DENMARK – COUNTRY REPORT

Background

This report outlines the main laws which provide law enforcement and intelligence agencies with legal powers in relation to lawful interception assistance, the disclosure of communications data, certain activities undertaken for reasons of national security or in times of emergency, and censorship of communications under Danish law.

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Consolidation Act on Electronic Communications Networks and Services, 2014

(Bekendtgørelse af lov om elektroniske kommunikationsnet og –tjenester (Act no. 128 of 7 February 2014, (the "Tele Act"))

The Tele Act, in conjunction with the Retention Order (described in section 2 of this report below), sets out a telecom provider's obligation to make data available to the police, both by providing access to retained data and by providing interception capabilities.

According to section 10 Tele Act, a network operator or service provider must ensure that all technical equipment and systems used to provide an electronic communication network or service to end-users are set up in such a way that the police may intercept current communications and conduct mobile phone surveillance. In this context, mobile phone surveillance means the procurement of data that makes it possible to locate a mobile phone on a continuous basis as long as it is turned on.

Under section 10, the systems of the network operator or service provider must be set up to allow interception and immediate transmission of telecommunications data to another EU member state under the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01).

In the case of a data interception request, the network operator or service provider must provide the IP-address, MAC-address or any similar identifier of the device making or receiving the communications that are to be intercepted.

1.2 Administration of Justice Act 2016 (Bekendtgørelse af lov om rettens pleje (Act no. 1257 of 13 October 2016, (the "AJA"))

Section 783 sets out the general rule that the police must obtain a court order and present it to the relevant network operator or service provider before an interception may be made. The application for a court order must comply with the following conditions:

- there must be specific indications that communications, using the method of communication that is to be intercepted, are taking place to or from a suspect of the investigation;
- the interception must be decisive to the investigation; and
- the alleged offence must have a sentence of at least six years' imprisonment, or be one of a list of specified offences, such as desertion from the military or possession of child pornography.

In addition, interception must always be proportionate to the purpose for which it is to be used.

Section 783(4) provides for an exception to the general rule. Where obtaining a court order would cause a delay that would defeat the purpose of carrying out the interception, the police may conduct the interception without obtaining a court order first.

However when this happens, the police must, as soon as possible and no later than 24 hours from the interception, submit an application for a court order for the interception as set out above. The court then determines whether the interception was lawful, and if so, the length of time it should be allowed to continue. If the court finds that the interception was not lawful, it is obliged to notify the Ministry of Justice, which has statutory authority to investigate any breach of this

process by the police.

1.3 Centre for Cybersecurity Act 2014 (Lov om Center for Cybersikkerhed (Act no. 713 of 25 June 2014, (the "Centre for Cybersecurity Act"))

The Danish Centre for Cybersecurity (the "Centre") is the national IT Security authority who has established a "network security service" (the "Service") to which companies whose businesses have a socially important function, such as pharmaceutical companies, food companies and companies that administer administrative IT-systems, as well as most public institutions, can apply for connection. Through the Service, the Centre aims to discover, analyse and prevent cybersecurity breaches within the connected entities in order to maintain a high level of information security in Denmark, for example, to prevent hacking.

In order to connect to the Service, the relevant company or public institution must enter into an affiliation agreement with the Centre. Once connected, the Centre may process content and traffic data in the networks of the connected entities to the Centre's Service, without obtaining a court order, so long as such interception is made with the purpose of ensuring a high level of information security. The Centre cannot connect a company or institution to the Service unless such a company or institution actively asks to be connected. Further cybersecurity related provisions under the Centre for Cybersecurity Act are explained in section 7 of this report.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Executive Order on the retention and storage of traffic data by providers of electronic communications networks and services (Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) (No. 988 of 28 September 2006, as ame nded by executive order of amendment no. 660 of 19 June 2014, (the **"Retention Order"**))

The Retention Order governs what data must be stored by a network operator or service provider.

Under section 5(1), a network operator or service provider must retain the following data about a user's access to the internet:

(a) the allocated user identity (for example, the user name or customer number);

(b) (b) the telephone number which has been allocated to the user's communications as a part of a public electronic communication network;

(c) (c) the name and address of the subscriber or registered user to whom an IP address or user identity or telephone number had been allocated at the time of communication; and

(d) (d) the time of the beginning and the end of a communication.

