Nordic Council of Ministers

Data Retention Law in the Nordic Countries

A Comparative Study

Contents

Summary 6

Abbreviations 7

Terms 8

References 13

EU legislation 13

Council of Europe 13

National legislation and legal sources 13

Denmark 13

Finland 14

Iceland 14

Norway 15

Sweden 15

Part 1:
Mandate, EU background and Nordic context 16

1. Mandate 17

2. EU legal background 18

3. The complexity 20

4. Data retention as concept 21

5. Nordic overview 24

5.1 E-com regulation 24

5.1.1 Introduction 24

5.1.2 National discretion and consequences to data retention 24

5.1.3 Electronic communications service 26

5.2 Access to subscriber data 31

5.2.1 Denmark 31

5.2.2 Finland 32

5.2.3 Iceland 32
5.2.4 Norway 32
5.2.5 Sweden 33
5.3 Expedited data preservation and partial disclosure of data 33
5.3.1 Denmark 33
5.3.2 Finland 34
5.3.3 Iceland 35
5.3.4 Norway 35
5.3.5 Sweden 36
5.4 Secret coercive measures interfering with private communication 36
5.4.1 Introduction – the criminality condition 36
5.4.2 Finland 37
5.4.3 Iceland 38
5.4.4 Norway 38
5.4.5 Sweden 38
5.4.6 Denmark 39
Part 2: National Data Retention Rules 42
6. Denmark 43
6.1 Introduction 43
6.2 Targeted data retention orders 43
6.2.1 Introduction – the criminality condition 43
6.2.2 Data retention targeting convicted persons 44
6.2.3 Data retention targeting communication equipment and persons 45
6.2.4 Data retention targeting geographical area 45
6.2.5 Data retention based on a concrete assessment 46
6.3 General, undifferentiated data retention 47
6.3.1 Introduction 47
6.3.2 National security 47
6.3.3 Internet access 48

6.4 The data to be registered 49
6.4.1 Traffic data 49
6.4.2 Internet access data 51
6.5 Provider 52
6.5.1 The definition 52
6.5.2 Internet Access Providers 53
6.6 Access to retained data 54
7. Finland 55
7.1 Introduction 55
7.2 The data to be registered and stored 55
7.3 Storage period 56
7.4 Provider 57
7.5 Access to data 57
8. Iceland 58
9. Norway 59
9.1 Introduction 59
9.2 The data to be registered and stored 60
9.3 Storage period 60
9.4 Provider 61
9.5 Access to data 62
9.5.1 Introduction 62
9.5.2 Purpose, who that may access the data, and personal scope 62
9.5.3 The necessity condition 63
9.5.4 Formal conditions – safeguards 63
9.5.5 Crime prevention 64
10. Sweden 65
10.1 Introduction 65
10.2 The data to be registered and stored 65
10.3 Storage period 67

10.4 The person obliged to register and store data 68
10.5 Access to data 68
10.6 SOU 2023:22: Proposal for a law revision 70
10.6.1 Introduction 70
10.6.2 Proposed amendments to SECA 70
10.6.3 General, undifferentiated data retention to protect national security 71
10.6.4 Targeted data retention to combat serious crime 71
10.6.5 Access to data 72
Part III: Concluding remarks 73
About this publication 75

This publication is also available online in a web-accessible version at:
https://pub.norden.org/temanord2024-532

Summary

This study shows that each Nordic country has its own approach to data retention regulation.

Currently, Norway stands out by limiting data retention rules solely to concern internet access services, regulating both the obligation to retain data and the access procedure in the electronic communications act. In the other end of the scale there is Denmark, where the data retention rules were revised with effect from 30 March 2022. In the Danish view, data retention belongs to the same family of interferences as secret coercive measures targeting private communication, and data preservation. Following the revision, the rules concerning these measures are all regulated in the same chapters in the Procedural Code *(Retsplejeloven)*. Finland, Iceland, and Sweden apply a combined model, laying down data retention rules in the national electronic communications act, while the access procedure is set out in criminal procedural law.

In the report SOU 2023:22 "Data retention and access to electronic information" the Swedish rules are proposed revised along the lines settled for in Denmark. Pursuant to the law in force, Sweden permits use of retained data not only for investigation and prosecution of serious crime, but also to prevent, avert and detect such crime. The other Nordic countries limit data retention to concern investigation and prosecution of crime. The Swedish proposal suggest retained data to be available for intelligence purposes also in the future.

A general feature is that the regulation is quite complicated and sometimes hard to understand. Presumably this is due to the complexity of the field itself, however the legislative adherence to the principle of technology neutrality adds to the problem as it results in a high level of abstraction that makes the law less accessible to users. Finally, it seems doubtful that to integrate rules of data retention as part of the of e-com regulation is the most suitable approach given the discrepancy between the purpose of electronic communication regulation and the mandate of the police, and the widely different terminologies used in the respective fields of the law.

Abbreviations

ECA	Electronic Communications Act. **DECA**: ECA, Denmark. **FECA**: ECA, Finland. **IECA**: ECA, Iceland. **NECA**: ECA, Norway. **SECA**: ECA, Sweden.
IMEI	International Mobile Equipment Identity.
N/A	Not applicable.
NAT	Network Address Translation.
NI-ICS	Number-independent interpersonal communication service.
SIM	Subscriber Identity Module.
VAS	Value Added Service.

Terms

End-user

e-kodex Directive Article 2 no. 14: a user not providing public electronic communications networks or publicly available electronic communications services.

DECA § 2 no. 3: a user of electronic networks or services who on a non-commercial basis makes the electronic network or service available to others.

FECA § 3 no. 10 a: a physical or legal person using or requesting access to telecom services or VAS without providing publicly available electronic communications networks or -services.

IECA

NECA § 1-5 no. 15: any natural or legal person who enters into an agreement about access to an electronic communications network or service for own purpose or for lending to others.

SECA 1:7: a user not providing a publicly available electronic communications network or service.

Electronic communications service

e-kodex Directive Article 2 no. 4: "a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:

A. Internet access service as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
B. Interpersonal communications service; and
C. Services consisting wholly or mainly in the conveyance of signals such as transmission services for the provision of machine-to-machine services and for broadcasting."

DECA § 2 no. 9: Elektronisk kommunikationstjeneste: Tjeneste, der helt eller delvis består i elektronisk overføring af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter, herunder både tovejskommunikation og envejskommunikation.

FECA N/A.

IECA

NECA § 1-5 no. 3: Tjeneste som helt eller i det vesentlige omfatter formidling av signaler i elektronisk kommunikasjonsnett og som normalt ytes mot vederlag

SECA 1:7: en tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som - med undantag för dels tjänster i form av tillhandahållande av innehåll som överförs med hjälp av elektroniska kommunikationsnät och elektroniska kommunikationstjänster, dels tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll är en

1. internetanslutningstjänst enligt artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och slutkundsavgifter för reglerad kommunikation inom EU och om ändring av direktiv 2002/22/EG och förordning (EU) nr 531/2012,
2. interpersonell kommunikationstjänst, eller
3. tjänst som utgörs helt eller huvudsakligen av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin-till-maskin-tjänster eller för rundradio,

IMEI

International Mobile Equipment Identity. A globally unique identification number for mobile electronic communications devices.

Internet access service

Regulation 2015/2120/EU (and e-kodex Article 2 no. 4): a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology or terminal equipment used.

NAT

Network Address Translation. Technology that allows an owner of an IP-address to share it with others at the same time.

NI-ICS

Number-independent interpersonal communication service

e-kodex Article 2 no. 7: an interpersonal communications service which does not connect with publicly assigned numbering resources, namely a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans.

DECA § 2 no. 20: Nummeruafhængig interpersonel kommunikationstjeneste: En tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer, hvem modtageren eller modtagerne skal være. Tjenesten omfatter ikke tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste. Tjenesten etablerer ikke forbindelse til offentligt tildelte nummerressourcer, dvs. et eller flere numre i nationale eller internationale nummerplaner, og muliggør ikke kommunikation med et eller flere numre i nationale eller internationale nummerplaner.

FECA § 3 no. 11 b: En interpersonell kommunikationstjänst som inte använder ett eller flera nummer i nationella eller internationella nummerplaner, (30.12.2020/1207).

IECA

NECA: N/A

SECA 1:7 en interpersonell kommunikationstjänst som varken etablerar en förbindelse till nummer i nationella eller internationella nummerplaner eller möjliggör kommunikation med sådana nummer.

Provider

Provider may be translated to *"udbyder"* and *"tilbyder"*, which are terms used in DECA and NECA. FECA uses both *"teleföretag"* and *"kommunikationsförmedlare,"* while the e-kodex Directive uses *"operator".*

e-kodex Directive: Article 2 no. 29 *"operator"*: an undertaking providing or authorised to provide a public electronic communications network or associated facility.

DECA § 2 no. 1: *"udbyder":* anyone providing products, electronic communications networks or services falling under the scope of [DECA] for a commercial purpose.

FECA § 3 no. 27: *"teleföretag*": anyone providing net services or communications services to a group of users not delimited in advance, i.e., operating a public tele service.

FECA § 3 no. 36: *"kommunikationsförmedlare":* A *teleföretag (§ 3 no. 27),* a *sammanslutningsabonnent* (§ 3 no. 41), or another actor who transmits electronic communication for purposes other than personal.

IECA

NECA § 1-5 no. 16: *"tilbyder":* a natural or legal person making access to electronic networks or services available to others.

SECA: N/A.

Signal data

Data generated by a connection established between a mobile phone and a cell mast when the mobile phone is turned on but not in use by the owner.

SIM

Subscriber Identity Module. A unique number on a SIM-card inserted into a mobile phone. The SIM connects to the telephone number through a Home Location Register. SIM and telephone number relate to one and the same subscription to a mobile phone service. SIM cards may be switched between phones, and many SIM cards may be used on one and the same phone. By combining IMEI and SIM, the provider keeps track of the SIM cards used on a device and the devices that have been used by a SIM. It is thus possible to detect the phones used by a subscriber, and the subscribers who have used a phone.

Subscriber

e-kodex: N/A.

DECA: N/A.

FECA § 3 no. 30: a legal or physical person who for any purpose other than operating a telenet or -services has entered into an agreement with a tele corporation about access to or use of the services.

IECA

NECA: N/A

SECA 1:7: Anyone who has entered into an agreement with a provider of publicly available electronic networks or -services.

User

e-kodex Directive Article 2 no. 13: a natural or legal person using or requesting a publicly available electronic communications service.

DECA: N/A.

FECA § 3 no. 7: a physical person who in the role of subscriber or otherwise, uses teleservices or VAS.

NECA § 1-5 no. 14: any natural or legal person using electronic communications networks or services for own purpose or as a resource in the production of other services.

SECA 1:7: anyone using or requesting a publicly available electronic communications service.

VAS

Value Added Service *(mervärdestjänst)* FECA § 3 no. 10: a service based on the processing of data related to electronic communication for purposes other than transmitting electronic communication.

References

EU legislation

Charter

Charter of Fundamental Rights of The European Union (2012/C 326/02).

Data Retention Directive

Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive (2006/24/EC).

e-kodex Directive

Directive establishing the European Electronic Communications Code (2018/1972/EU).

e-Privacy Directive

Directive on Privacy and Electronic Communications (2002/58/EU).

Regulation 2015/2120/EU

Regulation laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (2015/2120/EU).

Council of Europe

Cybercrime Convention 23 November 2001 (ETS 185) (the Budapest Convention).

Explanatory Report to the Convention on Cybercrime Budapest, 23.11.2001.

National legislation and legal sources

Denmark

BEK no. 380

Bekendtgørelse 2022-03-29 nr. 380 om generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet. In force 30 March 2022.

BEK no. 381

Bekendtgørelse 2022-03-29 nr. 381 om generel og udifferentieret registrering og opbevaring til og med den 29. marst 2023 og opbevaring til og med den 29 marts 2024. In force 30 March 2022 at 12 AM.

Criminal Code

LOV nr. 126 af 1930 *(Straffeloven).*

DECA

LOV nr. 169 af 3. marts 2011 om elektroniske kommunikationsnet og -tjenester *(Teleloven).*

Foreigners Act:

LOV nr. 226 af 1983 *(Utlændingeloven).*

Law revision 2022

LOV nr. 291 af 8 marts 2022 amending the Procedural Code and DECA (Lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester (Revision af reglerne om registrering og opbevaring af oplysninger om teletrafik (logning) m.v.).

LFF-2021

LFF-2021-11-18 no. 93 Forslag til lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester (revision af reglerne om registrering og opbevaring af oplysninger om teletrafik (logning) m.v.).

Procedural Code:

LOV nr. 90 af 11. april 1916 *(Retsplejeloven).*

Finland

Coercive Measures Act

22.7.2011/ 806 *(Tvångsmedelslag).*

FECA

Lag om tjänster inom elektronisk kommunikation, 7.11.2014/917.

Iceland

Code of Criminal Procedure no. 88, 12 June 2008.

IECA

Act no. 77/2022.

Norway

Copyright Act

Lov 15. juni 2018 nr. 40 *(Åndsverkloven).*

Criminal Code

Lov 20. Mai 2005 nr. 28 *(Straffeloven).*

Criminal Procedural Code Lov 22. Mai 1981 nr. 25 *(Straffeprosessloven).*

NECA

Lov om elektronisk kommunikasjon av 4. juli 2003 nr. 83 *(e-komloven).*

Police Act

Lov om politiet av 4. august 1995 nr. 53 *(Politiloven).*

Prop. 167 L (2020-2021)

Amendments to the NECA (storage of IP-addresses etc.) *(Endringer i ekomloven (lagring av IP-addresser mv.).*

Sweden

Electronic Intelligence Act

Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Government Regulation on Electronic Communications

Förordning (2022:511) om elektronisk kommunikation.

Procedural Code

Rättegångsbalk (1942:740).

SECA

Lagen (2022:482) om elektronisk kommunikation.

SOU 2023: 22

Data retention and access to electronic information. *(Datalagring och åtkomst till elektronisk information).*

Part 1: Mandate, EU background and Nordic context

1. Mandate

The Norwegian Ministry of Justice and Public Security has commissioned a comparative study of the legal frameworks of the Nordic countries concerning retention and access to data related to electronic communications for the purpose of preventing, investigating and prosecuting crime. The study shall address:

- The rules for registration and storage of data related to electronic communication,
- public authorities' access to such data when registered and stored by the provider; and
- the applicable legal guarantees and safeguards.

The study shall inform about new regulatory initiatives regarding data retention.

The study shall not perform an assessment of the national rules relative to the fundamental human rights.

The study shall be in English and be finalized by August 2023 (extended to September 2023).[1]

1. In September it was agreed that the report be used in a Nordic workshop concerning data retention regulation hosted by the Norwegian Ministry of Justice and Public Security. The workshop took place 9 November 2023 and resulted only in minor amendments to the report.

2. EU legal background

Use of electronic communication networks and services is protected by fundamental rights, notably the universal rights to privacy (private communication), data protection, and freedom of speech (particularly aspects concerning risk of chilling effect and protection of journalistic sources). To ensure the effectiveness of these rights in the context of electronic communication, the e-Privacy Directive (2002/58/EC) lays down an obligation to ensure that national legislation provides for a duty of confidentiality of e-com providers ("providers") (Article 5), as well as an obligation to delete or anonymize traffic data once the data are "no longer necessary for the purpose of the transmission of a communication" (Article 6(1)). Exception is made for a limited period with respect to data necessary for "subscriber billing" and "interconnection payments" (Article 6(2)).[2] Pursuant to Article 9 "location data other than traffic data" may be processed only when made anonymous.

