Preparedness, NHO Service
- Mona Naomi Lintvedt, PhD student, Norwegian Research Center for Computers and Law, University of Oslo
- Håkon Hukkelås, PhD student, Norwegian University of Science and Technology (NTNU)
- Tone Bringedal, Senior Advisor and Siri Eriksen, Norwegian Resource Centre for Sharing and Use of Data
- Fredrik Borgesius, Professor, University of Radboud, The Netherlands
- Sylvia Peters, Senior Adviser, Ministry of Justice and Public Security
- Christoph Lutz, Associate Professor, BI Norwegian Business School
- Mareille Kaufmann, Professor, Department of Criminology and Sociology of Law, University of Oslo

- Kjersti Løken Stavrum, Manager and Ivar Anders Iversen, Head of the Secretariat, Freedom of Expression Commission
- Marte Blikstad-Balas, Manager, Eirin Oda Lauvset, Hilde Hultin and Malcolm Langford, Committee members, Expert Committee for Digital Learning Analysis
- Anja Salzmann, PhD student at the Department of Information Science and Media Studies, University of Bergen
- Janicke Weum, Head of Analysis and Evaluation, Christine Hafskjold, Senior Adviser and Kristine Regine Buestad Asmaro, Senior Adviser from the Ministry of Local Government and Regional Development
- Aasta Margrethe Hetland, Senior Adviser, Norwegian Directorate of eHealth
- Nils Henrik Heen, General Counsel, Finance Norway
- Dag Hareide, author
- Hilde Nagell, Advisor, Agenda (think tank)
- Bår Stenvik, author
- Gisle Hannemyr, Researcher, Department of Informatics, University of Oslo
- Camilla Nervik, Head of Section, and Charlotte Bayegan, Senior Adviser, Norwegian Data Protection Authority
- Suhail Mushtaq, Technical Manager, Norwegian Association of Local and Regional Authorities (KS)
- Fredrik Andersen, Manager and Ida Dahl, Head of Product, Neddy
- Mari Hersoug Nedberg, Head of Privacy Section, Norwegian National Criminal Investigation Service (Kripos)

The Commission has also received oral and written input concerning the work from:

- Department of National IT Policy and Public Governance, Ministry of Local Government and Regional Development
- Change Factory
- Norwegian Data Protection Authority
- Norwegian Board of Technology
- Norsk Lektorlag (Norwegian Association of Lecturers)
- Norwegian Police Directorate
- Kristian Bergem, Deputy Director General of Digital Common Solutions, Norwegian Directorate for Education and Training
- Norwegian Directorate for Children, Youth and Family Affairs
- Norwegian Customs Service
- Norwegian Public Roads Administration
- Norwegian State Educational Loan Fund
- Norwegian Directorate of Health
- Norwegian Institute for Adult Learning (Kompetanse Norge)
- Norwegian Institute of Public Health (FHI)
- Norwegian System of Patient Injury Compensation
- Norwegian Agency for Quality Assurance in Education (NOKUT)
- Norwegian Digitalisation Agency
- KINS
- Norwegian Labour and Welfare Administration (NAV)
- Norwegian Directorate of Immigration
- Ola Kristian Hoff, Secretary, Media Harmfulness Committee

The *Commission* would like to thank all the contributors.

The work during the COVID-19 pandemic

The work of the *Commission* has been affected by the COVID-19 pandemic. As a result of the pandemic, many meetings have been held digitally. The *Commission* and the Secretariat have put considerable effort into maintaining progress and good cooperation in challenging times. The various restrictions have also meant that the *Commission* was not permitted to carry out a planned study trip abroad.

The *Commission* has invited both external researchers and professionals, as well as the committee members, to speak on various topics.

External reports

The *Commission* has commissioned six external reports:

- «Barns samtykkekompetanse på personvernfeltet» (Children's competence to give consent in the privacy field), Ingvild Sciøll Ericson (available as a digital attachment to the Commission's report)
- «Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering» (The requirement for a clear legal basis for the public administration's collection of control information and use of profiling), Mona Naomi Lintvedt (available as a digital attachment to the Commission's report)
- «Emerging technologies that can act on human body,» Gartner.

- «Intervjuer med barn og unge om personvern» (Interviews with children and young people concerning privacy), Christian Falch.
- «Informasjonsteknologi og personvern. Utviklingstrekk og forslag» (Information technology and privacy. Development trends and proposals), Gisle Hannemyr
- «Personopplysninger i skolen» (Personal data in schools), Norwegian Association of Local and Regional Authorities (KS)

Chapter 5
The technological landscape that affects privacy

Summary of the Norwegian Privacy Commission's recommendations

- The *Privacy Commission* supports a ban on the use of remote biometric identification in public spaces. The Norwegian authorities should work internationally, particularly in relation to the EU, to implement a ban.
- The *Privacy Commission* believes it is crucial that Norwegian politicians have a basic understanding of technology, but without becoming bogged down in a technology-deterministic approach, where fundamental principles and rights must cede priority in the service of technology.
- The *Privacy Commission* believes that it should be a fundamental societal principle that the introduction of intrusive technology does not take place without an evaluation of the problems that are actually to be solved and a thorough prior assessment of whether there are less intrusive ways of achieving the goal.
- The *Privacy Commission* believes that the introduction and use of new technology in society that could have significant implications as regards privacy must be the subject of public debate. This is especially true if the authorities wish to use potentially intrusive technology.
- The *Privacy Commission* believes that the precautionary principle should be applied before consideration is given to the introduction of technology that entails a particularly high risk to privacy, such as remote biometric identification in public spaces.

