The Danish Intelligence Oversight Board

Annual Report 2018

Danish Centre for Cyber Security (CFCS)

Contents

To the Minister of Defence

The Danish Intelligence Oversight Board hereby submits its report on its activities concerning the Centre for Cyber Security for 2018 in accordance with section 24 of the Danish Centre for Cyber Security Act (Act No. 713 of 25 June 2014, as amended (most recently by Act No. 555 of 7 May 2019)). The report must be published.

Copenhagen, June 2019

Michael Kistrup

Chairman of the Danish Intelligence Oversight Board

Foreword

The Danish Intelligence Oversight Board is a special independent monitoring body, which among other things oversees that the Centre for Cyber Security (*CFCS*) processes information about natural persons in compliance with CFCS legislation. The Oversight Board was set up under the Danish Security and Intelligence Service (*DSIS*) Act (*lov om Politiets Efterretningstjeneste (PET)*), which entered into force on 1 January 2014.

The aim of this annual report is to inform about the nature of the oversight activities performed with regard to CFCS. The report also provides information about the aspects which the Oversight Board has decided to examine more closely in 2018 as well as the number of instances where CFCS's processing of personal information has been found by the Oversight Board to be in violation of CFCS legislation. Furthermore, , where relevant, the report includes a follow-up on the Oversight Board's checks in 2016 and 2017.

Like in the preceding years, the Oversight Board has also in 2018 had particular focus on consolidating and strengthening the basis underlying its checks of the Danish Centre for Cyber Security (*CFCS*), the Danish Defence Intelligence Service (*DDIS*) and the Danish Security and Intelligence Service (*DSIS*), including by continuous development of the Oversight Board's risk and materiality assessment of the two intelligence services and CFCS as well as the standards and methods applied in the legal control thereof. It is of crucial importance to the Oversight Board that the individual checks are well-based and documented and that they are organised on the basis of an adequate professional and technical understanding from an intelligence perspective. Furthermore, in 2018, the Oversight Board has initiated various development projects for the purpose of securing more efficient system support for the Oversight Board's oversight activities.

In 2018, the Oversight Board carried out in-depth and intensive compliance checks with regard to CFCS's processing of information about natural persons. Like in the preceding years, the Oversight Board has given priority to checks with special focus on CFCS's compliance with CFCS legislation on interception of communications, on processing of personal information and on analysis, disclosure and erasure of data.

In addition, the Oversight Board has given priority to checking CFCS's compliance with CFCS legislation on security measures (information security) in connection with processing of personal information. While the rules on security measures are a focus area in all of the Oversight Board's checks of CFCS, the implementation of the ISO 27001 standard is addressed in a joint ISO 27001 implementation project for the Danish Defence Intelligence Service (*DDIS*) and CFCS. The results of these checks are described in more detail in the Oversight Board's annual report on its activities concerning the Danish Defence Intelligence Service (*DDIS*) for 2018, section 1.2.12. Finally, the Oversight Board has continued its work to identify and verify CFCS's system landscape at the server and component level.

In 2018, the Oversight Board has broadened the scope of its cooperation with the Dutch Review Committee on the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD)*), the Belgian Standing Intelligence Agencies Review Committee (*Comité permanent de contrôle de services de renseignements et de sécurité (Committee I)*), the Norwegian Parliamentary Intelligence Oversight Committee (the EOS Committee) (*Stortingets Kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget)*) and the Swiss Independent Oversight Authority for Intelligence Activities (OA-IA) (*Unabhängige Aufsichtsbehörde* über *die nachrichtendienstlichen Tätigkeiten (AB-ND)*). The focus of this cooperation is to share experience with respect to oversight methods and to discuss legal subjects of mutual relevance. One of the results of this cooperation is that in November 2018, the five oversight and review bodies published a joint statement on strengthening cooperation between national intelligence oversight bodies. The statement is available on the Oversight Body's website.

Also, in April 2018, the secretariat of the Oversight Board visited the Swedish oversight bodies, the Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden (SIN)*) and the Swedish Defence Intelligence Commission (*Statens inspektion för försvarsunderrättelseverksamheten (SIUN)*), to share experience about various oversight methods.

In addition to the Oversight Board's close cooperation with specific oversight and review bodies, in December 2018 the Oversight Board participated in a joint European conference for oversight and review bodies in Paris, which was attended by 14 European countries.

Michael Kistrup

Chairman of the Danish Intelligence Oversight Board

1 The Oversight Board's oversight activities

1.1 Oversight method

The Oversight Board continuously works to improve the methods it uses in the planning and performance of its oversight of CFCS in order for the oversight to be as effective as possible within the framework set for its work.