Pursuant to the Directive Article 15, national law may restrict the scope of these provisions, provided the restriction is,

> a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e., State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph.

Data generated by use of electronic communications services are important to the police in their crime countering operations. In the pre-digital age telecom providers often stored such data and the police could access them under legal powers of seizure or production order. To ensure that traffic and location data would be available to the police also after the e-Privacy Directive, some countries (referring to Article 15), imposed an obligation on providers to retain data related to use of their services. Noticing that differences between national regulations hampered the internal marked, the EU reacted by enacting the Data Retention Directive (2006/24/EC) ("DRD"),[3] which aimed to harmonize data retention rules across the Member States and EEC-countries. DRD acknowledged that such data are important to the prevention, detection, investigation, and prosecution of crime,[4]

2. Data storage could also be permitted by consent from the subscriber. This alternative is of little relevance in the context of crime prevention and investigation, and not considered here.
3. DRD recital 5 and 6.
4. DRD recital 7 to 9.

and compelled Member States to impose a legal obligation on providers to retain metadata for a period of minimum six months and maximum two years. The data was to be made available to the police for the purpose of combating serious crime.

In 2014, in the case *Digital Rights Ireland,*[5] DRD was voided by the European Court of Justice, as incompatible with the fundamental rights to privacy and data protection laid down in the EU Charter of Fundamental Rights (2012/C 326/02) Articles 7 and 8.[6] Since 2014, the Court has further developed its jurisprudence on the matter, indicating that there is some scope for data retention. To analyse this case-law is out of scope of this study.

5. Judgment 8 April 2014; joined cases C-293/12 and C-594/12.
6. The claim that DRD was also incompatible with the right to freedom of speech, was not considered as the Court had concluded already with a violation of privacy and data protection (*ibid.,* para. 70).

3. The complexity

Data governed by data retention rules may be referred to by different terms, e.g., "meta-", "traffic" or "location" data. The term "data related to use of electronic communications services" encompasses all. It should be noticed that content data are out of scope of data retention rules.

Data retention rules concern data generated in the operation of certain services. These services are run by some and used by others. Both the services and the communications equipment involved, may vary. This makes for sorting the data into different categories, for instance according to criteria concerning:

- The services (telephone, internet access, online communication services,[7] networks);
- The person offering the service/processing the data (provider, user, end-user, user-ID);
- The person using the service (subscriber, registered user, user, end-user);
- The communication per se (A-and B number, IP-address, time, duration);
- The identity of the communications equipment used in the communication;
- The geographical area where a specific communications device is or has been used, etc.

The categorization indicates that there is a great variety of data that could be retained, and that different layers in the chain of communications services (several layers of providers and users may be involved in one communication) could be relevant data retention points. The former is a question of the material scope of the rules, the latter of the personal scope of the rules. The technological complexity adds to the intricacies of EU law the legislator is faced with in this field. This could help explain the differences of the data retention rules of the Nordic countries, they seem to vary in every aspect of the categories set out above.

7. "Online communications services" is colloquial for NI-ICS, addressed in Section 5.1.3.4.

4. Data retention as concept

The purpose of data retention is to ensure the availability of data related to use of electronic communications networks and services, when necessary for combating serious crime or protecting national security. The legal framework is composed of two components, one setting out the conditions for registration and storage of data and another regulating access to the data. While "data retention" literally only means the first component, the term is often used to cover both. Retained data are stored with the provider and shall be deleted once the storage period ends. Stored data are not freely available to the police (or other public authorities). The data are protected by the statutory duty of confidentiality of the provider and may be accessed by the police only pursuant to a procedure laid down in law.

Rules of data retention form part of a larger legal framework whereby data related to electronic communication may be made available to the police. The other parts concern expedited data preservation and partial disclosure of traffic data; secret coercive measures targeting data related to electronic communication; production order targeting such data; and access to subscriber data.

Rules of *expedited data preservation and partial disclosure of traffic data* were introduced in criminal procedural law by the Council of Europe Cybercrime Convention (2001) Article 16 and 17.[8] The purpose is to prevent deletion of vulnerable electronic data important to a criminal investigation, before the police have had a chance to collect them. A preservation order may thus be issued already at an early stage, that is, before the investigation has uncovered sufficient information to use coercive measures such as production order, to secure the data. Served with a preservation order the custodian must keep the data intact "for as long as necessary, up to a maximum of ninety days", with a possibility for renewal (Article 16 no. 2). While Article 16 applies generally to natural and legal persons having data in their possession, Article 17 concerns *providers of electronic communications services*. The provision requires traffic data to be preserved "regardless of whether one or more service providers were involved in the transmission of that communication."[9] Concerning communications already transmitted, the provision requires "expedited disclosure" to the competent national authority (e.g., the police) of *traffic data that disclose the source and destination* of the communication. It is pointed out that determining the source or destination of a past communication can assist in the identification of a perpetrator.[10]

8. "Data preservation is for most countries an entirely new legal power or procedure in domestic law", Explanatory Report to the Cybercrime Convention ("ER") para. 155.
9. "Traffic data» is defined in the Convention Article 1(d) as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."
10. ER para. 155.

A preservation order may only concern data generated and stored in the ordinary operation of the electronic communications service, it may not compel the provider to register and store other data.[11] Consequently, if data are deleted forthwith as a matter of routine, there are no data to preserve. From a police perspective, rules of *data retention* improve the situation by laying down an obligation to register and store data *once they are generated* in a provider's system.[12] Thus, they trump providers' routines for data deletion as well as the general obligation to delete data stemming from the e-Privacy Directive. However, as data retention rules specify the data to be registered and stored, they do not always comprise *all kinds* of data generated in the operation of a provider's service. Data not subject to retention might still be collected by the police, pursuant to a production order or an initial preservation order backed by a production order. In Denmark *signal data* is a case in point, i.e., data generated by a connection established between a mobile phone and a cell mast when the mobile phone is turned on but not in use by the owner. Signal data fall outside the scope of the Danish data retention rules yet may be preserved and subsequently accessed by a production order. Alternatively, if stored already, the data may be accessed directly by a production order.[13]

The data retention and data preservation regimes have in common that the procedure for subsequent police access to the data is regulated separately in provisions setting out specific conditions that must be fulfilled. Data retention/ preservation do not provide for real-time access to data.

Secret coercive measures are another means by which the police may collect data related to use of electronic communications services. In this case police access to the data is a function of the legal permission to activate the measure (normally a court decision), entailing immediate access to the data. This applies both to data that are stored, and to data materializing in the future (real-time). Data retention rules differ in the sense that data registered and stored are not – as already noted – automatically made available to the police.

Providers of electronic communications networks and services may register data that identify the subscribers to their services. The data are an important supplement to retained data, providing a possibility to identify the person who used a communications service at a specific point in time. The legal framework for registration of and access to subscriber data thus matters to the police.

Originally, the legislative approach to data retention was to incorporate the first component (registration and storage) into the electronic communications act. The second component (the access procedure) was the set out in rules of criminal procedural law concerning coercive measures. Currently, Norway stands out by fully

11. ER., para. 150.
12. ER., para. 151 explains that "[d]ata retention connotes the accumulation of data in the present and the keeping or possession of it into a future time period. Data retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe."
13. See Section 6.6.

regulating both components in NECA.[14] In the other end of the scale there is Denmark, where the data retention rules were revised with effect from 30 March 2022.[15] In the Danish view, data retention belongs to the same family of interferences as secret coercive measures targeting private communication, and data preservation. Following the revision, the rules concerning these measures are all regulated in the same chapters in the Procedural Code *(Retsplejeloven)*. The legal basis is provided in Chapter 71 "Interferences with private communication, etc.", and the procedure for access (retained or preserved data) in Chapter 74 "Seizure and Production Order *(edition)."* Finland, Iceland, and Sweden apply the original model. However, in the report SOU 2023:22 "Data retention and access to electronic information" the Swedish rules are proposed to be revised along the lines settled for in Denmark.[16]

14. The Norwegian Electronic Communications Act.
15. LOV nr. 291 af 8. marts 2022 amending the Procedural Code and DECA (Lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester (Revision af reglerne om registrering og opbevaring af oplysninger om teletrafik (logning) m.v.).
16. See Section 10.6.

5. Nordic overview

This section provides the national legal context of the data retention rules. It raises some issues related to national e-com legislation and gives an overview of the rules concerning data preservation, secret coercive measures concerning data related to electronic communication, and police access to subscriber data. The aim is to make it easier to understand similarities and discrepancies of the Nordic data retention rules, addressed in detail in Sections 6 to 10.

Unfortunately, the English translation of the Icelandic Electronic Communications Act (Act. No. 70/2022) that entered into force 1 September 2022, is not yet available (September 2023). Lack of access to the legislative text itself has been an impediment, although the Icelandic contact person has been very helpful. The coverage regarding the Icelandic situation is therefore incomplete.

5.1 E-com regulation

5.1.1 Introduction

Each Nordic country has provided for an Electronic Communications Act ("ECA"), herein referred to as DECA, FECA, IECA, NECA, and SECA respectively. The purpose of the ECAs is first and foremost to provide a framework ensuring fair market conditions in the e-com sector, and public access to effective and secure electronic communications services.[17] The ECAs also implement the provisions of the e-Privacy Directive, thus laying down an obligation of confidentiality on providers of electronic communications networks and services.[18] The obligation comprises both the content of the communication and data related to use of the communications service. The ECAs also specify that data shall be deleted once they are no longer necessary for communications purposes or invoicing, or other purposes set out in law (e.g., data retention).[19] In terms of data protection law, the rules reflect principles of purpose specificity, data minimalization (data may be processed only when necessary for a lawful purpose), and storage limitation.

5.1.2 National discretion and consequences to data retention

This report shows that each Nordic country has its own take on data retention regulation.[20] However, at the outset they have in common that the first component (registration and storage) must specify:

17. DECA § 1; FECA § 1; IECA ; NECA § 1-1; SECA 1:1.
18. DECA § 7; FECA § 136 third para., IECA ; NECA § 2-9; SECA 9:31.
19. DECA § 8; FECA § 137 third para.; IECA ; NECA § 2-7 fifth para.; SECA 9:1.
20. See Sections 6 to 10.

a. The type of electronic communications services to be comprised by the rules;
b. The person that shall have a duty to register and store data; and
c. The person whose data that shall be retained (the data subject).

Relevant to litra a is that the EU regulatory restrictions on data retention concern data related to "electronic communications services". The EU definition of "electronic communications services" thus sets the perimeter for national data retention rules (the definition is further addressed in Section 5.1.3). The definition encompasses a range of services both on the sides of telephony and the internet. However, there is no obligation to ensure that data retention rules on national level comprise all these services. It clearly follows from the e-Privacy Directive that the rules may not exceed what is "necessary, appropriate and proportionate" (Article 15, cited in Section 2, i.e., the proportionality condition). Thus, within the perimeter set by the EU definition, a country is free to adopt data retention rules with narrower scope. The Norwegian rules which are limited to comprise *internet access services* only, make for a pertinent example.

The scope of services encompassed by litra a, logically sets the perimeter for the scope of persons mentioned in litra b and c. Taking account of the proportionality condition, it is not a given that national data retention rules encompass everyone eligible within each category, and unsurprisingly, national solutions differ in this respect. For instance, regarding (b) (the providers), Norway has opted for including every internet access provider, large or small. 95 % of the Norwegian market is controlled by 6 large internet access providers, and the remaining 5 % is shared among approximately 300 small providers. No matter the size, each of them must comply with the obligation to retain data.[21] In contrast, Finland has nominated four providers *(lagringsskyldigt företag)*, selected according to criteria concerning aggregate market share and geographical coverage of the services.[22] Finnish regulation makes clear that providers of "small significance" *(ringa betydelse)* may not be subject to an obligation to retain.

Regarding (c) (the data subject), to find out whose data that have to be retained according to national law, has proved itself to be a bit complicated. The problem is caused by the array of terms provided both on EU level and national level. On EU level the definitions laid down in the e-kodex Directive (2018/1972/EU) that replaced the former EC e-com regulation, apply. The Directive is implemented in Denmark, Finland, and Sweden, but not in Norway (as of November 2023) although EEC-relevant.[23] Differences in implementation result in differences between the definitions on national level. It adds to the variety that countries that have implemented the e-kodex Directive, do not always apply all the definitions, or

21. 2018 figures. Prop. L 167 (2020-2021) Ch. 8.1.2 and 8.1.4.
22. E-mail dated 4 August 2023, referring to *teleföretag* as defined in FECA § 3 no. 27.
23. Proposal for a new e-com act was publicly announced 2 July 2021, and deadline for feed-back set to 15 October 2021. Information about the preparatory process may be accessed here: Høring - Forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften - regjeringen.no (visited 15 September 2023).

provide national definitions whose scope may deviate from the Directive. This is the case with respect to the notions "user" and "end-user" that are crucial to data retention rules on the internet side. The fact that they are not quite in alignment with each other across borders, complicates a comparison.

From a police perspective it is important that the obligation to retain, encompasses data that enable the police to identify the person who used an electronic communications service at a specific point in time. Because electronic communications services often are provided in chains running through several service layers, the question arises about how far down the chain the obligation to retain applies. Does it end with data generated by the "user" or go further to include data of the "end-user" as well? To complicate matters, on one level a person may be a "provider" and on another a "user". This could be a matter of perspective. The problem is predominantly related to data retention regarding internet access services. However, having legal certainty about who that is deemed to be a provider, to be distinguished from the person whose data shall be retained, is important. It makes the meaning of notions such as "user" "end-user", "subscriber", "registered user" as well as "provider", crucial.[24] Unfortunately, their meaning is not always easily discerned. As this is a recurring theme the issue will hopefully be clarified over the pages that follow.

The *purpose* of e-com regulation is an aspect related to this problem. The purpose was described in the previous section and showed that assisting the police was not included. It is questionable whether the definitions developed for the purpose of the e-com sector are fully suitable for the needs of the police. National data retention law is free to specify the providers and data subjects in more detail, which could be a way to achieve greater legal certainty and make the rules more easily comprehensible.

5.1.3 Electronic communications service

5.1.3.1 The definition set out in the e-kodex Directive

The e-kodex Directive Article 2 no. 4 sets out the following definition of electronic communications service:

> a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:
>
> a. Internet access service as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
>
> b. Interpersonal communications service; and

24. Central definitions are provided in the Section "Terms", see p. 5-9.

c. Services consisting wholly or mainly in the conveyance of signals such as transmission services for the provision of machine-to-machine services and for broadcasting.

The services mentioned in point c of Article 2 no. 4, do not concern human use of electronic communications services, consequently they are not relevant to data retention rules. This leaves *internet access services* and *interpersonal communications services* as the remit of such rules. For a service to qualify, it must "normally [be] provided for remuneration." The definition does not explicitly require the service to be publicly available.

5.1.3.2 Internet access service

"Internet access service" means:

> a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology or terminal equipment used (cf. e-kodex Directive Article 2 no. 4 point a, referring to Regulation 2015/2120/EU Art. 2 second para., point 2).

This definition requires the service to be "publicly available" and provide "access to the internet." In addition, following from the general part of Article 2 no. 4, it must "normally [be] provided for remuneration."