Under section 5(2), a network operator or service provider providing wireless access to the internet must retain data concerning the local network's precise geographical or physical location and the identity of the user's communication equipment. Data retained under the Retention Order must be stored for one year.

2.2 Consolidation Act on Electronic Communications Networks and Services 2014 (the "Tele Act")

According to section 10 Tele Act, a network operator or service provider must ensure that all technical equipment and systems used to provide an electronic communication network or service to end-users are set up in such a way that the police may obtain access to information about telecommunications traffic in the form of;

- telecommunications data, meaning information regarding which telephones or similar communications devices have been connected to a specific telephone or similar communications device either prior to or after the issue of an authorising court order; and
- extended telecommunications data, meaning information listing the connections made by the telephones or similar communication devices within a defined area (described by the police) either prior to or after the issue of an authorising court order (this would typically be information from cell phone masts).

Under section 13, when required by the police, network operators and service providers are obliged to disclose to the police data which identifies an end-user's access to electronic communications networks or services. This includes static information such as a designated IP-address, address, or phone number that the network operator or service provider has assigned to the end-user. The police can lawfully obtain this information without obtaining a court order.

A network operator or service provider which offers encrypted data as an integrated part of its service is obliged to decrypt an encrypted communication when complying with a court order. If, however, encryption has taken place outside of the services offered by the network operator or service provider, it will be the police's own responsibility to remove any encryption from the provided data.

It is prohibited for network operators and service providers to retain content data. However, the police may retain, access and review the content of a person's correspondence, subject to the rules on lawful interception outlined in section 1 of this report above.

2.3 Administration of Justice Act 2016 (the "AJA")

The police may obtain access to historic telecommunications data in accordance with chapter 71 AJA. Section 783 sets out the general rule that, in order to do so, the police must obtain a court order and present it to the relevant network operator or service provider. The application for a court order must comply with the following conditions:

- there must be specific indications that communications are

taking place to or from a suspect of the investigation using the method of communication that is to be intercepted;

- access to the relevant telecommunications data must be decisive to the investigation; and
- the alleged offence must have a sentence of at least six years' imprisonment, or be one of a list of specified offences, such as desertion from the military or possession of child pornography.

In addition, access to historic telecommunications data must be proportionate to the purpose for which it is to be obtained.

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 Radio Frequencies Act

(Act no. 1100 of 10 August 2016, Lov om radiofrekvenser (the "RFA")), and the Order on maritime radio services in extraordinary situations (Bekendtgørelse om de maritime radiotjenester i ekstraordinære situationer (Executive order no. 916 of 13 November 2002, (the "Maritime Radioservice Order"))

According to section 32 RFA and the Maritime Radioservice Order, the Danish Navy Operative Command may, in situations of crisis, war, catastrophes and other extraordinary situations, shut down the coastal radio station and thus shut down normal public correspondence over coastal radio.

In accordance with section 33 RFA, the Danish Energy Agency (the "DEA"), who acts as the regulatory supervisory authority for the telecoms industry under the remit of the Danish Ministry of Energy, Utilities and Climate, may prohibit the use of certain radio frequencies when the safety of the state demands it.

Under section 6(5) of the RFA, the police, when exercising a power to disturb or interrupt radio and telecommunications that is granted under section 791(c) of the Administration of Justice Act, may do so without first obtaining a licence or other authorisation from the DEA to use the radio frequency spectrum in question.

3.2 Network and Information Security Act

(Net- og informationssikkerhedsloven (Act no. 1567 of 25 December 2015, (the "Network and Information Security Act"))

In 2016, the Network and Information Security Act, a framework regulation, was enacted. Following this the Centre has drafted new regulations on network and information security, including the 'Information and Security Order' (Bekendtgørelse om Informationssikkerhed og beredskab i net og tjenester) (Executive Order Number 567 of 1 June 2016) under which a provider of public electronic communications networks or services is responsible for information security in its network based on a documented risk management process. A provider must identify any possible cybersecurity risks and using this risk assessment, implement proper measures to ensure the accessibility, integrity and confidentiality of its networks and services. Further cybersecurity obligations under the Network and Information Security Act are set out in section 7 of this report.