Chapter 6
Privacy in the digital public administration

Summary of the Norwegian Privacy Commission's recommendations

Holistic approach to privacy in the public administration

- The *Privacy Commission* believes that the Storting should be afforded greater influence with regard to the digitalisation of the public administration and the impacts that this has on the privacy of citizens. The involvement of the Storting will, inter alia, help to shed more light on decisions and garner broader support.
- The *Privacy Commission* believes that measures which have a major impact on the privacy of citizens should have a legal basis, rather than be laid down in regulations. This will give the Storting the opportunity to obtain an overview of the public administration's processing of personal data.
- The *Privacy Commission* believes that the public administration has a special responsibility to safeguard the public's trust. This will require a thorough assessment of whether or not the purpose of the further processing of citizens' personal data is compatible with the purpose for which the data was originally collected, and how intrusive the further processing is. These assessments should be made public.
- The *Privacy Commission* recommends that the government draw up a comprehensive privacy policy for the public administration. This privacy policy must be viewed in the context of the digitalisation policy and set out guidelines for how the public administration should make principled assessments of privacy and ensure that the privacy of citizens is safeguarded in the solutions that are developed. In the privacy policy, the government should pay particular attention to the data protection impacts of more extensive sharing and further processing of personal data, and how these should be assessed in relation to other important considerations, such as efficiency and the rule of law.
- The *Privacy Commission* recommends that, every year, the government should present a report on privacy policy to the Storting, rooted in current data protection policy.
- The *Privacy Commission* believes there is a need for an independent advisory body for the public administration, which will specifically assess and discuss fundamental and general issues relating to the use of personal data within the public administration, including societal and ethical issues.

Drafting of statutory provisions

- The *Privacy Commission* believes that the assessment of data protection impacts in legislative processes should include an assessment of whether existing regulations are sufficient and whether use should be made of the national discretion provided for in the General Data Protection Regulation. National provisions can provide clearer and more comprehensive rules, and thus greater predictability for citizens. It will also provide a better basis for assessing the lawfulness of specific types of processing of personal data.
- The *Privacy Commission* recommends that the government consider whether the duty to consult pursuant to the General Data Protection Regulation is being adequately complied with. Such an assessment should also include an assessment of how the duty to provide advice can be formulated so as not to delay legislative processes and cause a disproportionately large resource burden for the Norwegian Data Protection Authority. These assessments should be made as part of the development of a privacy policy.
- The *Privacy Commission* recommends that the public administration publish assessments of data protection impacts in connection with legislative and regulatory processes.
- The *Privacy Commission* believes that it is necessary to establish a clear and applicable guide

for assessing data protection impacts in legislative and regulatory processes. The guidelines should enable the competent ministry to highlight both the data protection impacts of the measure that is being introduced in isolation, and the overall data protection impacts of different measures that are already in place in the area concerned.
- The *Privacy Commission* believes that the guide on legislative drafting and pre-legislative processes («lovteknikkheftet») should be updated.
- The *Privacy Commission* recommends that the public administration strengthens the privacy competence of managers, executive officers and other employees who need such expertise. In the work relating to regulatory development, requirements should be established for competence relating to privacy in the working group. A knowledge of privacy and data protection should be included in the mandatory basic training for newly appointed executive officers, in the same way as training concerning the Public Administration Act and the Freedom of Information Act already is.

Sharing of personal data between administrative bodies

- The *Privacy Commission* recommends that the division of responsibility should be established by law or regulations in cases to a greater extent where the sharing of personal data forms part of a wider collaboration between administrative bodies, and where ambiguity could lead to serious data protection impacts.
- The *Privacy Commission* believes that standards for sharing personal data must be drawn up and developed further. This will facilitate collaborate and help to raise the level of professional quality and ensure the efficient use of resources.
- The *Privacy Commission* recommends that the government investigate whether a consent-based implementation of the «once only» principle could alleviate some of the privacy-related drawbacks that arise from the sharing of personal data between government agencies.
- The *Privacy Commission* recommends that the Ministry of Local Government and Regional Development follow up the Norwegian Digitalisation Agency's report concerning access and control of how personal data is processed by government agencies in the work to facilitate the safeguarding of citizens' rights in the public administration.

Use of artificial intelligence

- The *Privacy Commission* believes that legal regulation of the use of artificial intelligence should be aimed at counteracting the power imbalance between the public administration and citizens. With greater intrusion comes a need to impose greater demands as regards transparency and other due process mechanisms.
- The *Privacy Commission* believes that the use of machine learning systems within the public administration should require human rights assessments in cases where the systems could have a significant impact on the lives of citizens.

Profiling for control purposes

- The *Privacy Commission* believes that profiling to uncover illegalities should always be seen as an intrusive process which requires a sound legal basis, partly because there is always a risk of slippage from decision support to decision. The intervention must be proportionate given the purpose that is to be achieved and expressed in clear and predictable legal rules.
- The *Privacy Commission* believes that the public administration should apply the precautionary principle in connection with the use of profiling for control purposes. Extensive or disproportionate use of profiling for control purposes can have serious negative effects for both individuals and society at large.

Public operators and major technology companies

- The *Privacy Commission* believes that government agencies must carry out thorough assessments of whether or not they should use social media to disseminate information and communicate with citizens. Social media should not be used in connection with specific individual case processing.
- The *Privacy Commission* believes that it is important that both privacy and data/strategic assessments are made whenever the public sector uses services provided by major technology companies. As the issues are often the same, the public administration should cooperate across sectors and levels to ensure that a

high level of professional quality is maintained and resources are used effectively.

- The *Privacy Commission* believes that the public administration must make information available to citizens via digital solutions where personal data is collected and used by commercial operators for commercial purposes, e.g. in order to build and enrich profiles or share with third parties.

Information security

- The *Privacy Commission* believes that the entities within the public administration must be given clearer recommendations (or a «code») for management activities, and basic levels of security measures and privacy measures that they can use as a starting point when managing risks relating to their tasks and services.
- The *Privacy Commission* recommends that the government give priority to the «Common security in the public administration» (Felles sikkerhet i forvaltningen) measure as a centrally funded measure. Central government agencies with adjacent areas of responsibility are given missions in letters of allocation concerning contributions to this work.