Access to the internet requires an IP-address. For a person to access the internet, s/he must either dispose an IP-address or make use of an internet connection provided by someone disposing an IP-address. An IP-address is a unique number representing the endpoint of an internet connection. IP-addresses are a limited resource, globally managed by Internet Assigned Numbers Authority ("IANA"). A regionalized system allocates "pools" of IP-addresses to providers, who are then in position to assign IP-addresses to users. The provider may be deemed to be a first level gatekeeper to the internet. A pool of IP-addresses may be split between IP-addresses that are assigned to the same users over time, and IP-addresses assigned to users only when they go online. The latter are withdrawn once users log off. Back in the pool the IP-addresses are available for reassignment to other users. The former are known as "static" IP-addresses, the latter as "dynamic" IP-addresses. There is no qualitative difference between static and dynamic IP-addresses, the classification depends entirely on the provider's decision about how to manage the pool. Usually, large organisations are assigned static IP-addresses, while private users go online based on dynamically assigned IP-addresses.

An IP-address identifies the communications equipment involved in an internet connection. The provider may have data that identify the owner of the communications equipment. This is certainly the case for static IP-addresses, which thus may be regarded as the internet equivalent to telephone numbers. It could

also be the case for dynamic IP-addresses, depending on the set-up. However, as a dynamic IP-address may be reassigned to a new user once freed up from the former, a specific point in time must also be provided (by the police) for the gatekeeper to determine whose communications equipment was in use for the relevant session. Naturally, the possibility to identify the user also requires that the provider keeps a record showing the periods the IP-address was in use and by whom.

A user disposing a static IP-address may share it to enable others to go online. This is something to be seen among users such as universities, private and public corporations and institutions wishing to provide internet to staff and clients. Sharing of an IP-address may be facilitated through a so-called NAT-system (Network Address Translation), which may also be a service of the provider, then known as Carrier-Grade NAT (CGNAT).[25] From the outside, only a single IP-address is observable. The NAT-system however keeps track of internal use of the IP-address, by logging the port number of the computer equipment used to go online by the internal user, and the time it was used. Based on data about time and port number, the computer equipment used in a specific internet session fronted by a static IP-address shared among many users, may thus be identified. In a criminal investigation identification of the communications equipment involved in a specific session, is an important step towards identifying the person who made use of the internet connection at a specific point in time.

Assigning IP-addresses to users is not sufficient per se to fall under the scope of the definition of internet access service. In addition, the definition requires the service to be "publicly available" and "normally provided for remuneration." On national level the condition "normally provided for remuneration" is found variously in the definition of "electronic communications service" and "provider". The condition is included in the definition of "electronic communications service" in NECA § 1-5 no. 3, and SECA 1:7, and in the definition of "provider" in DECA § 2 no. 2 ("for a commercial purpose"). It should also be noticed that the condition "normally provided for remuneration" is not uniformly interpreted in the Nordic countries. For instance, in Denmark, hotels and restaurants may have an obligation to retain, while the opposite is the case in Norway. The legal provisions however do not contain words indicating this difference. That said, a natural or legal person who offers a service that fulfils the conditions as interpreted in national law, is an "internet access provider" within the meaning of that law.

5.1.3.3 Internet access offered by other actors

As noted, a person may go online with an IP-address assigned to a different user, as do for instance children using parents' internet. There are however professional actors who offer their own internet access as a service to others. Such actors may be deemed to be second level gatekeepers to the internet. Some examples illustrate

25. Pursuant to the e-kodex Directive "access to number translation" is an "access service", which then may form part of an internet access service (Article 2 no. 27 read in conjunction with no. 4 point a).

that the motives for offering the service may vary considerably. For instance, the user could be an employer (e.g., a corporation or a public organisation offering internet to the employees), a caretaker (e.g., private or public hospitals, and other public institutions offering internet to patients and clients), a provider of research and education (e.g., universities and schools providing internet to researchers, students and pupils); the internet could be offered for a commercial purpose (e.g., restaurants and hotels offering internet to guests/clients), or, simply to meet general expectations about internet access (e.g., trains or airports offering internet to travellers).

It varies whether such services are subject to national data retention rules. Seemingly, the issue is sometimes framed as a question concerning interpretation of the criteria "publicly available" and "normally provided for remuneration". At the outset, "publicly available" could be interpreted as requiring the group of users not to be delimited in advance, in other words to be available to anyone competent to request the service and agree to the terms. The question is how strictly this should be understood. In the abovementioned examples the service is reserved for employees, guests, or clients. While the number of employees may be fixed and regarded as delimited in advance, the number of guests and clients are in principle open-ended, entailing that a service offered to them could be deemed as publicly available. Danish rules thus encompass internet "hot spots" offered by restaurants and hotels. This is the case despite that restaurants and hotels are not first level gatekeepers to the internet, but *users* of an IP-address assigned to them from such a gatekeeper. It appears that in the Danish view, internet "hot spot" is a "publicly available" service, and the preparatory works explicitly declares that the service also fulfils the condition "to be provided for remuneration." The rationale is that the service makes the hotel/restaurant more attractive in the competition for customers, thus is commercially motivated.[26] The Norwegian position is the opposite, concluding that "hot spot" internet service provided by hotels and restaurants are "private networks" not provided for remuneration.[27]

The crucial question is whether an internet access service provided by a second level gatekeeper is an electronic communications service within the meaning of the Directive. The approach of the Nordic countries to this question seems to vary, perhaps the question has not been raised per se. It also varies whether data retention rules refer to "electronic communications services" or "providers." This matters, because as previously noted a "user" may also be a "provider" of an electronic communications service. "Provider" is not a defined term pursuant to the e-kodex Directive Article 2. "User" however, is a person "*using* … a publicly available electronic communications service" (Article 2 no. 13). "User" shall be distinguished from "end-user", i.e., a person "*not providing* … publicly available electronic communications services" (Article 2 no. 14). An end-user is thus a user, and a user as

26. LFF-2021, Gen. Comm. Ch. 3.1.1.2 p. 12.
27. Prop. 167 L (2020-2021), Ch. 8.1.4.

opposed to an end-user, may provide an electronic communications service, for instance access to the internet. Second level gatekeepers may thus provide an "internet access service" within the meaning of the Directive.

The problem of determining the perimeter of the scope of national data retention rules, is important to the police, as exclusion of users providing internet "hot spots" to large groups of people from the remit of these rules, reduces the possibility to track down perpetrators based on data generated by their access to the internet. The concern also relates to large users/providers providing the service for a *non-commercial* purpose, such as libraries and universities. Just like hotels and restaurants, the number of clients is in principle open-ended, the difference being that the service is a part of the infrastructure necessary for the organisation to fulfil its mandate, as opposed to a commercially motivated add-on service. A commercial motive (if any) is therefore not clearly visible. However, the condition "for remuneration" is not absolute (indicated by "normally"), and this prompts the question whether such users could and should be imposed an obligation to retain data. To address this question is beyond the scope of this study.

To conclude, it is not always clear whether the remit of national data retention rules concerning internet access is determined according to formal considerations grounded in the definitions provided on EU level, or by proportionality considerations stemming from a human rights perspective (cf. the e-Privacy Directive Article 15). The rationale of the rules would be more accessible if the perimeter set by EU e-com regulation was determined first, then supplemented with proportionality considerations that could entail and explain a narrower scope.

5.1.3.4 Interpersonal communications services

"Interpersonal communications service" means:

> a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service (e-kodex Directive Article 2 no. 5)

Interpersonal communications services may be number-based or number-independent. Number-based services connect or enable communication with "publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans" (e-kodex Directive Article 2 no. 6). Fixed and mobile telephone services fall into this category.

As indicated by the term itself, "number-independent interpersonal communications services" ("NI-ICS") are not connected to national or international numbering *plans* (e-kodex Directive Art. 2 no. 7). They are typically internet-based, thus in a certain sense number-*based*, as the IP-packets transmitted over the internet contain source and destination numbers (IP-addresses). NI-ICS and internet access service are different electronic communications services. NI-ICS may provide real-time audio/video communication, chat and other forms of messaging. Services such as Messenger, WhatsApp, Signal, Telegram, Snapchat, FaceTime, Discord, Slack, Viber, Google Messages, Kik Messages, Line and Skype are NI-ICS. Use of NI-ICS is ever more common, privately and professionally, gradually overtaking telephony.

By including NI-ICS, the definition of electronic communications service set out in the Directive, is broader than the definition set out in the e-com regulation it replaced. It varies whether the Nordic data retention rules include data related to use of NI-ICS.

5.2 Access to subscriber data

Telephone numbers and IP-addresses (including port numbers and point in time) identify the communications equipment. From a police perspective it is important also to know the identity of the owner of the communications equipment. Although it might not be the owner who used the equipment at the critical moment, access to the owner opens possibility to ascertain the concrete circumstances in this regard. The questions are, firstly, whether national law requires providers to know the identity of their users, and secondly, whether the police may access the data.

5.2.1 Denmark

With respect to telephony, Danish law provides a system for "targeted person-oriented registration and storage of traffic data" the purpose of which is "to the widest extent possible" perform unambiguous identification of the user/end user of a specific electronic communications device.[28] Numbering data concerning fixed and mobile telephony are stored in a publicly available directory known as the "118 database." An end-user may reserve her data from being retrievable from the 118 database (DECA § 31 fourth para.). The police may still get access to the data, pursuant to DECA § 31 sixth para.

The preparatory works to the law revision in 2022 emphasise the importance of the quality of the 118 database. It is paramount to ensure that persons of interest in the fight against serious crime may be identified based on their telephone numbers/SIM cards, and that every telephone used by such a person may be identified. Conversely, one must avoid that data concern the wrong person.[29]

28. LFF-2021, Spec. Comm. to rpl. 786 h, p. 97.
29. LFF-2021, Spec. Comm. to rpl. 786 h, p. 97.

The Minister of Justice pursuant to negotiations with the Minster of Climate, Energy and Utilities, may lay down rules about registration and verification of "numbering data" *("nummeroplysningsdata"),* cf. the Procedural Code *(Retsplejeloven (rpl.))* § 786 h. This provision is placed in chapter 71 about interference with private communication in criminal investigations. The rules issued by the Minister may exclude the possibility to acquire and use anonymous tele cards.[30] Numbering data are defined in DECA § 31 second para., as

> data about subscriber numbers assigned to end-users, including name, address, job information, subscription number and the category of service for which the subscription number shall be used.

It is proposed to amend § 31 second para., also to include "end-users' unique ID".[31]

The police may also gain access by an order with legal basis in rpl. § 804 b.[32] Thus the police may order a "provider" to disclose data identifying an end-user's "access to electronic communications networks or -services." The measure is available in a criminal investigation concerning an offence subject to public prosecution (*"offentlig påtale").*[33] Based on rpl. § 804 b, the end-user may be identified, and the reverse is possible, namely, to identify the telephone numbers an end-user has connected from his number, as well as the IMEI- and IMSI-number that have been connected to a telephone number.[34] On the internet side the police may gain access to fixed IP-addresses and e-mail addresses. Dynamic IP-addresses and port numbers cannot be accessed with basis in this provision, instead rpl. § 804 *(edition)* apply.[35]

5.2.2 Finland

The police may request subscriber data directly from the provider. This is considered necessary to perform the duties under the Police Act etc.[36]

5.2.3 Iceland

...

5.2.4 Norway

Telephone numbers are stored in a publicly available database, however subscribers may reserve their data from being included. Unlisted numbers and identity data are protected by the duty of confidentiality set out in NECA § 2-9. Still the police and

30. LFF-2021, Gen. Comm. Ch. 3.4.2, p. 34-35.
31. Spec. Comm. p. 106, and 115. It is unclear if the amendment has become effective, it is not shown on elov.dk (15 September 2023).
32. Spec. Comm. To § 804 b, p. 103.
33. In addition, some special other offences are mentioned.
34. P. 103.
35. P. 103. See also this Report Section 6.6.
36. E-mail 11. August 2023.

the prosecuting authority may gain access to unlisted telephone numbers, other subscription information, and electronic communication addresses (including e-mail addresses), cf. § 2-9 third and fourth para. IP-addresses are retained data pursuant to NECA § 2-8 a, and must be accessed pursuant to the procedure set out in § 2-8 b. This procedure however largely corresponds to the one laid down in § 2-9 third and fourth para.

The provider shall comply with the request unless "special circumstances make it undesirable." The circumstances must concern issues internal to the provider (e.g., uncertainty causing risk of confusion with another person). The provider shall not review the necessity of the data to the police. The request may concern any purpose within the mandate of the police/prosecution. It follows that access to the data may be obtained also for tasks other than criminal investigation. Finally, the provision also provides for data to be handed out to "another authority" "pursuant to law". This is provided for with respect to owners of intellectual property rights as per the Copyright Act § 87.[37]

5.2.5 Sweden

Pursuant to SECA 9:24-25 providers of prepaid electronic communications services may not activate the service without first having registered the subscriber's name and address, unique ID and the ID of the agreement related to electronic communications service. Government regulation (2022:51) 9:11 authorises the Postal and Telecom Authority to lay down rules about identity control.

SECA 9:33 first para., no. 2 sets out that "data about a subscription agreement" (as per § 31 first para., no. 1) shall be made available pursuant to requests concerning "criminal activity or suspicion about a crime." The request may be put forward by the Economic Crime Authority *(Ekobrottsmyndigheten)*, the Police *(Polismyndigheten)*, the Police Security Service *(Säkerhetspolisen)*, the Customs Authority *(Tullverket)*, the Prosecuting Authority *(Åklagarmyndigheten)*, or «any other authority tasked with such intervention."

The obligation to disclose data concern providers of "electronic communications networks or -services". NI-ICS are not included.

5.3 Expedited data preservation and partial disclosure of data

5.3.1 Denmark

The police may order "providers" *("udbydere")* to perform expedited preservation of "electronic data" (rpl. § 786 a). An order may be issued if "electronic evidence

37. Act of 15 June 2018 no. 40 *(Åndsverkloven)*.

material *(elektronisk bevismateriale)* may be of importance" *(af betydning)* to the investigation. The investigation must concern an offence that qualify for *teleoplysning*, a coercive measure further explained in Section 5.4.6. By specifically mentioning "providers" the provision seems not to open for use of preservation order against other actors, even if they might be in possession of data important to the investigation. This is different from the rules for instance in Norway and Sweden.

The order must specify the data to be preserved. It may only concern data existing at the time when the order is served and must not exceed the amount of data necessary for the purpose. The preservation period must be as short as possible not exceeding 90 days, with a possibility for renewal.

Preserved "traffic and location data" may be collected by the police under a production order *(edition)* pursuant to rpl. § 804 a. The condition is that the investigation concerns an offence that could give basis for *teleoplysning* (see Section 5.4.6). Rpl. § 804 a is further explained in Section 6.6.

Pursuant to rpl. § 786 a third para., "providers of electronic communication networks or -services" shall upon request, as part of the preservation of data, *without undue delay disclose* source and destination data of a communication. The obligation to preserve and disclose data is criminally sanctioned (rpl. § 786 a fourth para.).

5.3.2 Finland

Preservation order is regulated in the Coercive Measures Act *(Tvångsmeddellagen (tvml.))* 8:24-26.

A preservation order may be issued by a police officer "entitled to perform arrest." The order may be issued "prior to a search of equipment" if there is "reason to believe that data that may be relevant to the investigation get lost or altered." The order may also apply to data "likely to arrive in the device or information system during the month following the order." The possibility to order preservation of *future data* sets the Finnish provisions apart from the data preservation rules of the other Nordic countries, which are limited to concern data existing when the order is served on the provider.

The order may also comprise data related to an electronic message, its source, destination, route and size, and the time and duration of the communications and similar data (traffic data). If the transmission of a message involves several providers, the pre-trial authority is entitled to get sufficient data to identify them. A preservation order may be issued for 3 months at a time (§ 25). It may be renewed if necessary for the investigation. It shall be terminated once preservation of the data is no longer necessary. The provider or possessor of the data shall keep the preservation order confidential (§ 26).