The Information and Security Order also governs a provider's obligations in relation to crisis management in emergency situations, such as large disasters, where it may be necessary to implement remedial actions in regards to networks and services in order to maintain critical services. Also, 'significant commercial providers' shall ensure that the Centre can make contact with them in connection with an emergency situation at any time. Centre may also direct such providers to participate in national or international crisis management practices.

In addition to the Information and Security Order, the Centre has also issued the "Emergency Operator Order" (Bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.) (Executive Order Number 564 of 1 June 2016), which sets out certain actions that providers must take in emergency situations, including the prioritization of calls in mobile networks, the provision of secure access to a telephone network and the prioritization of re-establishment of certain parts of a provider's network as directed by the Centre.

4. CENSORSHIP

4.1 The Constitutional Act of the Kingdom of Denmark, 1953 (the "Constitution")

Under section 77 of the Constitution, censorship and other measures prohibiting freedom of expression are prohibited.

4.2 Gaming Act 2016 (Act no. 1494 of 6 December 2016, Bekendtgørelse af Lov om spil, (the "Gaming Act"))

As a general rule, government agencies do not have the authority to block IP addresses. The Telecommunications Industry Association (Teleindustrien) (a private industry organisation of which the majority of Danish network operators and service providers are a part) has stated that network operators and service providers need only carry out DNS blocking following an authorising court order and that they will not carry out any DNS blocking based solely on requests from intellectual property rights holders, government agencies or other third parties.

The only current exception to this is the Danish Gaming Board who may request that a network operator or service provider blocks a website containing illegal gambling systems.

5. OVERSIGHT OF THE USE OF POWERS

5.1 Judicial Oversight

Insofar as a court order is required to intercept or access retained data or to block any website, the competent court will have oversight of this procedure.

5.2 Executive Order on the retention and storage of traffic data by providers of electronic communications networks and services (the "Retention Order")

The Retention Order was issued by the Danish Ministry of Justice (the "Ministry"). The Ministry oversees the compliance of network operators and service providers with the retention and storage requirements specified in the Retention Order. Non-compliance with the Retention Order may lead to financial penalties imposed by the Ministry.

5.3 Consolidation Act on Electronic Communications Networks and Services 2014 (the "Tele Act")

Following the Danish general election in 2015, it was decided to relocate much of the regulation of the telecoms sector from the Ministry of Business and Growth to the Ministry of Energy, Utilities and Climate and accordingly move the main parts of the regulatory authority from the Danish Business Authority (the "DBA") (an agency under the Ministry of Business and Growth) to the Danish Energy Agency (the "DEA") (an agency under the Ministry of Energy, Utilities and Climate).

Consequently, the DEA is now the main regulatory authority responsible for electronic communications who administers the legal framework within this area. This includes promoting information technology security, promoting individual and public use of information technology and the Internet, developing the telecoms market, administering scarce resources, protecting consumers, and protecting public information and communications business.

However, certain areas still remain under the Danish Business Authority (the "DBA"), including matters within telecoms regulations relating to personal data and sector-specific competition regulation.

Both the DEA and DBA therefore oversee compliance by network operators and service providers with the Tele Act. For example, the DEA ensures that electronic communication networks are set up to enable interception by the police. Under chapter 33, section 79 Tele Act, both the DEA and the Telecommunications Complaints Board (the "Board") may enforce compliance and issue financial penalties for breaches of the Tele Act described in this report.

The Board comes under the remit of the Ministry of Energy, Utilities and Climate. Decisions taken by the DEA may be brought before the Board and any decisions taken by the Board may be appealed to the High Court.

5.4 Administration of Justice Act 2016 (the "AJA"))

For the Danish police to conduct a lawful interception, section 783 AJA contains the general rule that they must first obtain a court order to do so. This rule is subject to certain exemptions which allow for an interception to take place without an order provided that the police make a submission to the court within 24 hours of the interception for its retrospective examination. If the court rules that the interception was not in compliance with law, it then notifies the Danish Ministry of Justice of the matter. The Ministry of Justice has statutory authority to investigate such non-compliance by the Danish police.