Chapter 7
Privacy in the justice sector

Summary of the Norwegian Privacy Commission's recommendations

Processing responsibility in the correctional services

- The *Privacy Commission* is of the opinion that, in its work relating to the new Execution of Sentences Act, the Ministry of Justice and Public Security should clarify the responsibility for processing within the correctional services and delegate responsibility to the entities that actually perform the processing of personal data.

International cooperation

- The *Privacy Commission* believes that the findings uncovered by EDPS, i.e. that EUROPOL receives large quantities of personal data from the police forces of the member countries, must be followed up by the Norwegian authorities to ensure that the privacy of Norwegian citizens is safeguarded whenever the police transfer information to EUROPOL. The Commission assumes that similar issues may exist in other contexts where information is exchanged between law enforcement agencies, e.g. between Norway and INTERPOL, and that this must also be followed up.

Data protection impact assessments in legislative processes

- The *Privacy Commission* believes that the ministries should consult with the Norwegian Data Protection Authority to a greater extent in connection with legislative and regulatory processes to ensure that data protection impacts are adequately discussed. A thorough assessment of the data protection impact in legislative processes is a prerequisite for democratic control.
- The *Privacy Commission* believes that the government must allocate funding for research into the societal impacts of surveillance measures in the justice sector. This represents important knowledge in order to be able to make overarching assessments in connection with the introduction of legislative changes.

Data protection impact assessments in the exercising of authority

- The *Privacy Commission* believes that the Ministry of Justice and Public Security must consider whether all the provisions of the Law Enforcement Directive should be implemented in the Police Databases Act. Harmonising the law with the directive would provide clearer guidelines regarding data protection assessments and make it easier for officials to apply the law.
- The *Privacy Commission* believes that the use of open sources on the internet can create special challenges relating to privacy. Among other things, the Commission is concerned about the chilling effects that may arise as a result of the justice sector's use of open sources online, and this perspective must be given emphasis when drawing up internal instructions and the like.
- The *Privacy Commission* believes that if measures are initiated that entail the mass collection of personal data for specified purposes, it is important that data separation methods are followed to ensure that the data is only used for purposes deemed necessary by the legislature.
- The *Privacy Commission* believes that senior police officers must have a high level of awareness of the risk of slippage of purpose, and that the risk of such slippage is reduced through the establishment of appropriate procedures and technical measures. An important measure in this context is the building of a sound culture surrounding privacy. This is a managerial responsibility.

Transparency

- The *Privacy Commission* recommends that a committee be appointed to study the use of methods in the justice sector. The committee should particularly consider the data protection impacts of policing methods, especially in relation to the principles of purpose and proportionality. This work presupposes that the committee has access to the necessary information concerning the use of intrusive methods and covert coercive measures. This is important both as a trust-preserving measure and in order to initiate an open and democratic debate regarding where the line should be drawn between privacy and crime fighting and prevention.

Judicial oversight

- The *Privacy Commission* believes that consideration should be given to whether or not the current judicial oversight of police measures should be expanded to cover more measures than as is currently the case. The Commission also emphasises the importance of formulating provisions which authorise various coercive measures in such a way as to facilitate effective and genuine judicial oversight.
- The *Privacy Commission* believes that an addendum to Section 170a of the Criminal Procedure Act should be implemented to ensure that an assessment is carried out which concludes that the combined use of various investigative methods does not constitute a disproportionate intervention. In such an addendum, it should be emphasised that privacy considerations shall be afforded weight in the assessment.

Specific issues relating to the use of new technology

- The *Privacy Commission* believes that transparency and opportunities for control in connection with procurements in the justice sector are crucial. In connection with the procurement of potentially intrusive tools, data protection assessments must be a pivotal factor in any decisions that are made.
- The *Privacy Commission* believes that special consideration should be given to verifiability and safeguarding of the rights of individuals when machine learning systems are used in the justice sector. In order for such methods to be adopted in Norway, they must also be explainable to anyone who is using the technology, and risk assessments and the requisite technical documentation must be made available in line with the proposed Regulation on artificial intelligence.
- The *Privacy Commission* recommends a general ban on the use of facial recognition and other remote biometric identification in public spaces. Although such a ban would obviously limit the scope for solving certain forms of crime, the Commission believes that the technology is so intrusive that it would be difficult to reconcile it with fundamental rights and societal values.
- The *Privacy Commission* believes that, although it is important that the police are given what they need to tackle serious crime, this should be done with the least possible interference in the opportunities for free and secure communication. Reasonable grounds for suspicion and requirements regarding a clear and unequivocal legal basis and judicial oversight in connection with intervention must remain unchanged.

Competencies

- The *Privacy Commission* does not believe that the police have afforded sufficient weight to raising awareness of privacy among employees. Competence and culture relating to privacy must be anchored among senior police officers. Resources must also be dedicated to enabling data protection officers to facilitate skills upgrading within the organisation.
- The *Privacy Commission* believes that police officers should be given more thorough training in privacy than is the case at present. The need for this is particularly great in connection with the use of ICT systems in day-to-day police operations, in connection with privacy and human rights assessments when collecting and disclosing personal data, and with regard to cooperation with other public or private entities.
- The *Privacy Commission* believes that the level of competence with regard to privacy among the digital policing units (DPA units) in the police districts should be raised, so that all operational decisions relating to the electronic processing of personal data are taken within the existing legal framework regarding privacy and following a robust risk assessment. The collaboration between the DPA units and data protection advisers and data protection officers

within the police force must be clarified and incorporated in a more uniform way, ideally through national guidelines.
- The *Privacy Commission* believes that teaching concerning privacy at the Norwegian Police University College must be strengthened. The Police University College plays an important role in building up an understanding at the training stage regarding the importance of privacy in the day-to-day work of the police force.