Access to preserved data follows the procedure applicable to *teleövervakning,* tvml. Ch. 10.[38]

5.3.3 Iceland[39]

The Code of Criminal Procedure Article 92, paragraph 3, states that the police can demand expedited data preservation.

For the purpose of the investigation of the case, the police are authorised to instruct an electronic communications undertaking (i.e., an e-com provider) to immediately save digital data, including traffic data related to electronic communications. Police instructions may only apply to data that already exists. The instructions shall state which data shall be saved and the duration for which it should be preserved, which may, however, not be longer than 90 days.

5.3.4 Norway

In the investigation of a crime, the public prosecutor may order the possessor to perform expedited preservation of electronic data *(sikringspålegg)*, and partial disclosure of traffic data (strpl. § 215 a). Concerning an order served on a provider of an electronic communications network or -service, it is also required that there is "reason to believe that a crime has been committed." The preservation period must "not be longer than necessary" and not exceed 90 days. If the order is issued upon the request of another state the period shall be at least 60 days.

Upon request the provider shall disclose "the traffic data necessary to trace the source of the data comprised by the order, and in case they have been sent, their destination."

A suspect shall be notified once the data are preserved, and procedural status as criminally charged is achieved. In practice this may entail that notification is given first when use of secret coercive measures is terminated.

Access to preserved data related to electronic communications may be obtained in secret pursuant to strpl. § 216 b (see Section 5.4.4), alternatively with notification to the person whose data are targeted pursuant to strpl. § 210 (production order/ *utleveringspålegg).* In the latter case it suffices that the data are assumed to be relevant as evidence. Notification may be postponed for 8 weeks with possibility for extension, cf., strpl. § 210 a, provided the investigation concerns an offence with a prescribed maximum penalty of imprisonment for at least 6 months, and notification is assumed to be seriously detrimental to the investigation.

38. E-mail 4 August 2023. Se furthermore Section 5.4.2 about *teleövervakning.*
39. E-mail 28 August 2023.

5.3.5 Sweden

Pursuant to the Procedural Code *(Rättegångsbalken ("RB"))* 27:16 – 16 a, the leader of the criminal investigation or the public prosecutor may order "a person in possession of specific electronic data" to preserve the data *(bevarandeföreläggande)*. The phrase "a person in possession…" shows that the measure is not limited solely to concern *providers* of electronic communications services.

The order must specify the preservation period which must "not be longer than necessary" and not exceed 90 days. Provided there are "special reasons" the preservation period may be renewed with another 90 days as a maximum. The possessor may be instructed to keep the preservation of data confidential. Access may be obtained pursuant to the provisions about seizure (RB 27:1 ff.).

An obligation to disclose traffic data showing the providers involved in the transmission of a preserved electronic message, is laid down in SECA 9:33 fifth paragraph. Naturally, the obligation is limited to concern providers of electronic communications services.

5.4 Secret coercive measures interfering with private communication

5.4.1 Introduction – the criminality condition

It follows from the very purpose of data retention rules that they are closely related to secret coercive measures targeting use of electronic communications services. Such measures may be applied in the investigation of serious crime, as well as (depending on national law), intelligence activities conducted outside the scope of a criminal investigation, and police interventions to protect national security. Legal basis for police use of such measures is provided in the national (Criminal) Procedural Codes and related acts, including e.g., the Finnish Coercive Measures Act *(Tvångsmedellågen "tvml.")*, the Swedish Electronic Intelligence Act *("EIA")*, and the Norwegian Police Act. All Nordic countries apply a criminality condition of "serious crime" as legal threshold for the application of secret coercive measures targeting electronic communication, and for granting access to retained data. This section provides an overview of *the criminality condition* applicable to the secret collection of data *related* to electronic communications, as context for the description of the national data retention rules set out in Sections 6 to 10.

The ordinary structure of this report is to follow alphabetical order, placing Denmark first and Sweden last. In this section however, Denmark comes last so to be placed in close proximity to Section 6, where the Danish data retention rules are presented first. The Danish approach to data retention rules stands out from the others, by fully integrating them into the comprehensive set of procedural rules

whereby the police may interfere with private communication for the purpose of investigating crime or protecting national security. Because of this integration, the Danish criminal procedural rules in explained in more detail than the others.

5.4.2 Finland

Secret coercive surveillance *(teleövervakning)* is regulated in the Coercive Measures Act *(Tvångsmeddellagen (tvml.))* 10:6 ff. The measure concerns data related to electronic communication *(förmedlingsuppgifter)*, processed by a "communication mediator" *(kommunikationsförmedlare),* i.e., a tele corporation transmitting electronic communications for purposes that are not personal.[40] "Tele corporation" *(teleföretag)* means "anyone providing net services or communications services to a group of users not delimited in advance, i.e., operating a public tele service."[41]

Put differently, the relevant subject is a commercial provider of a publicly available electronic communications services.

The data must relate to a "user", i.e. "a *physical* person who, in the role as subscriber or otherwise, uses electronic communications services or VAS"[42] or a "subscriber", i.e., a legal or physical person [...] who has entered into an agreement with a tele corporation about use of the services.[43]

The criminality condition:

Teleövervakning may be applied in the investigation of the following offences (10:6 second para.):

1. An offence for which the prescribed maximum penalty is imprisonment for at least 4 years;
2. an offence committed using a telecommunications address or telecommunications terminal equipment for which the prescribed maximum penalty is imprisonment for at least 2 years;
3. unlawful use of a computer system committed using a telecommunications address or telecommunications terminal equipment;
4. exploitation of a person who is the subject of sex trafficking, luring of children for sexual purposes or pandering;
5. drug offences;
6. preparation for an offence committed for terrorist purposes, participation in training for a terrorist offence, travelling for the purpose of committing a terrorist offence, promoting travel for the purpose of committing a terrorist offence or public provocation related to terrorist offences;

40. Defined in FECA § 3 no. 36.
41. FECA § 3 no. 27.
42. FECA § 3 no. 7. "VAS" means Value Added Service (see FECA § 3 no. 10).
43. FECA § 3 no. 30.

7. aggravated customs accounting offence;
8. gross concealment of illegal proceeds *(olagligt byte)*;
9. preparation for hostage-taking; or
10. preparation for aggravatedrobbery.

5.4.3 Iceland

...

5.4.4 Norway

Use of coercive measures is regulated in Part Four of the Criminal Procedural Code *(Straffeprosessloven ("strpl.))*, where rules concerning secret collection of data related to use of electronic communication services are laid down in Chapter 16 a.

Pursuant to strpl. § 216 b second para., point d, a provider of an electronic communications network or -service may be compelled to provide data to the police that

> disclose the communication equipment that within a specific period will be or has been in connection with communications equipment possessed by the suspect or the suspect is assumed to be using, and other data related to communication, and the geographical position of such communications equipment.

The criminality condition:

The investigation must concern an offence with a prescribed maximum penalty of imprisonment for at least 5 years (strpl. § 216 b first para., point a) or an offence mentioned in point b of the said provision (offences with lower level of punishment).

Such data may also be provided to the Police Security Service for preventative purposes when there is "reason to investigate whether anyone is preparing" a crime against national security, a terrorist act or the like, cf. the Police Act § 17 d.

5.4.5 Sweden

Use of coercive measures is regulated in the Procedural Code *(Rättegångdsbalk (RB))* Chapter 27. The provision RB 27:19 (in force from 1 October 2023) provides legal basis for "secret surveillance", i.e., secret collection of

1. data related to electronic messages[44] under transmission or that have been transmitted to or from a telephone number or other address,
2. data disclosing the electronic communications equipment that have been present in a specific geographic area, or
3. data disclosing in which geographic area a specific electronic communications equipment is or has been located.

Pursuant to RB 27:19 a (in force 1 October 2023) the data may be secretly collected by the police in *the investigation of an offence* (including attempt and preparatory acts),

- punishable with imprisonment for a minimum period of 6 months or more,[45]
- other offences as specified (hacking, child sexual abuse material, drugs), and
- offences that may incur secret interception of electronic communication pursuant to RB 27:18 a second para. (offences with lower level of punishment).

Secret surveillance may be applied also for *intelligence purposes* of the Police Authority, the Police Security Service, and the Customs Authority, pursuant to the Electronic Intelligence Act (2012:278) ("EIA"). The purpose must be to prevent, avert or detect an offence with a maximum prescribed penalty of imprisonment for at least 2 years (and some other offences as specified in EIA § 2).

5.4.6 Denmark

Provisions of secret collection of data related to electronic communication are set out in the Procedural Code (*Retsplejeloven* ("rpl.")) Chapter 71 "Interferences with private communication" § 780 first para., no. 3 (collection of data related to electronic communication *(teleoplysning))* and no. 4 (extended collection of traffic data, i.e., traffic data from cell masts in a geographical area *(udvidet teleoplysning))*. Conditions, procedure, and safeguards are set out in rpl. §§ 782 to 786.

Re: Conditions (rpl. § 781 first para. no. 1 to 3):

No. 1: There must be "specific reasons" *("bestemte grunde")* to assume that messages are submitted to or from the suspect by use of the electronic communications service identified by the police.

No. 2: The measure must be deemed to be "of crucial importance" *("af afgørende betydning")* to the investigation.

44. If "messages" *(meddelanden)* shall be interpreted to have the meaning used in SECA, the meaning is "electronic communication", see the comment made in this regard in Section 10.2.
45. Swedish criminal law sets out minimum penalties in the criminal provisions. This differs from the other Nordic countries which specify the maximum penalty that might be incurred.

No. 3: The criminality condition:

The criminality condition for *teleoplysning* and *udvidet teleoplysning* is set out in rpl. § 781 a in conjunction with rpl. § 781 first para., no. 3. Access to "traffic and location data" (rpl. § 781 a) may thus be obtained provided the investigation concerns an offence with a prescribed maximum penalty of imprisonment for at least 3 years. The general criminality condition of 3 years is supplemented with a list of offences with a lower level of punishment (rpl. § 781 first para., no. 3) and offences comprised by § 81 a of the Criminal Code (rpl. § 781 a).

- Rpl. § 781 first para., no. 3 mentions the following offences of the Criminal Code:[46]
    - Chapter 12 or 13 (offences against the Constitution and higher central state authorities, terrorism etc.),
    - § 124 second para., (assisting the escape of a detained person),
    - § 125 (assisting a criminal to evade prosecution / obstruction of justice),
    - § 127 first para., (evasion of military service),
    - § 235 (distribution, possession, and acquisition of child sexual abuse material),
    - § 266 (threats suitable to provoke serious fear of one's life, health etc.),
    - § 281 (extortion),
    - offences set out in the Foreigners Act § 59, eight para., no. 1 to 5 (assistance to unlawful immigration and residence, Denmark as destination or point of transit to a third country).
- In addition, there are the offences included in the list set out in § 81 a of the Criminal Code (rpl. § 781 a). Concerning the offences on that list, § 81 a determines that the level of punishment may be increased up to a maximum of twice the level set out in the criminal provision, provided the crime originates from or is suitable to spark a conflict between groups, who as measures in the conflict, avail themselves of weapons, explosives etc., which due to their particularly dangerous features are suitable to cause substantial harm, or arson is committed.

Finally, pursuant to rpl. § 781 second and third para., *teleoplysning* may also be performed in the investigation of hacking, stalking and breach of a contact restraint order, computer fraud, and unlawful use of a computer system performed by use of an electronic communications service, and offences related to certain EU regulations.

46. The list in rpl. § 781 first para., no. 3, includes § 233 first para. *(rufferi)*. This offence is excluded from the list set out here, as its prescribed maximum level of punishment is imprisonment for at least 4 years, thus exceeding the general condition applicable to *udvided / teleoplysing*.

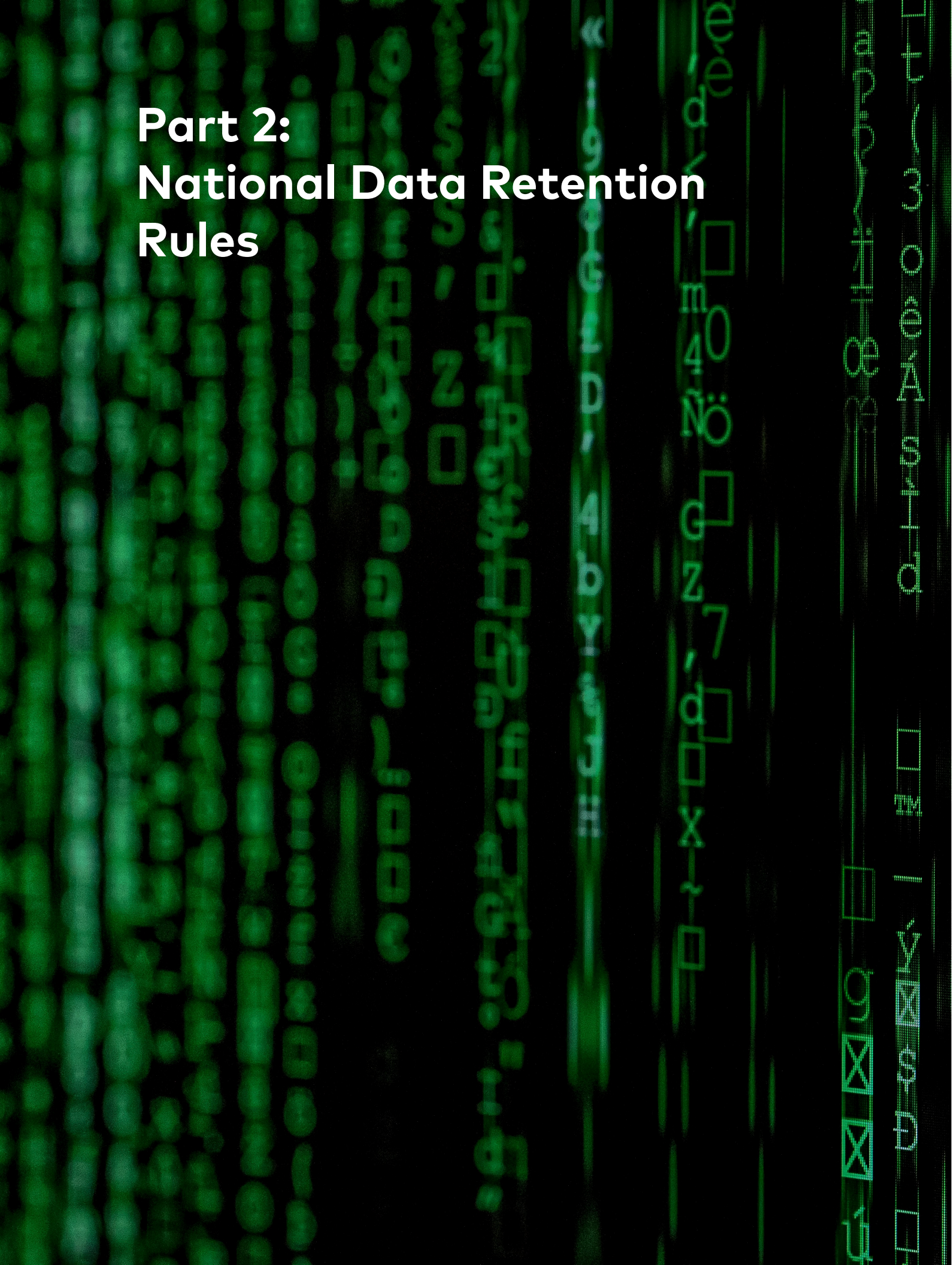
A general *proportionality* condition is set out in rpl. § 782.