The Oversight Board's oversight activities consist of three parts: planning, execution and verification. In addition, the Oversight Board regularly evaluates its work with all three elements.

The Oversight Board's planning of next year's compliance checks is based on an annual risk assessment of all processes and systems at CFCS. The purpose of the risk assessment is to assess the risk of non-compliance with legislation in relation to interception of communications, processing, analysis, disclosure and erasure of information about the groups of persons falling within the Oversight Board's scope of competence. On that basis, the Oversight Board prepares a risk analysis which forms the basis of the selection of the checks to be made in the coming year.

The purpose of the risk analysis is to ensure that the Oversight Board's oversight activities are focused on the areas with the highest risk of errors and that other relevant factors are taken into account, e.g. areas where the Oversight Board's oversight activities are given special weight by politicians. Areas that are deemed to have a low risk of errors are generally checked once every third year in order to achieve completeness in the oversight of CFCS and ensure that the assessment of the risk of errors in the area still holds. Furthermore, the Oversight Body inspects systems which in connection with the risk assessment are deemed irrelevant to the Oversight Board's checks in order to check whether the relevance assessment is correct.

The Oversight Board's planning of next year's compliance checks is completed at the end of the preceding year in order for the experience gained from this year's checks to be included as part of the risk assessment and analysis.

The actual checks are conducted regularly throughout the year. As a general rule, the individual areas are checked by the secretariat of the Oversight Board. Based on a specific assessment, CFCS is requested to provide clarifying comments. The secretariat will then submit the results of the checks to the Oversight Board for its decision as to whether sufficient information has been obtained in each individual case or whether further details or discussions with CFCS are required.

The Oversight Board uses various methods to check the individual areas, including full checks, random checks, screening of content and interview-based checks. The Oversight Board's choice of method is based on the risk analysis of the area, experience from previous checks and the

Oversight Board's findings in connection with the checks. Furthermore, prior to checking an area not previously checked, the Oversight Board holds a start-up meeting with relevant CFCS employees in order to ensure an adequate technical understanding of the area that will allow for the checks to be adjusted and adequately performed.

The Oversight Board's direct access to CFCS's systems prevents CFCS from predicting which data and files will be subjected to checks by the Oversight Board. However, the Oversight Board may sometimes have to notify CFCS about the time and method of a check if, for example, the Oversight Board needs access to specific physical premises or needs to interview specific employees.

Prior to initiating its checks for a particular year, the Oversight Board will share its risk analysis and oversight plan with CFCS for the purpose of ensuring, among other things, openness about the Oversight Board's assessment of the situation at CFCS. The openness also allows CFCS to take into account the Oversight Board's checks in the organisation of its own internal controls, which contributes to the Oversight Board's checks and the internal controls collectively covering a larger part of CFCS's activities. Finally, the openness allows CFCS to dedicate sufficient resources to service the Oversight Board.

The Oversight Board performs verification by continuously mapping CFCS's system landscape at the server, component and application level in order to be able to make a complete risk assessment of all processes and systems of CFCS. Each year, the Oversight Board dedicates substantial resources to verify the data received from CFCS on its system landscape. The purpose of the verification is to ensure that the Oversight Board's checks are based on data from CFCS the correctness of which has been verified by the Oversight Board.

The Oversight Board's direct access to CFCS's systems prevents CFCS from predicting which data and files will be subjected to checks by the Oversight Board. However, the Oversight Board may sometimes have to notify CFCS about the time and method of a check if, for example, the Oversight Board needs access to specific physical premises or needs to interview specific employees.

1.2 Oversight of CFCS in 2018

For the purpose of overseeing CFCS's compliance with the provisions of the CFCS Act when processing information about natural persons, the Oversight Board has carried out checks in 2018 of CFCS's:

- use of analytical tools (1.2.1),
- processing of information in relation to submitted media (1.2.2),
- disclosure of information to other public authorities, private businesses and partners (1.2.3),
- sharing of information with other parts of the Danish Defence Intelligence Service (*DDIS*) (1.2.4),
- work stations (1.2.5), and
- internal controls (1.2.6).

Summary of the Oversight Board's checks in 2018

The Oversight Board's checks concerning CFCS's compliance with the provisions on interception of communications, processing of personal information, analysis, disclosure and erasure of data verified, see sections 1.2.1-1.2.3 and 1.2.5, CFCS's general compliance with the legislation in this regard.