Systems and tools to protect privacy

- The *Privacy Commission* believes that the Norwegian authorities should collate experience from other countries concerning schemes for filtering out surplus information in connection with the seizure of digital storage devices, and consider establishing a similar scheme. Privacy considerations must always be weighed against the need to solve crime, where dynamic investigations do not always initially have a complete overview of the type of information that could subsequently prove to be important as evidence.
- The *Privacy Commission* believes that the Ministry of Justice and Public Security should establish a collaboration platform for document disclosure in the justice sector. This platform should be developed with privacy and security in mind, and should, among other things, include provision to limit downloading and logging functions with the aim of reducing the improper reuse of documents.
- The *Privacy Commission* believes that the Ministry of Justice and Public Security should establish a standard for ICT security and invest more heavily in the future in connection with ordering/stipulation of requirements and the development of solutions that satisfy the requirements regarding data protection by design.

Supervision and control

- The *Privacy Commission* believes that the Norwegian Data Protection Authority and the police should keep statistics on the number of people who exercise their right to complain about the processing of personal data by the police every year. The publication of such statistics could help to raise awareness of the right to complain.
- The *Privacy Commission* recommends that the proposed committee to be tasked with assessing the privacy implications of the methods used by the police also be asked to consider whether the mandate of the Communications Control Committee (Kommunikasjonskontrollutvalget) should be expanded to include controls on policing methods other than communication control, bugging and data extraction. Strengthening of the Communications Control Committee will be an important supplement to other legal safeguards, such as data protection impact assessments and judicial oversight.

Chapter 8
Privacy in schools and kindergartens

Summary of the Norwegian Privacy Commission's recommendations

National guidelines

- The *Privacy Commission* believes that a comprehensive and proactive national privacy policy must be established in the school and kindergarten sector. The *Commission* believes that the national privacy policy for kindergartens and schools must:
  - enable municipalities, schools and kindergartens to make use of digital services and learning tools in a way that safeguards the privacy of children and young people;
  - ensure that the right of children to an education and the protection of their personal data are safeguarded, while at the same time preserving municipal autonomy and the freedom to choose teaching methods in schools and kindergartens;
  - set out clear requirements regarding the quality of digital services, including with regard to privacy;
  - contain and specify a requirement that suppliers of services to the school and kindergarten sector are not permitted to use business models that profit commercially from children's personal data. In practice, this means that it is not acceptable to use suppliers who reserve the right to use data relating to children and young people for commercial purposes, particularly marketing activities.
  - identify measures that emerge from the work of the Expert Committee that has been appointed to look at privacy-related challenges concerning the use of learning analytics.
- The *Privacy Commission* believes that there is a strong need for a national service catalogue. Such a catalogue could be an important initiative to ensure that school owners are able to choose services that are not only functional, but also safeguard privacy in a satisfactory manner. It must be ensured that the service catalogue sets out clear and verifiable requirements regarding privacy and information security. The service catalogue should provide an overview of learning materials where risk and vulnerability analyses and data protection impact assessments have been carried out. A well-functioning service catalogue will require continuous changes and updates, as digital services can change continuously.
- The *Privacy Commission* believes that government agencies must take the initiative to develop a privacy standard for the school and kindergarten sector. A privacy standard could help to put municipalities in a better position to fulfil their responsibilities regarding processing and ensure the more comprehensive and reconciled safeguarding of children's privacy in kindergartens and primary schools. A standard could also help to simplify municipal procurement processes by stipulating requirements that suppliers must comply with and will be familiar with.

Competence and resources

- The *Privacy Commission* believes that it is crucial for the privacy of children in schools and kindergartens that municipalities are allocated sufficient resources to safeguard privacy and, as part of this, given access to resources with basic competence regarding technology. This is a prerequisite for being able to make appropriate assessments and safeguard privacy on an ongoing basis.
- The *Privacy Commission* therefore recommends that a multidisciplinary national testing and expert environment be established, or further developed in the case of existing structures, which performs the following functions:
  - *Expert environment that coordinates and develops tools and templates* that enable municipalities to conduct risk assessments

and data protection impact assessments, and establish effective internal controls.
- *Testing* of digital solutions to be used in schools and kindergartens. The outcome of the testing of the solutions should be communicated to those responsible for the national service catalogue.
- *Negotiation management and support* to municipalities involved in negotiations with platform suppliers. This will strengthen the bargaining power of municipalities by making it easier to stipulate the necessary requirements for the services.

Procedures and guidance

– The *Privacy Commission* believes that municipalities must to a greater extent ensure adapted procedures and guidance for school management and teachers. Among other things, guidelines should be drawn up which clarify roles and responsibilities relating to the procurement and use of new digital learning tools.
– The *Privacy Commission* believes that the Norwegian Directorate for Education and Training should to a greater extent assist and enable municipalities to fulfil their responsibilities regarding processing in accordance with the privacy regulations. Among other things, this will mean that the municipalities will receive assistance in establishing the necessary and adapted procedures and guidance.
– The *Privacy Commission* believes that it is important that the municipalities have procedures in place which ensure that children's privacy is safeguarded when digital tools are used outside school property. Among other things, this means clarifying any limitations in the school's responsibilities, and drawing up guidelines regarding how parents can help to safeguard their children's privacy in connection with the use of digital tools outside school property. Finally, the municipalities should regularly follow up and assess whether established measures and procedures are adequate at all times.
– The *Privacy Commission* believes that it is important that municipalities have procedures and guidelines in place which ensure that teachers and other staff at the school do not use information that has been collected and stored on pupils' digital devices for control purposes. Municipalities must also establish procedures which ensure that pupils and parents are kept informed about what information is being collected and what it is being used for.
– The *Privacy Commission* believes that there will be synergies to be gained for the municipalities if they work with other municipalities concerning the preparation of guideline procedures.
– As part of its efforts to strengthen internal controls in the school and kindergarten sector, the *Privacy Commission* believes that school and kindergarten teachers must be given better training as regards privacy and the purposes behind the data protection regulations.