Re: Procedure and safeguards:

Decision of *teleoplysning and udvidet teleoplysning* shall be made by the court (a decision supported by reasons *(kendelse))* (rpl. § 783). The decision shall specify the communication number, location etc., and must determine the period for which the interference may be applied. The period must be "as short as possible, not exceeding 4 weeks", though with a possibility for renewal, which also must be decided by the court (rpl. § 783 third para.). The police may make the decision should the purpose otherwise be compromised. A court review must be obtained within 24 hours (rpl. § 783 fifth para.).

A secret defence lawyer shall be appointed (rpl. § 784). The lawyer has a right to be present at court meetings regarding the case and have access to the case documents (rpl. § 785).

E-com providers have an obligation to assist the police in carrying out the coercive measure (rpl. § 786).



Part 2: National Data Retention Rules

6. Denmark

6.1 Introduction

Prior to the revision in 2022, Danish law on data retention imposed a general statutory obligation on providers to indiscriminately register and store data for a period of 1 year. The revision brought about a significant change.

Current law sets out data retention provisions in rpl. Chapter 71 "Interferences with private communication, etc.", § 786 b to § 786 j, and provisions of access in Chapter 74 "Seizure and Production Order". The law provides for *targeted* data retention (rpl. §§ 786 b to 786 d), and *general, undifferentiated* data retention (rpl. § 786 e and 786 f). There is but one instance of a *statutory* obligation to retain data on a general, undifferentiated basis, i.e., rpl. § 786 f relating to internet access. Data retention in other instances may be *ordered* for limited periods of time provided specific conditions are fulfilled. The competence to order data retention is held by the National Police Authority *(Rigspolitiet)*, the District Court or the Minister of Justice as further specified in the provisions.

The revised rules aim to ensure that retained data are available to the police "to the widest extent possible" within the framework of EU law.[47] The law provides procedural safeguards guaranteeing persons whose data are retained a level of legal protection corresponding to the protection applicable to other interferences with private communication, described in Section 5.3.1 (data preservation) and 5.4.6 *(teleoplysning)*.[48] Legal safeguards are afforded both at the stage of data registration and storage, and at the later stage when the data are accessed.

The following sections address the conditions for targeted data retention (6.2), and general, undifferentiated data retention (6.3). Then follows a description of the data to be registered and stored (6.4), and of whom that may be subject to an obligation to retain data (6.5). Finally, the procedure for accessing the data is described (6.6).

6.2 Targeted data retention orders

6.2.1 Introduction – the criminality condition

Targeted data retention of "traffic data" may be ordered for persons, communication equipment, and specific geographical areas pursuant to rpl.

47. LFF-2021 Gen. Comm. Ch. 2, p. 9 ff., and e.g., Ch. 3.7.3.1, p. 53.
48. LFF-2021 Gen. Comm. Ch. 2, p. 9 ff., and e.g., Ch. 3.7.3.1, p. 59.

§§ 786 b to 786 d (each provision making it explicit that the measure is targeted *("målrettet")).* The purpose is to combat serious crime. The provisions apply a criminality condition closely linked to the one applicable to *teleoplysning*. Consequently, aside from generally requiring an offence of a certain seriousness as determined by the statutory level of punishment, they include the offences already described in Section 5.4.6.

6.2.2 Data retention targeting convicted persons

Retention of "traffic data" may be ordered for persons *convicted* of serious crime (§ 786 b first para.). The rationale is that once discharged from prison such persons may be at risk of resuming criminal activity, besides that they might have a criminal social network. It is assumed that registration and storage of traffic data related to such persons "on occasion" might afford the police a possibility to use the data when investigating into "possible criminal connections" *("eventuelle kriminelle forbindelser")* that these persons might have. This could be helpful in the investigation and prosecution of serious crime.[49]

The length of the registration period is related to the seriousness of the crime for which the person is convicted. Rpl. § 786 b first para. no. 1 to 3, differentiate between offences with a prescribed maximum penalty of imprisonment for at least 3, 6 or 8 years, respectively (and, in addition, less serious offences as specified in Section 5.4.6). Thus, the registration periods are,

- 3 years for a person convicted of an offence with a prescribed maximum penalty of imprisonment for at least 3 years ("a 3 year offence") (no. 1),
- 5 years for a 6 year offence (no. 2), and
- 10 years for an 8 year offence (no. 3).

The registration period commences when the person is discharged from prison, or in the case of a conditional sentence, from the time when the verdict became final (rpl. § 786 b second para.).[50]

The storage period is 1 year (rpl. § 786 b fifth para.). It follows that the provider must delete data on a running basis one year from the date when the data were registered.

Order of data retention related to convicted persons is issued by the National Police Authority *("Rigspolitiet")* (rpl. § 786 b first para.). The person whose data are registered shall not be notified (rpl. § 786 b seventh para.).

49. LFF-2021 Gen. Comm. Ch. 2, p. 9 ff., and e.g., Ch. 3.7.3.1, p. 15.
50. The provision adds some details for special instances.

6.2.3 Data retention targeting communication equipment and persons

Rpl. § 786 b third para., no. 1 to 4, provide for retention of "traffic data" with respect to communication equipment and persons that *have been subject to* interception or *teleoplysning* as mentioned in rpl. §§ 780 first para., no. 1 or 3. Furthermore, data may be retained regarding persons who are or have been *in possession* of such communication equipment. Data may also be retained regarding communication equipment that was *contacted* by communication equipment subject to interception or *teleoplysning*.

It is not required that the persons whose data may be retained were prosecuted or convicted.

The registration period is 1 year. The period commences from the date when the interception or *teleoplysning* terminated, and the date at the end of that year is a *fixed* date. Thus, registration may follow immediately upon the termination of the coercive measure, and last for a year. Should the registration start later, it may not continue for a full year, only for the remaining part of it (rpl. § 786 b fourth para).

The storage period is 1 year after registration (rpl. § 786 b fifth para.).

Order of data retention related to communication equipment and persons is issued by the National Police Authority *("Rigspolitiet")* (rpl. § 786 b third para.) The person whose data are registered shall not be notified (rpl. § 786 b seventh para.).

6.2.4 Data retention targeting geographical area

Pursuant to rpl. § 786 c, retention of "traffic data" may be ordered for geographical areas, however, in this case with the limitation that "traffic data related to fixed telephony including the providers' own internet phone service" shall not be retained.

First paragraph states that data retention may be ordered for the parts of providers' networks necessary to cover geographical areas measuring 3 kilometres x 3 kilometres. For the area in question, it must be demonstrated that the number of serious crimes *reported* to the police, or the number of inhabitants *convicted* for serious crime, amount to at least 1,5 times the average national rate calculated as the average over the last three years. The offences in question must have a prescribed maximum penalty of imprisonment for at least 3 years or, be one of those mentioned in Section 5.4.6.[51]

Second paragraph states that data retention may be ordered with respect to "special security critical areas" *("særlig sikringskritiske områder")*. The provision sets out a list exemplifying such areas, e.g., the residences of the royalty and the prime minister, embassies, police premises, prisons, bridge-, tunnel- and ferryway connections, large traffic intersections, border gateways, bus terminals, train and

51. § 81 a of the Criminal Code is left out as irrelevant in respect of reported crime, see rpl. § 786 c first para., no. 1.

metro stations, military areas, high-risk enterprises involving storage of substances causing risk of fire or explosion, poisonous substances or substances causing environmental risk *("kolonne 3 virksomheder")*, and public airports.

The provision does not fix a maximum period for the registration of data.

The storage period is limited to 1 year (third para.).

Order of data retention related to geographical areas is issued by the National Police Authority *("Rigspolitiet")* (rpl. § 786 c first and second para.). Persons whose data are retained shall not be notified (fifth para.).

6.2.5 Data retention based on a concrete assessment

Rpl. § 786 d provides legal basis for retaining "traffic data related to communications equipment, persons or specific areas" pursuant to a concrete assessment *(konkret begrundede pålæg)*. Like rpl. § 786 c, the provision excludes "traffic data related to fixed telephony including the providers' own internet phone service" (rpl. § 786 d first para., last sentence).

Data may thus be retained if there is "reason to assume" *("grund til at antage")* that the object (i.e., the communications equipment, the person or the geographical area in question) "has connection with" *("har forbindelse til")* serious crime, i.e., offences with a prescribed maximum penalty of imprisonment for at least 3 years, or offences as mentioned in Section 5.4.6. The area does not have to be the same or be related to the geographical areas targeted with basis in rpl. § 786 c.[52]

The provision extends the possibility of the police to gain access to traffic data at an early stage of an investigation, beyond what is provided for in § 780 first para. (3) and (4), § 781 and § 781 a, as these provisions require "specific reasons" *("bestemte grunde")* to assume that messages to and from the suspect are transmitted by use of the targeted communication equipment, and that the measure is "crucial" *("af afgørende betydning")* to the investigation. In contrast, pursuant to § 786 d, it is sufficient that there is "reason to assume" that the object "has connection with" serious crime. However, in contrast to decisions about *extended/teleoplysning* the police do not get immediate access to the data, as access requires an additional procedure, see Section 6.6.

The rationale for rpl. § 786 d is that at the time when the measure is needed "there will not necessarily exist a concrete suspicion that a person has committed or will commit a crime, nor that a crime was or will be committed in a specific geographical area."[53] This is further supplemented with the observation that "a retention order may therefore also be issued in respect of specific areas when the police has reason to believe that it has a connection to the planning of serious crime."[54]

52. LFF-2021 Gen. Comm Ch. 3.1.3.3 p. 18, Spec. Comm. to rpl. § 786 d, p. 87.
53. LFF-2021 Gen. Comm Ch. 3.1.3.3 p. 18, Spec. Comm. to rpl. § 786 d, p. 87.
54. LFF-2021 Gen. Comm Ch. 3.1.3.3 p. 18, Spec. Comm. to rpl. § 786 d, p. 87.

A data retention order with basis in rpl. § 786 d must be issued by the court, as the conditions necessitate broad assessments. Such wide scope for discretion should be exerted by an independent judge. This sets the provision apart from the provisions dealt with in the preceding sections, where data retention is ordered by the National Police Authority, the reason being that the provisions apply objective conditions that make the law more foreseeable to the citizens.[55]

The court order must specify the registration period which must be "as short as possible, not exceeding 6 months". The period may be renewed (by court order) for a maximum of 6 months each time. The order shall specify the targeted person, communication equipment or geographical area (rpl. § 786 d second para).

The storage period is 1 year (third para).

Persons whose data are retained are entitled to the same procedural safeguards as applicable to *extended / teleoplysning,* described in Section 5.4.6 (rpl. § 786 d, fourth para.).

6.3 General, undifferentiated data retention

6.3.1 Introduction

The law provides for general undifferentiated data retention in two instances as per rpl. §§ 786 e and 786 f. The first instance necessitates the execution of an order, whereas the other concerns an obligation that follows directly from the legal provision itself.

6.3.2 National security

To protect national security the Minister of Justice may order providers to perform general, undifferentiated data retention (rpl. § 786 e). The obligation is comprehensive (no exception for data related to fixed telephony or the provider's own internet phone service).

The material condition is that there are "concrete circumstances sufficient to cause an assumption that Denmark is faced with a serious threat against national security that must be deemed as real and present or foreseeable" *("tilstrækkelig konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig.")*

The assessment shall be performed at regular intervals to ensure that both national and international circumstances are taken into consideration.[56] Moreover it shall be based on several elements, such as

55. Ch. 3.6.3, p. 41.
56. LFF 2021 Gen. Comm. Ch. 3.2.3.1, p. 28-29.

- analysis of criminal cases, pending and concluded, concerning offences laid down in Chapter 12 and 13 in the Criminal Code (offences against national security, the constitution and higher central institutions, and terrorism);
- unclassified analyses by the Intelligence Service of the Police *(PET)*, the Military Intelligence Service, and the Cybersecurity Centre; and
- the annual Assessment of the Terrorist Threat against Denmark by the Centre of Terrorism Analysis *("Vurderingen af Terrortruslen mot Danmark» (VTD))*.[57]

The registration period is 1 year as a maximum (rpl. § 786 e second para). The preparatory works emphasize that the period must in any case not be longer than "strictly necessary."[58]

The data shall be stored for 1 year (rpl. 786 e third para).

Prior to the order, the Minister of Justice shall have negotiated with the Minister of Commerce (rpl. § 786 e first para.).

Rpl. § 786 e was activated already at the date when the revised law entered into force (30 March 2022), by decision of the Minister of Justice after negotiation with the Minister of Commerce (BEK no. 381). The retention period was set to 1 year commencing 30 March 2022 ending 29 March 2023. The data shall be stored until 29 March 2024. Attached to the decision is an assessment that includes information as listed in the preparatory works, see above. The assessment was thus made publicly available.

6.3.3 Internet access

Providers have a general, undifferentiated obligation to register data related to "end-users'" access to internet (rpl. § 786 f). The data shall be stored for 1 year.

Data about internet access are deemed to be "of crucial importance" *("helt afgørende")* to the investigation of a broad range of crime, in particular crime committed "in the digital domain", notably child sexual abuse, distribution of illicit images, as well as hacking cases which have been on the rise recent years. Generally, circumstances indicate that the police have a need to - unambiguously and efficiently - be able to determine the identity of an end-user's identity on basis of data about internet access.[59]

In contrast to the other provisions, rpl. § 786 e does not require the crime to be serious.[60] The reason is that the data to be retained do not expose the person's private life as such, as they do not concern the servers accessed in the internet session, or third parties the person has communicated with. The data only identify

57. LFF 2021 Gen. Comm. Ch. 3.2.3.1, p. 28-29.
58. LFF 2021 Gen. Comm. Ch. 3.2.3.1, p. 29.
59. P. 31.
60. P. 32.

the person who used an internet connection at a certain point in time (see also Section 6.4.2). The interference is thus deemed to be rather small. The data however may be vital to the investigation of all types of crime.[61]

Further rules about retention of internet access data are set out in BEK no. 380. The regulation specifies the providers comprised by the regulation (Chapter 1 "Scope" §§ 1-3), the data to be registered and by whom (Chapter 2 §§ 4-7) and finally states that a contravention of the regulation is a criminal offence punishable with a fine, and that criminal liability may be incurred also by corporations (§ 8).

6.4 The data to be registered

6.4.1 Traffic data

The data to be registered and stored by the providers are referred to as "traffic data" (rpl. §§ 786 b to 786 e) and "data about an end-user's access to internet" (rpl. § 786 f). "Traffic data" are further specified in a regulation containing thirteen categories of data, set out with legal basis in rpl. § 786 fourth para. The data categories are reiterated in the preparatory works (see below).[62] The categories encompass more data than often regarded as traffic data, such as A- and B number, time, and duration of a communication. It also includes *location data* related to mobile telephony (point 6), as well as name and address of subscribers and registered users (points 8 and 12), the latter often known as *subscriber data*.

The list set out in the regulation is exhaustive. Data not on the list are not "traffic data" and may not be comprised by a retention order even if they are generated in the provider's service, for instance for network error detection. An example is signal data, i.e., data documenting a connection between a mobile phone and a cell mast when the mobile phone is turned on but not in use by the owner.[63] Such data may still be subject to a preservation order.

"Traffic data":

Data related to fixed and mobile telephone networks, as well as to communication by SMS, EMS and MMS:[64]

1. Source number (A-number), and name and address of the subscriber or registered user,
2. Receiving number (B-number), and name and address of the subscriber or registered user,
3. Change of receiving number (C-number), and name and address of the subscriber or registered user,

61. *"...med henblik på bekæmpelse af al kriminalitet..."* (p. 32). Still, to access the data, the investigation must concern an offence subject to public prosecution *(offentlig påtale),* see Section 6.6.
62. LFF-2021 Gen. Comm. p. 19 - 20.
63. LFF-2021 Gen. Comm. p. 20.
64. Short Messaging Service / Enhanced Messaging Service / Multimedia Messaging Service.

