The Legal 500 & The In-House Lawyer
Comparative Legal Guide
Norway: Technology

This country-specific Q&A provides an overview to technology laws and regulations that may occur in Norway.

It will cover communications networks and their operators, databases and software, data protection, AI, cybersecurity as well as the author's view on planned future reforms of the merger control regime.

This Q&A is part of the global guide to Technology. For a full list of jurisdictional Q&As visit http://www.inhouselawyer.co.uk/index.php/practice-areas/technology

Country Author: Brækhus Advokatfirma DA

The Legal 500

Christian Bendiksen, Partner

bendiksen@braekhus.no

The Legal 500

Alexander Mollan, Associate

mollan@braekhus.no

1. **Are communications networks or services regulated? If so what activities are covered and what licences or authorisations are required?**

   Electronic communication networks and services are governed by Act no. 35 of 23 May 2003 on certain aspects of Electronic Commerce and other Information Society Services (the E-commerce Act), the Regulation on Electronic Communication Networks and Electronic Communication Services of 16 February 2004 no. 401 (the Ecom Regulation) and Act no. 83 of 4 July 2003 on Electronic Communications (the Electronic Communications Act).

The Electronic Communications Act governs all activities related to electronic communications and associated equipment, irrespective of its underlying technology. Such activities may include the provision of mobile phone services, internet, satellite communications or radio and TV (including cable).

The Norwegian market for electronic networks and communication services is open for all, without any requirement of licences or authorisations. However, the Ecom Regulation Section 1-2 requires operators of electronic communication networks, public telephone services and leased capacity providers to register with the Norwegian Communications Authority (Nkom), prior to commencing their activities.

2. Is there any specific regulator for the provisions of communications-related services? Are they independent of the government control?

The Norwegian Communications Authority (Nkom) is tasked with ensuring the compatibility of electronic communication services and equipment in Norway, hereunder that the requirements laid down in or pursuant to the Electronic Communications Act are fulfilled.

As a sectoral authority, Nkom is subject to the Norwegian Ministry of Transport and Communications, who may instruct Nkom to deal with cases within the scope of the Electronic Communications Act.

3. Does an operator need to be domiciled in the country? Are there any restrictions on foreign ownership of telecoms operators?

An operator does not need to be domiciled within Norway. However, all operators subject to a duty of registration (see question 1) are required to have a Norwegian organisation number and a Norwegian postal address.

There are no restrictions on foreign ownership of telecommunication operators.

Are there any regulations covering interconnection between operators? If so are these different for operators with market power? What are the principal consumer protection regulations that apply specifically to telecoms services?

The Electronic Communications Act and the Ecom Regulation governs the interconnection between operators of electronic communication services. Section 4-2 of the Act prescribes that any operator with access to electronic communication networks and services is entitled and obligated to negotiate with other operators on the interconnection of the aforementioned services.

Section 4-1 of the Act prescribes that Nkom may oblige an operator with significant market power to meet any reasonable request from another operator to enter into or amend an agreement regarding access to electronic communication networks and services.

In determining whether a request is considered reasonable, an assessment shall be undertaken inter alia of the operator's interest in controlling their own infrastructure against the need to provide access to other operators, enabling them to offer competing services.

When necessary to secure all-in-all communication, Nkom may impose interconnectivity obligations on any operator, regardless of market power. Such interconnectivity obligations may include an obligation to enter into an agreement with another operator.

The E-commerce Act, the Ecom Regulation and the Electronic Communications Act provides operators of telecommunication services with certain duties towards their end users, hereunder informational duties and requirements pertaining to an agreement between the aforementioned parties, inter alia.

5. What legal protections are offered in relation to the creators of computer software?

4. The main rule under Norwegian law prescribes that the person who creates intellectual property has copyright to the work, cf. Act no. 2 of 12 May 1961 relating to Copyright in

Literary, Scientific and Artistic Works (the Copyright Act) Section 1. The aforementioned Section first paragraph no. 12 specifically defines computer software as falling under the act's definition of intellectual property.

Where an employee creates a computer software during the performance of tasks for, or in accordance with the instructions of, an employer, the copyright to such computer software shall befall the employer unless otherwise agreed, cf. the Act Section 39g.

As such, the employer is granted the exclusive right to dispose of the computer software and will be entitled to produce copies of the computer software or otherwise make available, modify or transfer the rights to said software, cf. the Act Sections 39 and 39h.