Use of pupils' personal data for commercial purposes

– The *Privacy Commission* believes that the government must initiate a broad study concerning digital tools which are in use in schools and how they impact on children's privacy. Such a study should cover all types of teaching aids and other methods and tools used in a teaching context. Such a study should examine the opportunities for surveillance that these tools offer, the knowledge that can be extracted from the information that has been collected and stored, and how this knowledge is being used for the benefit of pupils and educational institutions. Furthermore, a review should be conducted to determine how the personal data that is collected is being further processed for different purposes. The *Commission* believes that it is essential to also consider this from a data strategy perspective. Data concerning the learning patterns of Norwegian pupils is strategically important and cannot be handed over to commercial operators for further use, or in ways which means that Norway itself actually becomes dependent on such operators.
– The *Privacy Commission* believes that ad blocking tools or other measures on pupils' devices should be considered as a measure for reducing pupils' exposure to advertising. This could also help to reduce the tracking of pupils' digital activity for commercial purposes.

Procurement and negotiations

– The *Privacy Commission* believes that procurement and negotiations, especially from the major platform providers, should be professionalised and centralised. Government agencies and/or the Norwegian Association of Local and Regional Authorities (KS) should actively assist municipalities in negotiations

with platform suppliers to offset the power imbalance that many small municipalities face. Strengthening the bargaining power of municipalities will make it easier to stipulate essential requirements regarding services that will process personal data concerning school pupils and kindergarten children.
- The *Privacy Commission* believes that government agencies should look at the possibility of entering into collaborations with other countries in negotiations with the global platform providers, e.g. within the framework of the Nordic co-operation.
- The *Privacy Commission* believes that procurements and negotiations concerning solutions for the school and kindergarten sector must be rooted in the national privacy policy for schools and kindergartens. This policy must set out clear requirements regarding the quality of learning resources, and at the same time safeguard children's right to privacy and protection against data about pupils being used for commercial purposes.

Development of appropriate digital learning resources

- The *Privacy Commission* believes that the national privacy policy for the school and kindergarten sector should include measures to support Norwegian enterprises which develop solutions that underpin the principles of the national education policy and the fundamental rights of children – and that are not based on a business model that profits from children's personal data.
- The *Privacy Commission* believes that if assessments carried out by the national testing and resource centre show that existing solutions do not adequately safeguard privacy, government agencies must invest in the development of new and more appropriate solutions. The *Commission* considers that it may be appropriate to make such investments under European or Nordic auspices. In the view of the *Commission*, Norway can, and should, take a pioneering role in this work.

Teaching privacy

- The *Privacy Commission* believes that schools must strengthen the teaching they provide concerning privacy as a fundamental human right. Pupils should be educated in the social science aspects of privacy, including that good privacy protection is an important value in a democratic society. The teaching of privacy in schools can help pupils to become more aware that their personal data is being processed, and give them an insight into the information that digital learning tools are used to collect. The *Commission* stresses that the responsibility for safeguarding one's own privacy should not be placed on the individual pupil. Although educating children is important in order to provide children with adequate 'ballast', it should be seen not as a solution to the privacy challenges in schools, but rather as a supplement to the measures recommended by the *Commission*.

Safeguarding the rights of children and parents/guardians

- The *Privacy Commission* believes that municipalities must ensure that information about the type of data that is collected about pupils and kindergarten children is readily accessible.
- The *Privacy Commission* believes that municipalities should facilitate genuine opportunities for participation by pupils and parents/guardians in decisions that have a significant impact on the children's privacy. Pupils and parents/guardians can be involved in various ways, including when performing data protection impact assessments. Other arenas for participation where school owners can obtain and discuss views with students and guardians are the Student Committee (Elevutvalget), the Parents' Association (FAU) and the National Parents' Committee for Primary Education (FUP).

Chapter 9
Consumer privacy

Summary of the Norwegian Privacy Commission's recommendations

The ability of consumers to protect their own privacy

- The *Privacy Commission* recommends that the government pursue a proactive privacy policy in relation to the EU.
- The *Privacy Commission* recommends that the government take the initiative to investigate how technology can be used to protect consumers, e.g. through privacy-friendly default settings or automatic blocking of illegitimate tracking. It is important that the public sector takes such an initiative, to ensure that it is not exclusively the global platform players who lead the way in this work in practice.

Supervision and enforcement

- The *Privacy Commission* recommends that responsibility for enforcing the use of cookies and similar tracking technologies be delegated to the Norwegian Data Protection Authority.
- The *Privacy Commission* believes that the government should support a proposal for an E-privacy Regulation that sets out requirements regarding the use of tracking technology which complies with the General Data Protection Regulation.

Legislative processes in the EU

- The *Privacy Commission* recommends that the government become involved in the design of the Regulation on Artificial Intelligence and associated appendices, and work to promote regulation which ensures that AI systems are designed in a way that safeguards privacy during both the development and use of the systems.
- The *Privacy Commission* recommends that the government supports the European Commission's proposal for a horizontal ICT security law (the Cyber Resilience Act).
- The *Privacy Commission* believes that the government should be an active driving force in EU legislative processes which impact on consumer privacy.

Internet of Things

- The *Privacy Commission* recommends that Norwegian importers, retailers and trade associations have information available concerning how privacy is safeguarded before connected products are sold.
- The *Privacy Commission* recommends that retailers have control procedures in place to ensure that products sold in Norway operate in accordance with the privacy regulations and the Electronic Communications Act, and establish requirements for their suppliers concerning, inter alia, data minimisation, purpose limitation and privacy as a basic setting. Industry standards and labelling schemes can be an important tool for ensuring that suppliers fulfil such requirements.
- The *Privacy Commission* recommends that the government's position concerning regulatory development means that retailers are given legal responsibility for inadequate ICT security and privacy in products they sell.