5.5 Centre for Cybersecurity Act 2014 (the "Centre for Cybersecurity Act")

For interceptions made in accordance with the Centre for Cybersecurity Act, it is the Centre for Cybersecurity (the "Centre") who is solely responsible for determining whether or not to intercept. The Centre is placed under the Danish Defence Intelligence Service, which sits within the Danish Ministry of Defence. In relation to the data processed by the Centre, the Danish Data Protection Act 2000 will not apply (nor does it apply generally to the police). However, the Minister of Justice and the Minister of Defence appoints a supervisory board that supervises the Centre's use and processing of personal data.

5.6 Radio Frequencies Act 2016 (the "RFA") and the Maritime Radioservice Order 2002

Under the RFA, the DEA determines whether consideration to the safety of the state demands the prohibition of the use of certain radio frequencies.

Under the Maritime Radioservice Order, the Danish Navy Operative Command determines whether the coastal radio station should be shut down.

5.7 Gaming Act 2016 (the "Gaming Act")

The Danish Gaming Board oversees compliance by network operators and service providers with the Gaming Act.

5.8 Network and Information Security Act

(Net- og informationssikkerhedsloven (Act no. 1567 of 25 December 2015, (the "Network and Information Security Act"))

The Centre oversees compliance by network operators and service providers with the Network and Information Security Act. The Centre is placed under the Danish Defence Intelligence Security and Intelligence Service which sits within the Danish Ministry of Defence.

6. PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

Restrictions on network operators and service providers

There are no restrictions on whether a network operator or service provider may publish aggregate data regarding government powers of interception, disclosure of communications data or censorship as described in this report. Equally, there are no restrictions on whether a network operator or service provider may publish descriptions or analysis regarding such powers.

Aggregate data published by government agencies

Government agencies do not publish aggregate data in relation to the use of their powers of interception, disclosure of communications data or censorship as described in this report.

7. CYBERSECURITY

7.1 Consolidation Act on Electronic Communications Networks and Services,

(Act Number 128 of 7 February 2014 (the "Tele Act")) and The Executive Order on Personal Data as regards Public Electronic Communications Services, (Executive Order Number 462 of 23 May 2016 (the "EOPD"))

Pursuant to section 7(1) Tele Act, owners of electronic communications networks and providers of electronic communications networks or services and their employees and former employees shall not be entitled, without authorisation, to disclose or utilise information about an individual's use of the network or service in question, or the content thereof that comes to their knowledge in connection with the provision of these electronic communications networks or services. The owners and providers of such networks and services shall furthermore "...take the measures necessary to ensure that information about [an]other persons' use of the network or service or the content thereof will not be available to unauthorised persons."

Section 8 Tele Act contains a framework provision on personal data which has resulted in the EOPD. Pursuant to the EOPD, providers of public electronic communications networks or services must continuously ensure that they implement proper technical and organizational measures to control potential security breaches relating to the personal data that they process. Such measures shall, as a minimum, ensure:

1) (i) that authorized personnel are allowed access to personal data for legitimate purposes only;

2) the protection of stored personal data and personal data in transmission against accidental or unlawful destruction, loss or alteration and against unauthorized or illegal storing, processing, access, or distribution; and

3) that a security policy for personal data is prepared.

4) Providers of public electronic communications networks or services are further obligated to inform their end-users of any event that poses as a particular risk to their personal data security.

All providers must inform the Danish Business Authority (the "DBA") of an actual breach of personal data security within 24 hours of its occurrence. In doing so, they must state in detail the character of the breach, its consequences, and any counter measures they have initiated. Furthermore, if the breach of personal data security can be expected to violate the personal information or privacy of an end-user, the provider must also immediately inform the end-user of this breach.

7.2 The Danish Act on Network and Information Security

(Act Number 1567 of 15 December 2015 Lov om Net-og Informationssikkerhed (the "Network and Information Security Act"))

The Centre for Cybersecurity (the "Centre") has issued four Executive Orders under the Network and Information Security Act, including:

1) the Executive Order on Information Security and Emergency in Networks and Services (Bekendtgørelse om Informationssikkerhed og Beredskab i Net og Tjenester) (Executive Order Number 567 of 1 June 2016) (the "Information and Security Order")); and

2) the Executive Order on Information and Disclosure obligations regarding Network and Information Security" (Bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og Informationssikkerhed,Executive (Order Number 566 of 1 June 2016) (the "NIS Disclosure Order")).