4. Receipt of received messages,
5. The identity of the devices used in the communication (e.g., IMSI- or IMEI-numbers),
6. The cell or those cells a mobile phone is connected to at the beginning and end of a communication, as well as precise data about the associated cell masts' geographical or physical location at the time of the communication, [65] and
7. The time when the communication begins and ends.

Data related to the providers' own e-mail services:

8. Sender's e-mail address, and
9. Recipient's e-mail address.

Data related to the provider's own internet-based phone services (IP-telephony):

10. The allocated user identity ("User-ID"),
11. The User-ID and phone number allocated to communications performed in a public electronic communication network,
12. Name and address of the subscriber or registered user, to whom an IP-address, a user identity or a phone number was allocated at the time of the communication, and
13. The time when the communication begun and ended.

The data listed in points 10 to 13 concern the provider's own internet-based phone service (IP-telephony). Such service is possibly an NI-ICS. This entails that the Danish data retention rules encompass NI-ICS in so far as the service is made available by a provider under Danish jurisdiction.

Although not explicitly stated in the legal provisions, the providers' obligation to retain data only concerns data "that are generated or processed in [their] network." [66] If data specified on the list are not generated in the provider's network, for technical or other reasons, they fall outside the scope of the obligation. The provider is not obliged still to generate and store them.

The obligation may be limited also by the scope of the legal provisions. This is the case for rpl. § 786 c (geographical areas) and 786 d (order based on a concrete assessment), both explicitly excluding traffic data about fixed telephony and providers' own internet phone services from the obligation (cf. first paragraph of both provisions).

65. Other geo-location data may be secured by preservation order and accessed by a production order. LFF-2021 Gen. Comm. p. 20.
66. Other geo-location data may be secured by preservation order and accessed by a production order. LFF-2021 Gen. Comm. p. 21.

6.4.2 Internet access data

BEK no. 380 § 4 specifies internet access data as "data that are generated or processed in providers' network"[67] concerning:

1. The User-ID allocated to the end-user by the provider. The User-ID may be a customer number, subscriber number[68] or similar data that identify the end-user vis a vis the internet access provider,
2. The User-ID and telephone number allocated to communications in a public electronic network. «User-ID» means identifying data allocated by the provider to the end-user when the end-user accesses the internet, including IP-address, source port number and other identifying data,
3. Name and address of the subscriber or registered user regarding whom an IP-address, a User-ID or a telephone number was allocated at the time when the internet was accessed.
4. The points in time when the internet was accessed, and the access was terminated.

As noted in Section 6.3.3, the purpose of retaining data about internet access pursuant to rpl. § 786 f, is to ensure availability of data that may identify the person who used an internet connection at a certain point in time. These data are referred to in rpl. § 786 f as "data about an *end-user's* access to internet" (italics added). "End-user" *(slutbruger)* is defined in DECA § 2, no. 3 as

> a user of electronic communications networks or -services, *who on a non-commercial basis makes the said networks or services available to others* (italics added).

This could be organisations such as universities and public libraries and hospitals that offer internet access to their students, clients, patients. However, clearly the provision also aims for the possibility to identify individuals using their private internet connection, without making it available to others. In such case they are possibly to be regarded as "users", which is not a defined term in DECA § 2 (the preparatory works comment that "user" and "end-user" shall be regarded as synonyms).[69] Pursuant to the definitions set out in the e-kodex Directive Article 2 points 13 and 14 there is a difference though: "user" meaning a person "*using* … a publicly available electronic communications service", and "end-user" meaning a person "*not providing* … publicly available electronic communications services."[70] The Danish notions seems to be somewhat at odds with the e-kodex definitions.

67. «*…i udbydernes net…*»
68. «Subscriber number» is «any number included in the comprehensive Danish number plan, that may be allocated to an end-user", cf. DECA § 2 no. 15.
69. LFF-2021 Gen. Comm. p. 30.
70. See Section 5.1.3.3.

6.5 Provider

6.5.1 The definition

The data retention provisions specify generally that the obligation to retain data is incumbent on "providers" *("udbydere")*. "Provider" is defined in DECA § 2, no. 1as

> anyone who for a commercial purpose makes products, electronic communication networks or -services encompassed by DECA available to others.

The condition "for a commercial purpose" is central to the definition and means that the product, network, or service must be offered for the purpose of gaining a profit directly or indirectly.[71] Seemingly, the condition is easily applicable to actors providing fixed and mobile telephony. On the internet side however, the situation is a bit more complicated.

Firstly, it is not relevant whether the activity in fact generates a profit or not. For instance, a hotel offering "hot-spot" internet in the lobby, or internet or telephony in the hotel room, and does this without compensation, is still deemed to be a "provider" as the reason for offering the service is to make the hotel more attractive, thus gain a profit.[72] The commercial purpose is also fulfilled if the activity normally is offered for profit, even though commercial activity is not the main objective. For instance, a local municipality renting out a building to local entrepreneurs including "free" internet, is a "provider" within the meaning of DECA, therefore also within the meaning of the data retention rules.[73]

Libraries, hospitals, universities, schools etc., offering electronic networks or services to their clients, are not deemed to do this for a commercial purpose, hence are not "providers".[74] Instead, they are "end-users" as explained in Section 6.4.2. To illustrate: A provider must retain data related to its own e-mail service (see Section 6.4.1, points 8 and 9). A provider is a provider within the meaning of the law only if the service is offered for a commercial purpose. With an example from a Norwegian context; the commercial e-com company Telenor that offers the e-mail service @online.no, would (pursuant to Danish regulation) have an obligation to retain data about the sender's and the recipient's e-mail address, while the University of Oslo that offers the e-mail service @uio.no, to its 33 000 students and staff members, is deemed not to have a commercial purpose and would not have to retain such data.

71. See Section 5.1.3.3.p. 21
72. See Section 5.1.3.3.
73. See Section 5.1.3.3.
74. See Section 5.1.3.3.

Furthermore, recalling that the list of traffic data includes data related to the "provider's own internet-based phone services,"[75] the question is who these providers are, specifically whether providers of NI-ICS generally are included.[76] The question was touched upon in Section 6.4.1, but it is possible to dig a little deeper. At the outset, to be provider of a service within the meaning of DECA § 2, no. 1, the service must be an "electronic communications service" as defined in DECA § 2, no. 9. The definition requires the service to be transmitted between "network termination points", i.e., physical end points in the electronic network (DECA § 2, no. 8). NI-ICS as defined in DECA § 2 no. 20 is not a service transmitted between physical endpoints, rather use of NI-ICS requires that internet access (a network termination end point) is already available. This prompts the question whether a provider of an internet-based phone service as mentioned in the list of "traffic data" set out in Section 6.4.1, must offer the service *in addition* to a service that is transmitted between network termination points such as fixed and mobile telephony, or internet access. In such case, only a small number of NI-ICS providers are "providers" within the meaning of the data retention rules.

6.5.2 Internet Access Providers

As rpl. § 786 f concerns retention of internet access data, a "provider" within the meaning of the provision must mean one who provides an internet access service. Reg. 380 sets out further details. Firstly, § 1 makes clear that the term "provider" shall have the same meaning as in DECA § 2, no. 1., entailing that the condition "for a commercial purpose" applies. However, transmission of radio- or TV-programs (over the internet) is positively excluded from the regulation (§ 2). This is in line with the e-kodex Directive Article 2 no. 4, which excludes services exercising editorial control over electronic content (see Section 5.1.3).

Organisations that provide internet access to their members are not comprised by the obligation unless the number of members is 100 or more (§ 3). Organisations set up to manage apartment complexes could be covered by this rule.[77] If several providers register the same data, at least one of them shall do this as an obligation under rpl. § 786 f (§ 5). A provider may enter into an agreement with another provider or a third party about registration and storage of internet access data on its behalf (§ 6).

75. See Section 6.4.1 points 10 to 13.
76. NI-ICS is explained in Section 5.1.3.4.
77. § 3: "... andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger og sammenslutninger heraf der indenfor foreningen eller sammenslutningen tilbyder elektroniske kommunikationsnet eller -tjenetser til færre enn 100 enheder.»

6.6 Access to retained data

The police may gain access to retained data by use of production order pursuant to the provisions set out in rpl. Ch. 74 Seizure and Production Order *(beslaglæggelse og edition).* A production order may compel a person who is not a suspect to provide access to an object in his or her custody, if the object is deemed to be relevant as evidence in a criminal investigation (rpl. § 804 in conj., with § 801 first para., no. 1). The offence under investigation must be subject to public prosecution *(offentlig påtale)*. A production order with legal basis in rpl. § 804 must be issued by a court (rpl. § 806 second para.).

However, in respect of "traffic and location data" retained pursuant to rpl. §§ 786 b to 786 e, rpl. § 804 a is the legal basis for a production order. This provision makes the conditions and safeguards applicable to udvidet/teleoplysning) applicable to police access to retained traffic and location data as well, see rpl. § 804 a in conj., with §§ 805 and 806. These conditions and safeguards were explained in Section 5.4.6. The decision is made by the court. The police may make the decision should the purpose otherwise be compromised. In such case a judicial review must be obtained within 24 hours (rpl. § 806 fourth para.). Importantly, to access traffic and location data the investigation must concern an offence with a prescribed maximum penalty of no less than three years. This substantially raises the threshold compared to production order issued pursuant to rpl. § 804. The regulation of access to traffic and location data is also in alignment with the conditions for access to preserved data (rpl. § 786 a) (see Section 5.3.1).

Rpl. § 804 b concerns production order regarding data that "identify an end-user's access to electronic communications networks or-services." The provision is applicable to retained static internet access data, IMEI and IMSI numbers. The order may be issued by the police. This differs from §§ 804 and 804 a, according to which the court must make the decision. However, similar to the condition set out in rpl. § 804, the investigation must concern an offence liable to public prosecution. Dynamic data about internet access, such as dynamic IP-addresses and source port numbers may not be accessed on basis of rpl. § 804 b, instead the procedure prescribed in rpl. § 804 must be applied, entailing that a court order is needed as opposed to an order of the police.[78] This extra safeguard was deemed necessary as identifying relevant dynamic data might not be as straightforward as for static data. The difference in legal procedure for access to static and dynamic IP-addresses is however not easily discerned from the text of the legal provisions themselves. Also data not subject to retention such as signal data must be accessed pursuant to § 804. As the provider's possession of the data is unrelated to any duty to retain, such data fall outside the scope of rpl. §§ 804 a and 804 b.

78. LFF-2021 Spec. Comm. to rpl. §§ 804 a and 804 b, p. 103-104.

7. Finland

7.1 Introduction

FECA § 157 provides for data retention "in the interest of public authorities." The provision is localized in FECA Part VI "The confidentiality of communication and protection of integrity." This part also includes, i.a., the general obligation of confidentiality (§ 136), and general principles for the processing of data (§ 137). To data retention the following principles seem particularly relevant:

- Electronic messages *("meddelanden")*[79] and related data *("förmedlingsuppgifter)*[80] may be disclosed solely to actors who have a legal basis for processing the data (§ 137 second para.).
- Once lawful processing is finalized the data shall be destructed or transformed so they cannot be related to the subscriber[81] or user,[82] unless further storage is mandated by law (§ 137 third para.).

7.2 The data to be registered and stored

The data to be retained are specified in FECA § 157 second and third para., as follows:

Second paragraph: Data related to the following services:

1. **Telephone services and text messaging services in mobile networks**, including communications connecting with the endpoint without reaching the recipient (*unsuccessful calls*), and communications that were hindered due to operational interventions in the network,
2. **Internet telephone services**, i.e., services based on internet protocol all the way to the end-user[83] making conversation possible,
3. **Internet access services**.

Third paragraph sets the data out in detail:

79. See FECA § 3 no. 22: "electronically transmitted or distributed information".
80. See FECA § 3 no. 40: "information related to a legal or natural person and is processed in order to transmit electronic messages ... [omitted]."
81. See FECA § 3 no. 30, and Section 5.4.2.
82. See FECA § 3 no. 7, and Section 5.4.2.
83. See FECA § 3 no. 10 a: "a physical or legal person using or requesting access to a communications service or VAS, and does not itself provide publicly available electronic communications networks or services to others."

Re: The data related to the services mentioned in points 1 and 2 above:

- the subscriber's and registered user's name and address,
- data identifying the subscription agreement *("abonnemang")*,
- data on basis of which users of communication services may be identified, and the users' transactions, including forwarded communications *("omstyrda samtal"),* based on the type of message, the recipient, time and duration of the communication.

In addition, regarding services mentioned in point 1 above, the following data:

- Data that may assist in the identification of the communications equipment used in the transaction, and the geographical position of the communications equipment and of the subscription agreement at the time when the transaction commenced.

Regarding a service as mentioned in point 3 the following data:

- The subscriber's and registered user's name and address,
- data identifying the subscription agreement and the address where it is installed,
- data that may assist in the identification of a user of communications services and the equipment used, and time and duration of use of the service.

The registration of data shall not exceed that what is necessary for the purpose (FECA § 157 third para., last sentence). It is emphasised that the obligation does not concern content data or data exposing servers accessed by the user (§ 157 fifth paragraph). Finally, it is made clear that the obligation is limited to concern data that are available and have been generated or processed as part of the ordinary operation of the service (§ 157 sixth paragraph).

7.3 Storage period

The storage time is specified in § 157 fourth paragraph:

- 12 months regarding services mentioned in point 1 above,
- 6 months in respect of services mentioned in point 2 above,
- 9 months in respect of services mentioned in point 3 above.

The storage time commences when the "the transaction" begins.

7.4 Provider

The Ministry of the Interior decides who shall retain data (FECA § 157 first para.), who then gets status as *"lagringsskyldigt företag*." However, only *"teleföretag"* may be designated, i.e., providers of publicly available electronic communications networks or -services (FECA § 3 no. 27). Providers of "small significance" *(ringa betydelse)* may not be subject to an obligation to retain (§ 157 second sentence). Prior to the entering into force of the retention obligation, the provider and the Minister of Interior shall negotiate the "authorities' needs" regarding data storage (FECA § 158). As per August 2023 there are 4 *lagringsskyldige företag*, selected according to their aggregate market share and geographical coverage of the services.[84]

7.5 Access to data

Retained data may be used only in the investigation and prosecution of offences that may give basis for *teleövervakning and the* same procedure as for *teleövervakning is applicable* (FECA § 157 first para., last sentence, in conj., with tvml. 10:9). The decision is made by the court (in exigent circumstances by a police officer, to be reviewed by the court within 24 hours). The offences that may give basis for use of *teleövervakning* were described in Section 5.4.2.

84. E-mail 4 August 2023.

8. Iceland

[85]

The IECA Article 89 third para., states that telecommunications companies must, in the interests of *criminal investigations and public safety*, keep a minimum record of data on users' electronic communications traffic for *six months.*

The minimum registration must ensure that a telecommunications company can inform which of its customers was the user of a particular telephone number, IP address or username, as well as providing information on all connections made by the user, their dates, who was connected and the amount of data transfer to the respective user, as well as which phone number a particular customer had during a particular period.

A telecommunications company must ensure the safekeeping of the above-mentioned data and is not permitted to use, or hand over, said information to anyone other than the police or the prosecution in accordance with the provisions of IECA Article 92. The traffic data *must be deleted* after this time as it is no longer needed.