Computer software are also excluded from the right to produce copies of published copyrightable work for private and non-commercial use or to use such work for commercial educational purposes, cf. Sections 12 first and second paragraph letter b and 21 first and third paragraph.

6. Are specific intellectual property rights in respect of data/databases recognised?

Norwegian law recognises specific intellectual property rights in data/databases, which is protected under the Copyright Act Section 43 first paragraph. The aforementioned paragraph and Section 39 prescribes that anyone who produces a database or similar work that aggregates a large amount of information, or which results from a substantial investment, shall have the exclusive right to use all or substantial parts of the content of the database by producing copies of it, making it accessible to the general public or transfer such rights to another entity.

Database rights are also excluded from the right to produce copies of published copyrightable work for private and non-commercial use or to use such work for commercial educational purposes, cf. the Act Sections 12 first and second paragraph letter c and 21 first and third paragraph.

7. What key protections exist for personal data?

Act no. 31 of 14 April 2000 relating to the Processing of Personal Data (the Personal Data Act) Section 1 prescribes that the Act shall protect data subjects from violation of their rights to privacy through the processing of personal data and help to ensure that personal data are processed in accordance with the subjects fundamental rights to privacy.

As the Act has implemented Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the data subjects are offered the Directive's key protections such as the requirements of:

- A lawful basis to process personal data;
- explicit, lawful and specified purpose that restricts the processing of personal data to said purpose;
- adequate, relevant and not excessive processing of the personal data;
- accurate and, where necessary, up to date personal data;
- personal data not being stored longer than necessary for the achievement of the stated purpose;
- appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of, or the accidental loss or destruction of, or damage to, personal data; and
- limitations on the transfer of the personal data to other countries.

8. Are there restrictions on the transfer of personal data overseas?

The Personal Data Act Chapter V governs the transfer of personal data to other countries. Section 29 of the Act prescribes that the transfer of personal data to another country mandates that said country is capable of ensuring an adequate level of protection of the data in question. The assessment of the adequacy of the level of protection shall be based on the nature of the personal data, the purpose and duration of the proposed processing and the rules of law and the professional rules and security measures that apply in the country in question.

Countries that have implemented Directive 95/46/EC are deemed to fulfil the requirement with regard to an adequate level of protection. These include the 28 EU

countries and the three EEA member countries (Norway, Liechtenstein and Iceland).

Furthermore, the European Commission has determined, through a series of Commission decisions, that a number of countries fulfil the abovementioned requirement. At the time of the publication of this guide, these countries include Andorra, Argentina, Canada (commercial organisations), the Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

Where a Norwegian entity wishes to transfer personal data to a receiving party in the United States, such transfer is allowable where the receiving party is certified under the EU-U.S. Privacy Shield Framework, cf. https://www.commerce.gov/tags/eu-us-privacy-shield for a complete list of all certified entities.

Except as provided above, the transfer of personal data overseas usually entails an application to the Norwegian Data Protection Authority, providing safeguards for the protection of the rights of the data subject concerned. Depending on the situation, the transferring party may choose to utilise the EU Model Contracts for the transfer of personal data to third countries. By using the Model Contracts for the transfer of personal data to a data processor, the transferring party need only to notify the Data Protection Authority of the transfer itself.

Where the transfer is between a group of companies, the transferring party may choose to transfer the personal data under Binding Corporate Rules (BCR). While not mentioned in the Directive 95/46/EC nor the Personal Data Act, BCR is usually accepted where they provide sufficient safeguards for the protection of the rights of the data subject concerned. The Data Protection Authority, as well as at least one other Data Protection Authority within the European Economic Area, must approve the BCR prior to it being used as basis for the transfer of personal data.

In accordance with Section 30 of the Act, personal data may also be transferred to countries that do not ensure an adequate level of protection if, inter alia, the data subject has consented to the transfer or the transfer is necessary in order to establish, exercise or defend a legal claim.

The Data Protection Authority may allow the transfer of personal data even if the aforementioned requirement are not fulfilled, where the data controller provides adequate safeguards with respect to the protection of the rights of the data subject. The Data Protection Authority may stipulate requirements for the transfer.

9. What is the maximum fine that can be applied for breach of data protection laws?

The Data Protection Authority may issue orders to the effect that violation of provisions laid down in or pursuant to the Personal Data Act shall result in a fine to the Treasury of maximum 10 times the National Insurance Basic Amount, currently NOK 936 340.

10. Are there any restrictions applicable to cloud-based services?

Norwegian law imposes several restrictions on the provision and use of cloud-based services.