Precautionary measures in terms of Information Security

In addition to the cybersecurity obligations referred to in section 3.2 of this report, under the Information and Security Order, providers of public electronic communications networks or services are responsible for their personal information security based on a documented risk management process.

Stricter rules apply for specific providers, including 'commercial providers' and 'significant commercial providers'. These providers are required to additionally prepare an information security policy approved by their management, based on an international standard such as the DS/ISO/IEC 27001. They are also required to establish an information security organization which is responsible for managing all of the provider's relevant security tasks. Significant commercial providers are additionally subject to a number of general information security obligations, including the obligation to ensure awareness of current information security threats and to implement security plans for the protection of specific critical net components and systems.

Pursuant to section 25-26 of the Information and Security Order, the Centre may issue specific directions to 'commercial providers' and 'significant commercial providers' provided that these directions are of 'material public interest'. Such directions may require the provider to ensure:

1) the security clearance of specific personnel;

2) the retention of certain employees necessary to perform the risk management processes; and

3) the performance of an independent safety valuation.

A disclosure regime is set out in the NIS Disclosure Order. Pursuant to section 7, providers of public electronic communications networks and services are required to notify the Centre of any security breaches that result in significant implications for the operation of their networks and services. A significant implication for the operation of networks and services will occur if the stated threshold values, in terms of the duration of the breach as set out in section 8, are reached (for example, for internet access, the threshold would be met if the security breach results in 10,000 user hours being affected and where the effect lasts longer than one hour). The Centre may in this context issue a specific direction to a provider that it shall inform the general public of the security breach in question provided that the publication is considered as being of public interest, as per section 11.

7.3 Centre for Cybersecurity Act 2014

(Lov om Center for Cybersikkerhed (Act no. 713 of 25 June 2014, (the "Centre for Cybersecurity Act"))

The main regulatory supervisory authorities for the telecoms industry in Denmark in terms of cybersecurity are the Centre for Cybersecurity (the "Centre") and the Danish Business Authority ("DBA"). As referred to in section 1.3 of this report, the Centre for Cybersecurity Act regulates the Centre's 'network security service' (the "Service"), which analyses internet traffic to and from the authorities and companies that are connected to this Service in order to detect any signs of intrusion.

In the event of an unauthorised intrusion and potential cyber-attack, the Centre conducts an advanced analysis to expeditiously determine the nature and severity of the threat. In the case of a specific cyber-attack, the Centre will directly inform the targeted organization and advise them of the measures to take to respond to the attack.

In addition to the above, the Centre also informs and advises on the preventive measures that may be taken and issues guidelines and recommendations on the strengthening of cybersecurity efforts and the prevention of cyber-attacks to Danish public authorities and private companies.

The executive powers provided for under the cybersecurity legislation governing the Centre do somewhat affect an individual's general rights, in particular their right to privacy. However, balancing such human rights with the protection of cybersecurity and resistibility against cyber threats in Denmark has been the subject of well-considered public debate and ultimately such legislation has been deemed necessary and proportionate. Nonetheless, the relevant authorities are subject to clear guidelines in their operations. For example, the Centre may only process data in connection with the 'Network Security Service' provided it is in compliance with the specific guidelines as of 30 June 2014.

Moreover, the 'Danish Intelligence Oversight Board' is a special independent monitoring body that oversees the Centre and ensures that it processes information about natural persons in connection with the Service in a manner that is compliant with the relevant legislation, including when intervening in secret communications. Any decisions made by the Centre may be appealed to the Danish Ministry of Defence.

Non-compliance with the legislation on network and information security is subject to a fine imposed by the Centre or the DBA.