IECA Article 92 states that a telecommunications company is obliged to comply with the police's requests for assistance in the investigation of a criminal case, given that those requests are based on *a court order or are authorized by law.* Telecommunications companies must establish procedures for responding to requests for police access to users' personal information. The rules on how the police authorities can obtain such data can be found in the Code of Criminal Procedure (CCP), no. 88/2008. CCP Articles 80-82 are the provisions that the authorities use to obtain a court order for telephone tapping/interception and other comparable measures. In addition to this, the Director of Public Prosecution has published instructions no. RS: 12/2017 on how surveillance with an interception and other measures should be carried out (available in Icelandic).

85. The information is provided in attachment to e-mail dated 17 March 2023.

9. Norway

9.1 Introduction

In 2011 Norway passed the Data Retention Act *(Datalagringsloven),*[86] which implemented the DRD in the national legal system. The Government got delegated power to determine the date for its entering into force. At the same time the case *Digital Rights Ireland* made its way through the justice system, causing national hesitation to make the law become effective. As per current, the law has not entered into force, nor is it repealed. Norway has initiated preparations for implementing the e-kodex Directive, but as of September 2023 the process is not completed.[87]

In 2021 the Retention of IP-addresses Act was passed.[88] The act amends NECA by supplementing it with a provision imposing an obligation on providers to register and store IP-addresses etc. (§ 2–8 a), and a provision setting out the procedure for police access to the data (§ 2–8 b). It further amended § 2–7 fifth para., to provide for a duty to delete retained data once the storage period expires. The act entered into force 1 January 2022.

The data retention rules are separated from procedural provisions concerning coercive measures related to private communication, production order and expedited data preservation.[89]

Prop. 167 L (2020-2021) is the main preparatory document to the act. It states that as electronic communication services are increasingly becoming internet based, and criminals commonly make use of such services, access to data related to the communications are important and sometimes vital to the possibility of the police to investigate and prosecute crime.[90] It is therefore important to ensure that the data are available to the police in criminal investigations. This purpose is accentuated in NECA § 2–8 a first para., according to which providers shall retain data so that they may be used "in the investigation of serious crime."

86. Act of 15 April 2011 no. 11.
87. Proposal for a new e-com act was publicly announced 2 July 2021, and deadline for feed-back set to 15 October 2021. Information about the preparatory process may be accessed here: Høring - Forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften - regjeringen.no (accessed 15 September 2023).
88. Act of 18 June 2001 no. 131 (Lov om lagring av IP-adresser mv.)
89. Described in Section 5.3.4 and 5.4.4.
90. Prop. 167 L (2020-2021) Ch. 2.1

9.2 The data to be registered and stored

Pursuant to NECA § 2–8 a, providers shall "store the data necessary to identify the subscriber on basis of:

a. The public IP-address and time of the communication, or
b. When a public IP-address is shared simultaneously by several subscribers, also data about the source port, and the time of the communication."

The data on the list refer to the source of the communication. Destination data shall not be retained (§ 2–8 a first para., last sentence).

"Subscriber" *("abonnent")* as mentioned in § 2–8 a, is not a defined notion in the NECA, which instead offers definitions of "user" and "end-user" (§ 1–5 no. 14 and 15). The definitions comprise a natural or legal person who "uses electronic communications networks or -services for own use or as a resource in the production of other services" ("user" (no. 14)), or "enters into an agreement about access to an electronic communications network or -service for own purpose or to lend out to others" ("end-user" (no. 15)). Depending on the situation, a "subscriber" as mentioned in § 2–8 a, could possibly be "user" and "end-user." This is further discussed in Section 9.4 in relation to the definition of "provider."

A provider shall thus register and store data necessary to identify the person to whom an IP-address has been assigned. Identification may be based on data (provided by the police) about the IP-address that was used, and the time it was used (§ 2–8 a, point a). The provider must thus maintain a register that keeps track of the persons to whom IP-addresses (fixed or dynamic) were assigned at any time of the storage period.

When a provider arranges for an IP-address to be shared between several users at the same time, the source port number must be registered in addition to the time of the communication. As explained in Section 5.1.3.2, this is necessary to identify the equipment used to access the internet, and thereby the user. This is provided for in § 2–8 a point b.

9.3 Storage period

The data shall be stored for 12 months from the date "when the communication ended" (§ 2–8 a second para.), whereupon they shall be deleted (§ 2–7 fifth para., point 2).

As the obligation to retain data concerns "data necessary to identify the subscriber" based on the data mentioned in § 2–8 a, it seems a bit odd that the provision relates the storage period to the time when the "communication" ended.

The meaning is probably 12 months from the time when the subscriber's entitlement to the IP-address was terminated, that is, for instance with respect to dynamic IP-addresses, be when s/he logs off. That would correspond to point 4 of the Danish regulation of internet access data.[91]

9.4 Provider

Pursuant to § 2–8 a first para., the obligation to retain data is incumbent on

> provider of electronic communications network used for public electronic communications service, and provider of such service.

The provision must be read in conjunction with the legal definitions set out in § 1–5 no. 3, 4 and 16, pursuant to which a "provider" is a natural or legal person who makes access to electronic communication networks or -services available to others (no. 16); an electronic communication service is "normally provided for remuneration" (no. 3); and to be "public" the service must be "available to the public or intended to be used by the public" (no. 4). It follows that the obligation is incumbent on internet access providers who offer the service to the public for remuneration.

It has been noted that actors such as libraries, hospitals and other public institutions, hotels, airports, cafes, and restaurants, offer their internet access as a service to others. This raises a question about the interpretation of "public" service. Prop. 197 L (2020-2021) Ch. 8.1.4 emphasises that large numbers of users is not sufficient per se to make the service public within the meaning of § 2–8 a. It is underlined that this type of actors rather is deemed to be "owners of private networks." The interpretation entails that the Norwegian definition of "provider" is less broad than the Danish (see Section 6.5).

Prop. 197 L (2020–2021) makes clear that there shall be no legal differentiation between small and large providers in relation to data retention. Hence, a few big providers holding a 95% market share, and approximately 300 small providers sharing the remaining 5%,[92] all are subject to the obligation to retain and store data. There are different business models among providers, and they may enter into agreements settling who in the chain of services that shall fulfil the obligation.[93]

91. Section 6.4.2 *«The point in time when the internet was accessed, and when the access was terminated".* A corresponding remark is made in relation to the Swedish regulation, see Section 10.3.
92. 2018 statistics. Prop. L 167 (2020-2021) Ch. 8.1.2.
93. Prop. 197 L (2020-2021) Ch. 8.1.2.

9.5 Access to data

9.5.1 Introduction

Data retained as per § 2–8 a may be accessed in accordance with the procedure laid down in § 2-8 b. The provision clarifies that the confidentiality obligation set out in § 2–9 does not prevent the police and prosecuting authority from accessing the data. Furthermore, it lays down conditions concerning purpose, criminality, and necessity, and provides some safeguards.

9.5.2 Purpose, who that may access the data, and personal scope

Pursuant to § 2–8 a retained data may be disclosed to "the police or prosecuting authority" in a criminal investigation. As indicated in § 2-8 a, the investigation must concern "serious crime", and the relevant offences are further specified in § 2-8 b as follows:[94]

- any offence with a statutory level of punishment of imprisonment of 3 years or more, or
- the following offences with a lower level of punishment as set out in the Criminal Code:[95] §§ 125, 168, 184, 201, 202, 204, 205, 251, 263, 266, 297, 298, 305, 306, or 309. In addition, the Copyright Act § 104 in conjunction with § 79.

The specification includes offences for which internet is deemed to be a practical and sometimes necessary tool to commit.[96] Thus included are sexual offences of children, such as lascivious speech, grooming and solicitation of sexual services (§§ 297, 298, 305, 306 and 309), forcefully submitting a person to one's own will, or use of threat (§§ 251, 263), breach of an official contact restraint order, etc. (§ 168), identity theft (§ 202), ruthlessness (266), offences targeting computer and electronic communication systems (§§ 201, 204 and 205), neglectful exposure of state secrets (§ 125) and disturbance of the peace of another state (§ 184). Finally, the Copyright Act § 104 protects the right to one's own photograph, that is, the right of an identifiable person on a photograph. Making such photo public without consent from the identifiable person is punishable with a fine or imprisonment for a period not exceeding one year (§ 79).

The criminality condition for access to retained data is lower than the one applicable to secret collection of data related to electronic communication, as per strpl. § 216 b.[97] For the latter the condition is imprisonment for a maximum period of at least 5 years, instead of 3 years as set out for retained data. The difference may be explained in light of the measures' difference in scope; strpl. § 216 b

94. Prop. 167 L (2020-2021) Ch. 2.1
95. Act of 20 May 2005 no. 28.
96. Prop. 197 L (2020-2021) Ch. 8.5.4.1.
97. See Section 5.4.4.

providing access to traffic and location data including data related to internet communication, whereas NECA § 208 b is limited to concern internet access data.

9.5.3 The necessity condition

Providing access to IP-addresses etc., is deemed to interfere with the right to private communication. To be lawful, such interference must be "necessary" to the investigation of a serious crime, as per § 2–8 b. A concrete assessment of the necessity of the data for the purpose of the investigation must be made, and it is implied that the assessment also involves proportionality.[98] The assessment must balance the needs of the investigation against the interests in protecting private communication. Concretely, the condition entails that the request put forward to the e-com provider must not ask for more data than needed for the purpose. Necessity does not imply that the data must be *critical* to the investigation, but it is not sufficient that the data would be "nice" to have. For instance, if a different yet more cumbersome option is available, the necessity condition might not be fulfilled. [99] The assessment is highly contextual as the right to private communication may weigh in differently depending on the circumstances of the case.

The assessment is to be conclusively made by the police or public prosecutor. The provider receiving the request shall not review the assessment.[100]

9.5.4 Formal conditions – safeguards

The request may be issued by the police or a public prosecutor. It shall be made in writing, stating what the investigation is about, the purpose of the request and the data necessary for that purpose. The request may go both ways, meaning that subscriber data may be disclosed based on data about the IP-address, and IP-addresses may be disclosed on basis of subscriber data (historic list of IP-addresses allocated to a subscriber).[101] This opens the possibility for using data collected in the investigation as basis for a request to the provider, for instance to find out which IP-addresses a specific person used at a point in time relevant to the crime under investigation.

The request shall further confirm that the necessity assessment has been performed.

NECA § 2-8 b fourth paragraph, emphasises that data that are stored "solely" pursuant to § 2–8 a, may not be disclosed for purposes other than those already specified. Production orders issued pursuant to other provisions, e.g., in the Civil Procedural Code, the Copyright Act or other acts, may not compel disclosure of the data.

98. Prop. 197 L (2020-2021) Ch. 8.5.4.3.
99. Prop. 197 L (2020-2021) Ch. 8.5.4.3.
100. Prop. 197 L (2020-2021) Ch. 8.5.4.3.
101. Ch. 8.5.4.4, p. 57-58.

Retention of IP-addresses etc., is regarded as less intrusive than retention of traffic data, as the IP-addresses are not suitable for making profiles of subscribers' internet habits. Hence there is no court review, and the procedure for gaining access is rather informal. However, the police and the prosecuting authority shall produce an annual report describing the collection of data (NECA § 2–8 b). The report shall be submitted to the National Authority for Electronic communication (Nkom).

9.5.5 Crime prevention

The preparatory works show that the legislator considered whether the police should have access to retained subscriber data related to internet access, also in crime prevention. This is relevant, i.a., to intelligence activities in order to prevent and detect economic crime, serious crime, and protect national security. It was concluded that the issue needed further deliberation. As per current the data may be used for the purpose of criminal investigation only.[102]

102. Prop. 167 L (2020-2021) Ch. 8.5.4.2.

10. Sweden

10.1 Introduction

Following the *Tele2-judgement*[103] the Swedish data retention rules were revised, with effect from 1 October 2019. The law prior to the revision provided for general undifferentiated retention of data related to telephony, messaging, and broadband services. The data were to be stored for a period of 6 months. The data could be accessed both for the purpose of criminal investigation pursuant to rules set out in the Procedural Code *(Rättegångsbalken ("RB")),* and intelligence gathering by law enforcement authorities pursuant to rules set out in the Electronic Intelligence Act ("EIA") *(Lag om innhämntning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelsesvärksamhet).* In the Tele2 judgment, the European Court of Justice concluded that the regulation exceeded the limits of strict necessity and could not be justified in a democratic society.

The current data retention provisions are laid down in SECA.

10.2 The data to be registered and stored

The data to be registered and stored are broadly specified in SECA 9:19, and the data must at the outset be such "as referred to in 9:31 first para., no. 1 and 3". No. 1 concerns "data about subscription" *(en uppgift om abonnemang);* no. 3 concerns "other data that concern a specific electronic communication" *(en annan uppgift som angår ett särskilt elektroniskt meddelande).*[104] No. 2 concerning content data is not relevant to the present context.

SECA 9:19 further specifies that the data are such as are

> necessary to trace and identify the source of the communication, the final destination of the communication, date, time, and duration of the communication, type of communication, communication equipment, as well as the location of mobile communication devices at the time of the communications' beginning and end.

103. Joined cases C-203/15 and C-698/15.
104. *"Elektroniskt meddelande"* could be translated to "electronic message," but the definition set out in SECA 1:7 rather suggests "electronic communication" to be more suitable, as the definition includes interpersonal communication no matter the form (message, audio/video communication, etc.): *"Elektroniskt meddelande"* means "all information exchanged or transmitted between a delimited number of persons through a publicly available electronic communications service, except for information transmitted as part of transmissions of audio radio or TV-program directed towards the general public through an electronic communications network, unless the information may be connected to *(sättes i samband med)* a specific subscriber or user of the information."

Second paragraph of the provision clarifies that the obligation to register and store data concerns data "generated or processed" at

1. a telephone service, or the processing of messages *(meddelandehandtering)* [105] through a mobile network termination point,[106] or
2. internet access.

Data shall be retained also in respect of communications that reach the end-point without reaching the recipient *(misslyckad uppringning)*[107] (9:19 third paragraph).

The data are described in more detail in Government Regulation on Electronic Communications (2022:511) 9:7 and 9:8.

A. Telephony services and messaging; only communications via a mobile access point:

1. calling and called numbers or equivalent address;
2. for telephony services: callers and called subscriber- and equipment identity;
3. data on subscriber and registered user connected to 1 and 2;
4. date and time when the communication was initiated and terminated, or a message was sent and received;
5. data on location at the beginning and end of the communication;
6. date, time and location of first activation of pre-paid, anonymous services.

B. Internet access:

1. Users IP-addresses and other data necessary to identify a subscriber and registered user*;
2. data on subscribers and registered users;
3. date and time regarding logging on and off the service that provides internet access;
4. data that identify the equipment that finally seclude the communication from the service provider to the subscriber.

* Carrier Grade NAT

Re: A, Telephony: The heading specifies that the obligation concerns "only" mobile communication. This leaves out fixed telephony and IP-telephony, thus a reduced scope compared to the regulation in Denmark.[108]

Re: B, Internet access: B no. 1 deals with the situation where one IP-address is shared by several users. In addition to users' IP-addresses "other data necessary to identify a subscriber and registered user" shall be registered. A similar wording is

105. *"meddelandehandtering"* means "exchange or transmission of an electronic message which is not a real-time voice communication nor is information transmitted as part of radio- or TV-transmission" (SECA 1:7).
106. "*nätanslutningspunkt*", (SECA 1:7) and "network termination point" (e-kodex Art. 2 point 9).
107. "*misslyckad uppringning*" (SECA 1:7).
108. Section 6.4.1.

used in B no. 4. A corresponding situation is dealt with in NECA § 2–8 a point b, however here the data are specified ("source port" and "time of the communication"). The general wording in the Swedish regulation might make it more resilient to changes caused by technical development, as it encompasses the data that are relevant for the stated purpose under any given technical solution.