Cloud-based services that processes personal data are governed by the Personal Data Act, cf. question 7 for further information. A common issue with cloud-based services is their conformity with the rules and regulations on the transfer of personal data to another country, cf. question 8 on the restrictions pertaining to such transfer.

Where an administrative body utilises cloud-based services in its internal administrational work or to communicate with private individuals or other administrative bodies, the Regulation on Electronic Communication with and in the Government Administration of 25 June 2004 no. 988 provides certain rules on security. Of interest to an administrative body’s use of cloud-based services, the Regulation prescribes requirements pertaining to risk assessment, access control, and the safeguard of confidential information.

Furthermore, the Norwegian National Archive has stated that Act no. 126 on Archives of 4 December 1992 Section 9 letter b prohibits the transfer or storage of the archive databases or security copies thereof by cloud providers who store the material in another country, without prior consent from the Norwegian National Archive.

Act no. 73 of 19 November 2004 relating to Bookkeeping (the Bookkeeping Act) Section 13 second paragraph prescribes that as a main rule, accounting materials must be stored within Norway. Exceptions are provided for the permanent storage of such materials in Denmark, Finland, Sweden or Iceland. Where entities are subject to the rules for the financial management of administrative bodies, the storage of accounting materials outside of Norway is strictly prohibited.

11. Are there specific requirements for the validity of an electronic signature?

Act no. 81 of 15 June 2001 on Electronic Signatures (the E-signatures Act) Section 3 no. 1 defines an electronic signature as data in electronic form which are attached to or logically associated with other electronic data and which serves as a method of authentication.

The Act differentiates between different types of electronic signatures. The most commonly used form of electronic signature within Norway is the advanced electronic signature, which requires that the electronic signature be:

- Uniquely linked to the signatory;
- capable of identifying the signatory;
- created using means that the signatory can maintain under his sole control; and
- linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

A qualified electronic signature is an advanced electronic signature that is based on a qualified certificate and produced by an approved secure signature creation system, cf. the Act Section 4. Providers of qualified electronic signatures and certificates are subject to requirements in the Act Chapter III and the Regulation on the Requirements of Qualified Certificates of 15 June 2001 no. 611, as well as the supervision of Nkom.

Where law, regulation or other instruments prescribes that a signature is a requirement necessary to obtain a specific legal effect, and such act can be conducted electronically, a qualified electronic signature shall always be deemed to fulfil such a requirement, cf. the Act Section 6. Furthermore, an electronic signature that is not qualified may also

fulfil such requirement.

Digital signatures are the most commonly used form of electronic signatures. A digital signature must be linked between a physical person and the electronic data, and requires an electronic certificate consisting of information of the signatory (the private key) and a public key, in which the latter is linked to a certificate that confirms the signatory's identity to other parties. The Act prescribes that the private key must be under the certificate holder's control, for instance as a plastic card or a data chip (smartcard).

12. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

When outsourcing IT services, a company will decide which assets, resources or otherwise it will transfer to the outsourcing company. The parties will then enter into an outsourcing service contract, which governs the sale or disposal of rights to systems, source code, infrastructure, personnel and other intellectual property rights or assets. As such, the transfer of employees, assets or third party contracts is contingent on the parties understanding as stipulated in their outsourcing service contract. The transfer of third party contracts may also be subject to assignment clauses contained in such contracts.

13. If a software program which purports to be an early form of A.I. malfunctions, who is liable?

When the liability is a question between the software provider and a purchasing party, the allocation of liability would primarily depend on the contract between these parties and/or mandatory consumer protection law, where applicable. If no such regulation exist, is lacking or if the question of liability concerns a third party, the allocation of liability would be decided by either Act no. 27 of 13 May 1988 on the Sale of Goods, non-statutory contract or tort law or otherwise applicable laws and regulations.

The choice of applicable law depends on how the software was provided, how and when the malfunction manifested itself, the consequences of said malfunction and an assessment of the respective parties' degree of culpability.

For instance, if a company or consumer purchased the software on a physical disk, the Sale of Goods Act or Act no. 34 of 21 June 2002 on Consumer Protection would usually apply. Under these Acts, software malfunctions would normally constitute a defect that could give grounds for the purchasing party's claims of repair, replacement or price reduction etc. While compensation may also be claimed in such instances, the aforementioned acts disclaims indirect losses as unallowable.