Behavioural advertising

- The *Privacy Commission* shares the government's view that behavioural advertising aimed at children should be banned. The *Commission* also supports the prohibition of the use of special categories of personal data for marketing purposes. The ban should also apply to special categories of personal data that is derived from data which was not sensitive at the point of collection, such as location data which could collectively be used to determine political or religious affiliation.
- The *Privacy Commission* recommends that, in the event of a ban on behavioural advertising

that only applies to children, service providers must be subject to the precautionary principle. Solutions that lead to increased tracking and profiling in order to map the identity and age of consumers are not desirable.

- The *Privacy Commission* further recommends that the use of children's personal data for behavioural advertising purposes be prohibited. Children's personal data should not be used for behavioural advertising, even if the marketing is not actually aimed at children.
- The *Privacy Commission* split into a majority and a minority regarding the question of whether a *general ban* on behavioural advertising should be evaluated:
- The majority of the Privacy Commission, members Busch, Grande, Haugli, Hertzberg, Høyer, Myrstad, Schartum, Veum, Ytre-Arne and Aasberg, wish to stress that behavioural advertising can also be harmful to the general population. For this reason, the majority of the Commission believes that an evaluation should be carried out to determine whether or not a general ban is necessary in order to protect Norwegian and European consumers. The evaluation should consider both the positive and negative impacts that such a ban would entail in Norway and in Europe, including for the media industry.
- A minority of the *Privacy Commission, members Moen and Næss*, believe that behavioural advertising can be done in different ways – either responsibly or irresponsibly. Members Moen and Næss believe that, as long as behavioural advertising is done responsibly, a general ban would be disproportionate. Moen and Næss therefore do not support the majority's proposal that an assessment be carried out to determine whether or not a general ban is necessary.

Transparency and information

- The *Privacy Commission* recommends that strict information and transparency requirements be imposed regarding how consumers are profiled and segmented in connection with the targeting of advertisements and political messages. This means that businesses, organisations and political parties are open about the messages that they send out and who they are trying to reach through the messages. Platforms that facilitate the segmentation and profiling of consumers should also offer tools to show which advertisements appear on the platform and which segments they use. Transparency is necessary in order to uncover unreasonable or harmful influence. The government should work to put such requirements in place through the EU.

Manipulative design

- The *Privacy Commission* believes that a ban on manipulative design, as proposed in the DSA, would strengthen the ability of consumers to protect their own online privacy. Such a ban should be complemented by the enforcement of current consumer legislation, as well as guidelines issued by the supervisory authorities which clarify the boundary between what is deemed to constitute the acceptable and unacceptable use of design respectively. The proposal should be anchored and secured through the EU cooperation.

Profiling, segmentation and discrimination

- The *Privacy Commission* recommends that the Equality and Anti-Discrimination Ombud should work with the Norwegian Data Protection Authority to counteract discrimination arising from the use of machine learning systems.
- The *Privacy Commission recommends* that enterprises that use machine learning systems to profile and segment consumers should report how they counteract discriminatory effects in their systems. Government agencies should require such reporting in connection with procurements and the awarding of funding. The government should strive to ensure that such requirements become part of the impending Regulations on artificial intelligence and its annexes.

The Oil Fund's investments

- The *Privacy Commission* recommends that, whenever the Oil Fund invests in technology companies, requirements be established for the protection of privacy, in the same way as requirements for the protection of other fundamental human rights.
- The *Privacy Commission* recommends that the Oil Fund refrain from investing in companies which invade privacy and which it is unable to influence, e.g. because of majority owners.

Competition

- The *Privacy Commission* recommends that Norway instigate and lead an international effort to investigate how instruments in the Competition Act could be used to prevent negative privacy impacts in connection with acquisitions and mergers. The study must assess whether the Competition Act has been formulated in such a way that it deals with the challenges of the data economy. This must also be viewed in the context of the introduction of new competition tools under the forthcoming Digital Markets Act (DMA).
- The *Privacy Commission* believes that government agencies should stimulate the development of solutions and standards for data portability and technical interoperability. The existence of such solutions is a prerequisite for healthy competition in many digital product and service markets.
- The *Privacy Commission* believes that it is a fundamental prerequisite for strong privacy that it should not pay to break the law. The effective enforcement of privacy regulations will therefore be essential in order to establish a level playing field and stimulate innovation in privacy-enhancing technologies.
- The *Privacy Commission* believes that the fact that Norwegian companies and global technology giants do not operate on a level playing field raises data protection issues. The government must take steps to limit the market power of the giants to ensure a level playing field and thus facilitate innovation that supports privacy.

Special considerations concerning children's privacy

- The *Privacy Commission* recommends that the government appoint a legislative committee to review and propose changes to regulations to protect children and young people in digital interfaces.
- The *Privacy Commission* recommends that privacy challenges relating to content shared by parents and other children be overcome through skills development, including through education. This is an area where measures relating to netiquette and judgement are important.
- The *Privacy Commission* believes that the Ombudsman for Children should develop a guide for children and parents aimed at strengthening the understanding of children's right to privacy in familial situations.