8. CYBERCRIME

The Danish Criminal Code (Straffeloven) (Consolidation Act Number 1052 of 4 July 2016, (the "CC")) considers the following activities as cyber offences under Danish law:

Statutory Reference	Offence	Penalty
Criminal Offences against Property		
Section 291	Attack on IT-system Described as destroying, damaging or removing any property belonging to another person. Note that attacks on IT-systems may comprise of knowingly sending computer viruses and 'denial-of-service-attacks' (i.e. where the owner or holder is cut off any access to operate their IT-system)	A fine or imprisonment for a term not exceeding one year and six months
Section 293(2)	DDoS ('Distributed Denial of Service') Described as wrongfully preventing another person from disposing of an item in full or in part / exposing a computer system to a DDoS (i.e. Distributed Denial of Service) attack If the offence is committed in a systematic or organised manner or in otherwise particularly aggravating circumstances	A fine or imprisonment for a term not exceeding one year Imprisonment for up to two years
Section 279a	Data Fraud Described as wrongfully editing, adding or deleting data or programs for electronic data processing or otherwise wrongfully attempting to influence the output of such data processing, in order to obtain an unlawful gain for himself or others For example where a perpetrator, who gets into an IT-system for account transfers unlawfully transfers amounts to his own account and withdraws the cash	Imprisonment for approximately one year and six months
Various acts harmful to the General Public		
Section 193	Comprehensive interference in the operation of Information Systems Described as wrongfully causing comprehensive interference with the operation of any public transport means, public postal service, telegraph or telephone service, radio or television broadcasting system, information system or service providing public utility of water, gas, electricity or heating Note that this criminal offence is generally targeted at addressing attacks on large IT-systems of social importance (e.g. attacks on high street banks or other big companies) but also attacks on central internet-functions such as DIX and hostmaster It is of no importance how the specific attacks are accomplished. Both hacking minor controlled attacks in the form of virus and physical attacks by way of interruption of a teleconnection will fall within the scope of this criminal offence If the offence is committed through gross negligence	A fine or imprisonment for a term not exceeding six years A fine or imprisonment for a term not exceeding six months

Statutory Reference	Offence	Penalty
Criminal Offences concerning means of payment and evidence		
Section 169, 171 and 301	Described as criminal offences relating to the means of payment and evidence If the act was of a particularly aggravating nature	A fine or imprisonment for a term not exceeding two years Imprisonment for up to six years
Invasion of Privacy		
Section 263(1)	Monitoring or wire-tapping of telecommunication Described as, wrongly, by means of a listening device, secretly wiretapping or recording statements made in solitude, telephone conversations or other conversations between other persons	A fine or imprisonment for a term not exceeding six months
Section 263(2)	Hacking Described as wrongly gaining access to any data or programs of another person intended for use in an information system If the offence is committed with the intent to obtain or become acquainted with the business secrets of an enterprise, or if other particularly aggravating circumstances apply (e.g. organized criminal activities) If the offence is committed in a systematic or organised manner	 A fine or imprisonment for a term not exceeding one year and six months Imprisonment for a term not exceeding six years Imprisonment for a term not exceeding six years

The Danish Ministry of Justice (Justitsministeriet) is responsible for creating legislation concerning the criminal law and is the part of the Ministry who issues any amendments to the Criminal Code.

As a general rule, acts falling within Danish criminal jurisdiction are acts committed within the Danish state, which implies that any criminal offence committed in Denmark can be prosecuted in Denmark, regardless of the perpetrator's nationality.

However, pursuant to section 9 CC, if the criminality of an act depends on or is influenced by an actual or intended consequence, the act is also deemed to have been committed at the place where the effect occurred or where the offender intended the effect to occur (referred to as the 'Principle of Impact'). Consequently, a cybercrime committed outside of Denmark may still end up being subject to Danish criminal jurisdiction.

Any victim (person or a company) affected by the commission of a cybercrime may report this to the Danish Police, and more specifically the National Police Cyber Crime Centre ("NC3"), a special section of the Danish Police. It will be the Danish Prosecution Service (Anklagemyndigheden) however that will make the decision as to whether to press charges against the perpetrator. On a practical note, whilst the prosecutors will work closely with the police officers that investigate the criminal offence, it is the prosecutors who will have to assess whether a case is likely to stand up in court. If so, the prosecutor is to appear before a District Court judge and attempt to have the perpetrator convicted. Any decision made by the District Court judge may be appealed to the High Court or the Supreme Court (which is the highest tier of the Danish legal system).

Law stated as at 21 February 2017.