14. What key laws exist in terms of obligations as to the maintenance of cybersecurity?

Cybersecurity is primarily a private matter and responsibility for organisations and other entities. However, certain laws and regulations prescribes duties relating to cybersecurity.

The Personal Data Act Section 13 prescribes that the data controller and the data processors shall, by means of planned and systematic measures, ensure satisfactory data security with regard to confidentiality, integrity and accessibility in connection with the processing of personal data. To that end, the aforementioned parties shall document their data system and security measures. Such documentation shall be available to the employees of the aforementioned parties, as well as the Data Protection Authority and the Privacy Appeals Board. Furthermore, the Regulation on the Processing of Personal Data of 15 December 2000 no. 1265 Chapter 2 imposes several duties on the data controller with regard to risk assessments, security revisions or other organisational, physical, procedural or technical measures suitable for preventing the loss, misuse, unauthorised access, disclosure, or modification of any personal data.

Other laws and regulations providing similar requirements on cybersecurity are the Electronic Communications Act and Act no. 10 of 20 March 1998 on Preventive Security Service (The Security Act).

15. What key laws exist in terms of the criminality of hacking/DDOS attacks?

Attacking a website via a denial of service attack, a distributed denial of service attack, or otherwise engaging in conduct that could damage, disrupt, impair or interfere with a website, computer system, server or database, is a criminal offence under the

Norwegian General Civil Penal Code of 20 May 2005 no. 28 Sections 351 or 352. Depending on the severity of the attack, the offence may carry a penalty of fines and/or up to six years in prison.

The aforementioned Act Sections 201 and 204 governs the act of hacking. In accordance with Section 201, the unlawful manufacture, acquirement, possession or distribution of passwords, other information or malicious software carries a penalty of fines and/or up to 1 year in prison.

Gaining unauthorised access to a website, password, computer system, server, and database or otherwise is punishable with up to two years in prison, cf. the Act Section 204.

16. What technology development will create the most legal change in the jurisdiction?

Artificial intelligence as a means of analysing Big Data or providing services that applies machine learning will greatly affect the Norwegian legal system and necessitate a significant number of changes with regard to liability and the assignment of rights and obligations. For instance, Norwegian law would have to be amended in order to solve legal issues concerning the allocation of intellectual property rights of AI created intellectual property, product liability of autonomous vehicles or robots, smart contract management and the certification and liability of medical and health care diagnostics and procedures conducted by AI and robots, inter alia.

17. Which current legal provision/regime creates the greatest impediment to economic development/ commerce?

While it is difficult to pinpoint an exact legal provision as the greatest impediment to economic development/commerce within Norway, a number of Acts can be deemed as impeding the economic development caused by digitalisation, for instance by imposing requirements on physical and/or original documentation or identification in matters pertaining to insurance, accounting, debt enforcement, money laundering and financial agreements etc.

18. Do you believe the legal system specifically encourages or hinders digital services?

On a general note, the Norwegian legal system encourages the provision and use of digital services. As a result, Norway is considered an early adopter of new technology. Furthermore, Norway has implemented a large number of Acts governing the use of digital services and technology.

It also bears mentioning that the Norwegian Government has devoted its attention to the provision and use of new digital services provided by the sharing economy. On 6 February 2017, the government-appointed Committee on the Sharing Economy published their report on, inter alia, new technologies that might change the economy by; lowering the transactional costs associated with entering into contracts and complete transactions, creating new market- and business models, streamlining the utilisation of resources such as transportation vehicles, tools, or other property, and creating new employment opportunities. The Committee proposed several changes in legislation, and encouraged the Norwegian Tax Authority and the Ministry of Finance to examine these challenges.

19. To what extent is the legal system ready to deal with the legal issues associated with artificial intelligence?

While Norway does have a strong IT-environment, its legal system is not currently equipped to deal with the potential legal issues that would arise out of AI.

For instance, the current laws and regulations relating to the processing of personal data does not necessarily pose any hurdles on the analysis of pseudonymised and aggregated data by AI. However, the details surrounding such analysis remains unclear, hereunder the breadth and traceability of the data collected, the determination of who has used the data, the right of access, or the requirements of pseudonymisation.

Furthermore, the debate on the allocation of ownership rights of such data is still ongoing in Norway, hereunder whether such rights shall befall the party collecting the data or the party conducting the analysis.

Lastly, contract and torts law is unequipped to deal with potential issues of product liability of autonomous vehicles or robots, or malfunctions or malice in the provision of health services by AI and robot diagnostics.