Chapter 10
Regulatory complexity and national discretion

Summary of the Norwegian Privacy Commission's recommendations

- The *Privacy Commission* believes that the Norwegian authorities should not accept a situation where it is difficult to establish which regulations apply or how they should be interpreted. Both the need to ensure the legal protection of individuals and legal certainty for controllers and processors indicate a need to work continuously to ensure that the regulations are as clear and comprehensible as possible.
- The *Privacy Commission* believes that the government should actively participate in legal and political processes within the EU to work for better privacy regulations.
- The *Privacy Commission* recommends that expertise be built up in EU and EEA law within the public administration, to ensure solid processes in legislative work.
- The *Privacy Commission* believes that the government must pursue an active legislative policy to promote privacy. It should always be an ambition to use the Norwegian national discretion provided for by EEA legislation, both to *supplement* the European rules and to *support* and *strengthen* current EEA legislation that the Norwegian authorities regard as being particularly important. Where appropriate, the Norwegian authorities should adopt *deviating Norwegian rules* if there is access and sufficient reason to do so.
- The *Privacy Commission* believes that there is *a general need* to clarify the legal basis for the processing of personal data linked to the public sector. Legal clarification is in line with the fundamental principles of the rule of law, because it contributes to a greater degree of predictability and verifiability. In addition, statutory regulation means that any future wishes regarding revised and expanded access to process personal data will require further political decisions. Thus, key privacy issues also become part of the political and democratic shift of opinion, which the *Commission* considers to be valuable in itself.
- The *Privacy Commission* believes that consideration must be given to whether or not national rules should be issued which either maintain or introduce new conditions for the processing of genetic, biometric and health-related data.
- The *Privacy Commission* believes that special protection must be afforded to persons who are exposed to fully automated decisions in line with the provisions of the Regulation. Relevant guarantees could for example be stricter requirements regarding justification of the decisions that machines generate. Documentation of the system may also be an appropriate guarantee, possibly in combination with schemes for the manual assessment and review of the content of the system solution itself.
- The *Privacy Commission* believes that there is a need for regulations which ensure adequate documentation and transparency in automated decision-making processes. Documentation is a prerequisite for ensuring that individuals, where necessary with the aid of a non-profit organisation or lawyer, are *actually* able to dispute the outcome of automated decisions and have grounds for appealing the decision.
- The *Privacy Commission* recommends that the national access to clarify who is responsible for compliance with privacy regulations must be actively utilised. In the event of any doubt as to who the controller is, provisions concerning this should therefore be laid down in legislation or regulations, as provided for by the Regulation.
- The *Privacy Commission* believes that the government should facilitate the establishment of non-profit organisations with the general aim of promoting privacy and data protection. It is important that national rules are laid down which clarify the requirements that apply to the

establishment and work of such organisations. Such a national regulatory framework should also clarify whether, and if so how and to what extent, non-profit organisations may act on behalf of data subjects without their authorisation. This will place particularly strict requirements on the appropriate organisation and operation of such associations, which will require further legal clarification.

- The *Privacy Commission* believes that the government should pursue an active policy to promote pan-European rules. Where this will not be possible or realistic within a reasonable time frame, the government should propose national provisions. Such regulations should preferably be proposed following consultation with other countries in the EEA.
- The *Privacy Commission* believes that, if used cautiously, information provisions in Norwegian national legislation could be one of a number of instruments for creating greater coherence between the General Data Protection Regulation and other relevant regulations. In particular, there may be reason to utilise this method in legislation concerning individual rights which must be clear and comprehensible to a large number of people without any legal education. The approach can also be considered in the context of regulations that concern obligations which many small and medium enterprises must comply with.

Chapter 11
Technology in the service of privacy

Summary of the Norwegian Privacy Commission's recommendations

- The *Privacy Commission* believes that the supervisory authorities should advise private individuals on how to use technology to protect themselves against unlawful or unwanted processing, including by providing specific instructions for relevant tools.
- The *Privacy Commission* believes that measures should be implemented to create clearer obligations to use privacy by design in technical and organisational solutions. The *Commission* is unsure regarding the extent to which such clarification is permitted within the framework of the General Data Protection Regulation. However, the *Commission* believes that the obligation can be made clearer and more concrete when the basis for the processing of personal data is «a legal obligation», «a task carried out in the public interest» and «the exercise of official authority»; see Article 6 (1) (c) and (e) of the General Data Protection Regulation.
- The *Privacy Commission* believes it is important to specify privacy by design obligations in concrete terms in order to promote transparency in the processing of personal data.
- The *Privacy Commission* believes that provisions setting out clear obligations regarding privacy by design should be incorporated in the new Public Administration Act.
- The *Privacy Commission* believes that an obligation should be established for educational institutions to have access and information procedures for pupils and students. Such obligations could, for example, be laid down in the Education Act and the Universities and University Colleges Act.
- The *Privacy Commission* recommends that the Norwegian authorities stimulate the development of Norwegian privacy technology. Measures could include procurement requirements in the public sector, research funding to promote privacy-enhancing technologies, and funding through various grant schemes.

Chapter 12
Transparency

Summary of the Norwegian Privacy Commission's recommendations

- The *Privacy Commission* believes that transparency is such a key precondition that full explainability must be the clear starting point, and lower standards should only be accepted when the impacts are considered to be insignificant.
- The *Privacy Commission* believes that government agencies and other influential social actors must at all times have as one of their most important tasks the strengthening of transparency relating to the application of digital technology with a direct bearing on citizens' obligations, rights, freedoms and opportunities.
- The *Privacy Commission* believes that controllers should to a greater extent than is the case today make available information relating to the processing of personal data. It should be a goal to ensure that data subjects and other interested parties are able to gain access to information independently of others, through the information being made available online, without this requiring the individual to request access from the controller or the controller to inform the individual data subject specifically.
- The *Privacy Commission* believes that accessibility should apply as a general rule at both individual level and collective level. Insofar as is permitted by the GDPR, individuals should have direct access to personal data through secure login routines. In this context, ensuring the confidentiality, integrity and availability of the data is in itself a privacy challenge. However, the *Privacy Commission* believes that the same types of security measures that currently apply to logging in to banking services, Altinn and the summary care record, for example, will be sufficiently secure for the vast majority of other services and associated personal data.
- The *Privacy Commission* emphasises that a requirement to use plain language must apply generally to all relevant operators, and to all information that is important for the protection of people's privacy. Important information should be made available to everyone, regardless of whether or not they are an active participant in the digital society.
- The *Privacy Commission* believes that responsiveness should be developed into genuine *participation* insofar as is possible. By this, the *Commission* means that data subjects, or their representatives, should be actively *invited* to participate in processes that have a direct bearing on how personal data is processed.
- The *Privacy Commission* believes that an overview should be established of administrative decisions relating to the enforcement of the privacy regulations. In connection with the establishment of such an overview, consideration should be given to the entities that are covered by the controls, and how this can be alleviated through the form in which the overview is established, e.g. by preventing indexing or permitting the names of enterprises to be omitted from published overviews in certain cases. This must not be seen as a restriction on access to public information in individual cases under the Freedom of Information Act.
- The *Privacy Commission* believes that updated and systematic records should be made available with information on the extent to which and in what way the Norwegian Data Protection Authority exercises its authority. This applies to individual decisions generally, administrative fines and decisions concerning coercive fines.
- The *Privacy Commission* believes that controllers should *make available* information relating to the processing of personal data to a greater extent than is currently the case. It should be a goal to ensure that data subjects and other interested parties are able to gain access to information independently of others, by ensuring that the information is readily accessible in a way that is easy to understand. Advanced pro-