The Post and Telecom Authority may specify in a delegated regulation which data shall be retained according to Chapter 9:7 and 9:8 of the Government Regulation. This is relevant in relation to the retention of data for the purpose of identifying subscribers and registered users in connection with the use of Carrier Grade NAT-technology. On this issue, the Post and Telecom Authority has laid down a specific retention obligation that entered into force 1 April 2020. The obligation entails retention of data on public IP-address and appurtenant UDP or TCP port numbers linked to the users' IP-address and traceable time for the connection.[109]

The persons whose data are registered are referred to as "subscriber", "registered user" and "user". "User" is "a natural or legal person using or intending to use an electronic communications service." "End-user" is a sub-category, meaning "a user not providing a publicly available electronic communications service" (SECA 1:7). The obligation to retain data concerning internet access thus encompasses both users and end-users.[110]

10.3 Storage period

The storage period is set out in SECA 9:22 as follows:

- Data related to telephony or the processing of messages through a mobile termination point: 6 months. However, location data may be stored for 2 months only.
- Data related to internet access shall be stored for 10 months. However, data that identify the equipment that finally secludes the communication from the service provider to the subscriber shall be stored only for 6 months.

The storage period commences on the date when the communication ended.[111]

The data shall be deleted upon expiration of the storage period (9:22 third para.). Exception is made in respect of data comprised by a request of access based on

- SECA 9:33 first para., point 2 and 5; (access to subscriber data)[112]
- RB 27:19; (secret surveillance in the investigation of serious crime)[113]

109. E-mail 21 March 2023.
110. It has not been possible to clarify how far down the service chain the obligation is applied.
111. Regarding internet access, the meaning must rather be when use of the IP-address ended. This also corresponds to Government Regulation B no. 3 "date and time regarding *logging on and off* the service that provides internet access." See similar comment to the Norwegian regulation in Section 9.3.
112. See Section 5.2.5.
113. See Section 5.4.5.

- EIA *(lag 2012: 278),* (secret surveillance in intelligence activities),[114] or, the data are subject to a preservation order as per RB 27:16.[115]

In such case, the provider shall continue to store the data until they have been disclosed as per the request or the preservation period has expired. Then the data shall immediately be deleted (9:22 third para.).

10.4 The person obliged to register and store data

The obligation to register and store data comprises "anyone who conducts activities that must be notified" to the Post and Telecom Authority (SECA 9:19). The Post and Telecom Authority shall be notified when the activity concerns "public communications networks that are usually provided against compensation or publicly available electronic communications services" (SECA 2: 1). Pursuant to SECA 1:7 an "electronic communications service" is a service that is "usually provided against compensation." The regulation corresponds prima facie to the regulation in Denmark and Norway. Whether the application is the same a different question. As noticed, especially regarding internet access, the interpretation may vary despite similarities in the wording of the legal provisions. Differences in interpretation have thus resulted in different data retention regimes for internet hot spots in Denmark and Norway.

10.5 Access to data

Pursuant to SECA 9:21, retained data may be accessed with legal basis in

- SECA 9:33 first para., points 2 and 5;
- RB 27:19; or
- EIA *(lag 2012: 278).*

As noted in Section 5.2.5, SECA 9:33 applies to providers of electronic communications networks or -services, excluding providers of NI-ICS. The provision must be read in conjunction with SECA 9:31, laying down the duty of confidentiality in respect of:

1. Subscriber data,
2. The content of the communication, and
3. Data related to the communication.

114. See Section 5.4.5.
115. See Section 5.3.5.

SECA 9:33 first para no. 2: Access to *subscriber* data was dealt with in Section 5.2.5, reiterated here: The provision is applicable to requests concerning "criminal activity or suspicion about a crime", put forward by Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten or «any other authority tasked with such intervention." The data that may be made accessible by the provider are "data about a subscription agreement" (as per § 31 first para., no. 1).

SECA 9:33 first para no. 5: Access to data related to an electronic message *preserved* in accordance with RB 27:16.[116] The data necessary to disclose the providers involved in the transmission of the message, shall be disclosed to the public authority who ordered that the data be preserved. The same must apply if the data have also been retained.

RB 27:19 (in force from 1 October 2023): The provision concerns "secret surveillance", i.e., the secret collection of

1. data related to electronic messages[117] under transmission or that have been transmitted to or from a telephone number or other address,
2. data disclosing the electronic communications equipment that have been present in a specific geographic area, or
3. data disclosing in which geographic area a specific electronic communications equipment is or has been located.

Retained data of the kind mentioned above may be disclosed to the police in the investigation of an offence (including attempt and preparatory acts)

- punishable with imprisonment for a minimum period of 6 months or more,
- other offences as specified (hacking, child sexual abuse material, drugs), and
- and offences that may incur secret interception of electronic communication pursuant to RB 27:18 a second paragraph. This follows from RB 27:19 a (into force 1 October 2023).

The Electronic Intelligence Act ("EIA"): This act provides for the collection of the same data as mentioned in RB 27:19 when necessary for intelligence activities aimed at preventing, intervening against, or uncovering criminal activities as further specified in that act.[118] The reference to the EIA in SECA 9:21 entails that retained data may be accessed for intelligence purposes. The activity must concern an offence with a prescribed penalty of imprisonment for at least 2 years or other offences as specified in EIA § 2. The authorities that may access retained data for intelligence purposes are the Police Authority, the Police Security Service, and the Customs Authority.

116. See Section 5.3.5.
117. If "messages" *(meddelanden)* shall be interpreted to have the meaning used in SECA, the meaning is "electronic communication", see the comment made in this regard in Section 10.2.
118. Data related to number-independent interpersonal communications services are not included.

10.6 SOU 2023:22: Proposal for a law revision

10.6.1 Introduction

SOU 2023: 22 *Datalagring och åtkomst till elektronisk information* (data retention and access to electronic information) ("the Expert Report") proposes a law revision resembling the regulation in Denmark. The proposal concerns general, undifferentiated data retention to protect national security, and targeted data retention to combat serious crime. Data related to NI-ICS are included. The Expert Report was publicly distributed for feedback *(remiss)* 7 July 2023, with deadline 1 November 2023.

10.6.2 Proposed amendments to SECA

The revision requires the passing of new laws that shall refer to SECA, to Chapter 9 in particular. The material amendments to SECA Chapter 9 are as follows:[119]

Also providers of NI-ICS shall retain data (supplement to SECA 9:19).

The data to be retained are categorized in §§ 19 a to 19 e. The storage time is set out in § 22.

- § 19 a: *Subscriber data*. To be stored 1 year from termination of the subscription or of a temporary assignment of a service (§ 22).
- § 19 b: Data retained for the purpose of *protecting national security*. To be stored for 2 years (§ 22).
- § 19 c: Data related to *geographic area*. To be stored for 1 year (§ 22).
- § 19 d: Data necessary to *combat serious crime* (extended targeted data retention). To be stored for 1 year (§ 22).
- § 19 e: The data to be retained pursuant to § 19 b *shall* include data related to *unsuccessful calls*. The data to be retained pursuant to §§ 19 c and 19 d *may* include data related to unsuccessful calls.

Providers have a duty to ensure that their services are arranged so that data retention obligations become effective. Moreover, they shall ensure that data retention is not disclosed (§ 29). Access to retained data shall be facilitated in a manner that maintains secrecy of the measure (§ 29 b).

119. Expert Report p. 60 ff.

10.6.3 General, undifferentiated data retention to protect national security

"Proposal of an Act (2025:000) concerning retention of and access to data related to electronic communication for the purpose of protecting national security."[120] The act has a counterpart in the Danish rpl. § 786 e.

A data retention order may be issued if there is a "serious threat against Swedish security that is real and present or foreseeable." Pursuant to § 3, an order may be issued only if deemed "strictly necessary" *("absolut nödvändigt")* to protect national security. The order shall be limited only to concern that which is strictly necessary for the purpose, concerning,

1. The *providers* that should retain data,
2. The *duration* of the data retention period, and
3. The *data* comprised by the order.

The order may be made by the Police Security Service *(Säkerhetspolisen)*. Prior to making the decision the Service shall seek advice from the Military Defence (§ 2).

The order may be issued for 1 year as a maximum (§ 2 second para.) and be prolonged if the threat against Sweden persists. An order must generally not exceed what is necessary for the purpose (§ 3 no. 2) and shall be repealed once the reason for the order ceases to exist (§ 2 second para.).

There is an oversight mechanism provided by a national public authority to be designated by the Government (§§ 4 and 7).

10.6.4 Targeted data retention to combat serious crime

"Proposal of an Act (2025:000) concerning retention of data related to electronic communication for the purpose of combating serious crime."[121]

Data retention in a specific geographic area. (Danish counterpart in rpl. § 786 c). Data retention shall be performed in "specific municipalities" *(vissa kommuner)*, where the level of *reported* crime is on par with or exceeds the aggregate national crime rate (§§ 2 and 3). The Post and Telecom Authority shall determine the municipalities that shall have to retain data, and do this on an annual basis not later than 1 June (§ 4).

Extended targeted data retention. (The provisions do roughly correspond to the Danish rpl. §§ 786 b to 786 d).

120. Förslag till lag (2025:000) om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet, Expert report p. 42 ff.
121. Förslag till lag (2025:000) om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet, Expert report p. 47 ff.

Data retention in a specific area may be supplemented with a decision about extended targeted data retention by the Police Authority, the Police Security Service or the Customs Authority. The decision is not subject to complaint (§ 11).

The decision may concern:

1. A delimited geographical area where offences as mentioned in RB 27:19 third para., is committed, or is likely to be committed;[122] Maximum retention period: 1 year.
2. A place worthy of protection (Danish counterpart: rpl. § 786 c second para.). Maximum retention period: 3 years.
3. A person who is or has been subject to (Maximum retention period: 1 year)
    a. secret coercive measures as set out in RB,
    b. secret computer surveillance, as per law (2020:62) about secret computer surveillance
    c. a decision pursuant to EIA (collection of data for intelligence purposes),
4. a person who has been sentenced or accepted punishment regarding an offence as mentioned in no. 1 (Maximum retention period: 1 year).
5. Communications equipment or subscriber identity used or likely to be used in the commitment of an offence as mentioned in no, 1, or in criminal activity *(brottslig verksamhet)* involving such offences. Maximum retention period: 1 year.

The data retention periods are specified in § 8.

The Swedish provisions do not require a court decision to retain data. The Danish rpl. § 786 d stands out in this regard. However, decisions about extended targeted data retention shall be subject to oversight by the Committee for the Protection of Security and Integrity *(Säkerhets- och integritetsskyddsnämnden)* (Law (2007:980).[123]

10.6.5 Access to data

Retained data may be accessed pursuant § 11, according to a decision about secret interception or secret electronic surveillance pursuant to RB 27:18 and 27:19, or a permission issued pursuant to the EIA. Data retained for the sake of protecting national security may be accessed *solely* for that purpose (§ 21 second para.).

122. The offences were described in Section 10.5.
123. Expert Report p. 50-51.

Part III: Concluding remarks

The study shows significant discrepancies in the data retention regulation of the Nordic countries. Denmark has aligned the data retention rules with the rules of data preservation and secret coercive measures interfering with electronic communication, as well as rules concerning subscriber identification. The aim is to the widest extent possible, ensure the availability of data that may be necessary to an investigation of serious crime or protect national security, including to identify perpetrators of serious crime, while still respecting fundamental human rights.

Seemingly, among the Nordic countries only Sweden performs data retention for the purpose of preventing, averting, and detecting crime in addition to criminal investigation and prosecution. The Swedish Expert Report SOU 2023:22 proposes a revision of the data retention rules to closely resemble the Danish. It is proposed that retained data shall be available for intelligence purposes also in the future. In contrast, Denmark has provided legal basis for general undifferentiated data retention to protect national security, without extending the right of access to include intelligence purposes.

Norway stands alone with data retention rules that are limited to concern internet access services only. The other countries include telephone services and IP-telephony in addition, though the extent to which the services are included is not identical. The legal situation regarding NI-ICS is also a bit unclear.

A recurring question concerns the scope of data related to internet access services. It has been demonstrated that legal provisions that prima facie are similar may have different outcomes, illustrated by the differences between Denmark and Norway in the application of data retention rules to “hot spot” internet at restaurants and hotels. The issue seems to be influenced by several factors that are quite different from each other. Firstly, there is the interpretation of the e-com definitions, that is, how to interpret “publicly available” and “normally for remuneration.” A point in this regard is that there seems to be no explanation offered by the legislator, for not making use of the reservation provided by the word “normally.” For instance, it seems odd that Norway imposes a flat obligation to retain data on 300 providers with only a 5 % market share, while large institutions such as universities, or operators such as airports, do not have this duty.

Secondly, there is the problems associated with NAT and Carrier Grade NAT technology. Both are solutions allowing several users to share and IP-address simultaneously. It is not clear whether it is the technological solution, the level in the

communication chain where it is applied, or other considerations that are at play when determining the scope of the obligation to retain data. Thirdly, the proportionality assessment each country must perform, may be influenced by circumstances special to that country, such as the threat assessment and crime statistics.

Looking at the regulation in each country, Denmark, Finland and Sweden have aligned the data retention rules with the rules of secret coercive measures regarding data related to use of electronic communications services *(teleoplysning, teleövervakning, hemlig övervakning av elektronisk kommunikation)*. In each of these countries, the conditions for access to retained data correspond to those applicable to the said coercive measure. The situation in Norway is different, but then again, the scope of the data retention rules is much narrower than for the secret coercive measure *kommunikasjonskontroll.*

Finally, the regulation on national level is often quite complicated and abstract. It seems doubtful that to integrate rules of data retention as part of the of e-com regulation is the most suitable approach given the discrepancy between the *purpose* of electronic communication regulation and the *mandate* of the police, in addition to the widely different terminologies used in the respective fields of the law. While the regulatory field is quite complicated in itself, it adds to the opacity of the law that the principle of technology neutrality is applied to make the law as resilient as possible to technological change. This is a valid consideration, but at some point the cost to the foreseeability of the law may be too high. National data retention law is free to specify the providers and data subjects in more detail, which could be a way to achieve greater legal certainty and make the rules more easily comprehensible.

About this publication

Data Retention Law in the Nordic Countries

A Comparative Study

Inger Marie Sunde, Professor, Norwegian Police University College (Politihøgskolen)

TemaNord 2024:532

ISBN 978-92-893-8033-1 (PDF)
ISBN 978-92-893-8034-8 (ONLINE)
http://dx.doi.org/10.6027/temanord2024-532

Citation for published version (APA): Sunde, I.M. (2024) *Data Retention Law in the Nordic Countries: A Comparative Study.* The Nordic Council of Ministers. TemaNord 2024:532

Cover photo: Unsplash, in collaboration with Getty Images
Published: 5/9/2024

Disclaimer

This publication was funded by the Nordic Council of Ministers. However, the content does not necessarily reflect the Nordic Council of Ministers' views, opinions, attitudes or recommendations.

Rights and permissions

Nordic co-operation

Nordic co-operation is one of the world's most extensive forms of regional collaboration, involving Denmark, Finland, Iceland, Norway, Sweden, and the Faroe Islands, Greenland and Åland.

Nordic co-operation has firm traditions in politics, economics and culture and plays an important role in European and international forums. The Nordic community strives for a strong Nordic Region in a strong Europe.

Nordic co-operation promotes regional interests and values in a global world. The values shared by the Nordic countries help make the region one of the most innovative and competitive in the world.

The Nordic Council of Ministers
Nordens Hus
Ved Stranden 18
DK-1061 Copenhagen
pub@norden.org

Read more Nordic publications on www.norden.org/publications