cessing of personal data should be described in layers, so that the information covers citizens with different skills and different interests in the details of the processing.

- The *Privacy Commission* believes that the Norwegian Digitalisation Agency's report is very apposite and should be incorporated as a key part of the national privacy policy proposed by the *Commission*.

Chapter 13
Guidance, supervision and complaints

Summary of the Norwegian Privacy Commission's recommendations

- The *Privacy Commission* recommends that the government work to establish supervisory authorities at European level with the authority and responsibility to ensure the effective enforcement of privacy legislation with regard to the global platform players, similar to the provisions that have been incorporated into the Digital Markets Act.
- The *Privacy Commission* believes that regular evaluations of the Norwegian Privacy Appeals Board should be carried out. These evaluations should consider whether the board is well-functioning and performing its functions adequately.
- The *Privacy Commission* believes that there is a clear need to strengthen the Norwegian Data Protection Authority. However, privacy cannot only be ensured by a strong, central supervisory authority. The *Privacy Commission* therefore believes that the prerequisites necessary to enable other social actors to contribute to sound data protection must also be strengthened at the same time.
- The *Privacy Commission* is of the view that it is very positive that Norwegian supervisory authorities are working together to protect consumer rights. This cooperation should be secured for the future.
- The *Privacy Commission* believes that other supervisory authorities with responsibilities that are of great and direct importance to the protection of privacy could play a greater role in privacy than they do at present. For example, the Norwegian Labour Inspection Authority must be able to supervise the control measures implemented by employers pursuant to the provisions of the Working Environment Act, and at the same time apply the general provisions of the General Data Protection Regulation that become relevant as a result of the control measure.
- The *Privacy Commission* believes it is important to establish a clear framework for guidance and supervision respectively within the Norwegian Data Protection Authority. The *Commission* believes that it may be appropriate for the supervisory authority to organise itself in such a way that controllers are not at risk of being subjected to supervision as a result of information which originates from a dialogue linked to guidance provided to the entity by the Norwegian Data Protection Authority.
- The *Privacy Commission* believes that if the Norwegian Data Protection Authority's sandbox is to be continued, the questions that are considered in each project should be openly presented for comment before any conclusions are reached. In the conclusions, strong emphasis should also be placed on eliciting assumptions and any doubts relating to the conclusions. At a general level, reports should be structured in such a way that they are not perceived as being advance decisions wherever possible.
- The *Privacy Commission* furthermore believes that authorities other than the Norwegian Data Protection Authority should provide guidance regarding privacy issues that are directly linked to their area of authority. This will be crucial to ensure that these authorities take privacy into account in their operations. The *Commission* stresses that such guidance would be in addition to the guidance issued by the Norwegian Data Protection Authority. Furthermore, the Norwegian Data Protection Authority will always have supervisory competence.
- The *Privacy Commission* believes that all administrative bodies should be given clear advisory responsibility in Section 11 of the Public Administration Act regarding issues that relate to the processing of personal data within their respective areas of authority. Any expansion of advisory responsibility must not interfere with the Norwegian Data Protection Authority's statutory advisory responsibility.

- The *Privacy Commission* recommends that systematic efforts be initiated to strengthen the work of the sector-based supervisory authorities relating to the privacy regulations, and to clarify the legal basis for such exercising of authority.
- The *Privacy Commission* is of the opinion that Article 36 (4) presupposes a specific duty to consult. The provision cannot be considered to have been complied with by giving the Norwegian Data Protection Authority the opportunity to act as a consultative body in line with the right of every entity and citizen in accordance with the Instructions for the Preparation of Central Government Measures (Official Studies). It is in any case incumbent on the government to examine legislation both as comprehensively and thoroughly as is necessary, and in a balanced, systematic and comprehensive manner when the issues are fundamental in nature.
- The *Privacy Commission* believes that the Norwegian Data Protection Authority must be given access to early involvement in legislative and regulatory matters that raise fundamental questions regarding privacy and when there is a strong threat to fundamental rights and freedoms. In the view of the *Privacy Commission*, ensuring that the Norwegian Data Protection Authority's views become known at an early stage in the legislative process would obviously result in the most balanced case study. Arguments relating to the protection of privacy that come up at an early stage in the process are normally easier to take into account than views that are expressed during the public consultation round.
- The *Privacy Commission* recommends that all the Norwegian Data Protection Authority's consultation statements be made publicly available on the Authority's website. Although the statements will normally be made available on the relevant ministry's consultation pages, it is essential that such statements are available in a collated and updated form at all times.
- The *Privacy Commission* believes that it is unfortunate that the Personal Data Act does not clearly state the right of data subjects to have questions considered and reviewed. Such clarification is important for strengthening the legal position of data subjects.

Published by:
Norwegian Ministry of Local Government and
Regional Development

Additional copies may be ordered from:
Norwegian Government Security and Service
Organisation
publikasjoner.dep.no
Telephone: + 47 22 24 00 00
Publications are also available on:
www.government.no

Photo: Colourbox

Print: Aksell as 04/2023