However, the Oversight Board's checks concerning CFCS's processing of information in relation to submitted media showed, see section 1.2.2, that at the time of the Oversight Board's first inspection, CFCS was not in compliance with the requirements under section 18(1) of the CFCS Act concerning security measures. The check also showed that CFCS's internal guidelines contained procedures that were not in accordance with the provisions of the CFCS Act. At the time of the Oversight Board's second inspection, however, CFCS had implemented various measures to ensure that the processing of information in relation to submitted media was in accordance with the provisions of section 18(1) of the CFCS Act, and CFCS had also revised its internal guidelines for the processing of submitted media.

The Oversight Board's check concerning CFCS's sharing with other parts of the Danish Defence Intelligence Service (*DDIS*) of data containing personal information obtained by interception of communications, see section 1.2.4, verified CFCS's compliance with the relevant provisions of the guidelines issued by the Danish Ministry of Defence concerning processing of data in and from the CFCS Network Security Service (the "CFCS Guidelines"), but in one instance no legal approval had been obtained in advance, as prescribed by CFCS's internal guidelines. On the basis of the check, the Oversight Board encouraged CFCS to ensure uniform documentation and registration of CFCS's sharing of data, including in order to perform efficient checks thereof.

The check of CFCS's internal controls showed, see section 1.2.6, that CFCS's internal controls in 2018 – as announced in 2016 and 2017 – were not planned on the basis of a documented risk and materiality assessment approved by management. In light of CFCS's failure to report on its internal controls in 2018, the Oversight Board has been unable to assess on the basis of the information available at the time of completion of the check whether CFCS's internal controls in 2018 were satisfactory. However, the Oversight Board has noted that CFCS subsequently submitted a documented risk and materiality assessment approved by management as well as a report on internal controls performed in 2018.

1.2.1 Checks of CFCS's use of analytical tools

CFCS uses various analytical tools in connection with analysing data from its sensor network and from media that are submitted to CFCS. CFCS's analysis is continuously adapted to the threats that CFCS learns about in connection with its activities, and the analytical tools that are relevant to use therefore constantly change.

For the purpose of its compliance check in this regard, in 2018 the Oversight Board had regular discussions with CFCS about its use of analytical tools.

! **Comments by the Oversight Board**

Based on CFCS's report, the Oversight Board has completed its check of analytical tools in 2018 and initiated further checks of the area in 2019.

1.2.2 Checks of CFCS's processing of information in relation to submitted media

CFCS regularly receives media such as computers, hard disks, mobile telephones, etc. from CFCS's customers, the Danish Security and Intelligence Service (*DSIS*), other private businesses and private individuals for technical analysis, including in case of suspected compromise. Furthermore, CFCS procures media in connection with on-site assistance to customers by collecting data, including images of computers, partitions and log files.

For the purpose of its compliance check of CFCS's processing of information in relation to submitted media, in 2018 the Oversight Board carried out two inspections at CFCS where the Oversight Board drew random samples from the information held by CFCS, examined CFCS's documentation and interviewed key employees.

! **Comments by the Oversight Board**

The Oversight Board's checks of CFCS's processing of information in relation to submitted media showed that at the time of the Oversight Board's first inspection, CFCS was not in compliance with the requirements under section 18(1) of the CFCS Act concerning security measures. The check also showed that CFCS's internal guidelines contained procedures that were not in accordance with the provisions of the CFCS Act.

However, the Oversight Board notes that at the time of the Oversight Board's second inspection, CFCS had implemented various measures to ensure that the processing of information in relation to submitted media was in accordance with the provisions of section 18(1) of the CFCS Act, including that CFCS had revised its internal guidelines for the processing of submitted media.

1.2.3 Checks of CFCS's disclosure of information

In 2018, the Oversight Board performed regular checks of CFCS's disclosure of data containing personal information to other public authorities, private businesses and foreign partners, focusing on CFCS's compliance with sections 10 and 16 of the CFCS Act and the CFCS Guidelines.

! **Comments by the Oversight Board**
The Oversight Board's check of CFCS's disclosure of data containing personal information to other public authorities, private businesses and partners verified CFCS's compliance in all cases with the provisions of the CFCS Act in this regard.

1.2.4 Checks of CFCS's sharing of information with other parts of the Danish Defence Intelligence Service (*DDIS*)

In 2018, the Oversight Board performed a check concerning CFCS's sharing with other parts of the Danish Defence Intelligence Service (*DDIS*) of data containing personal information obtained by interception of communications, focusing on CFCS's compliance with the provisions of the CFCS Guidelines in this regard.

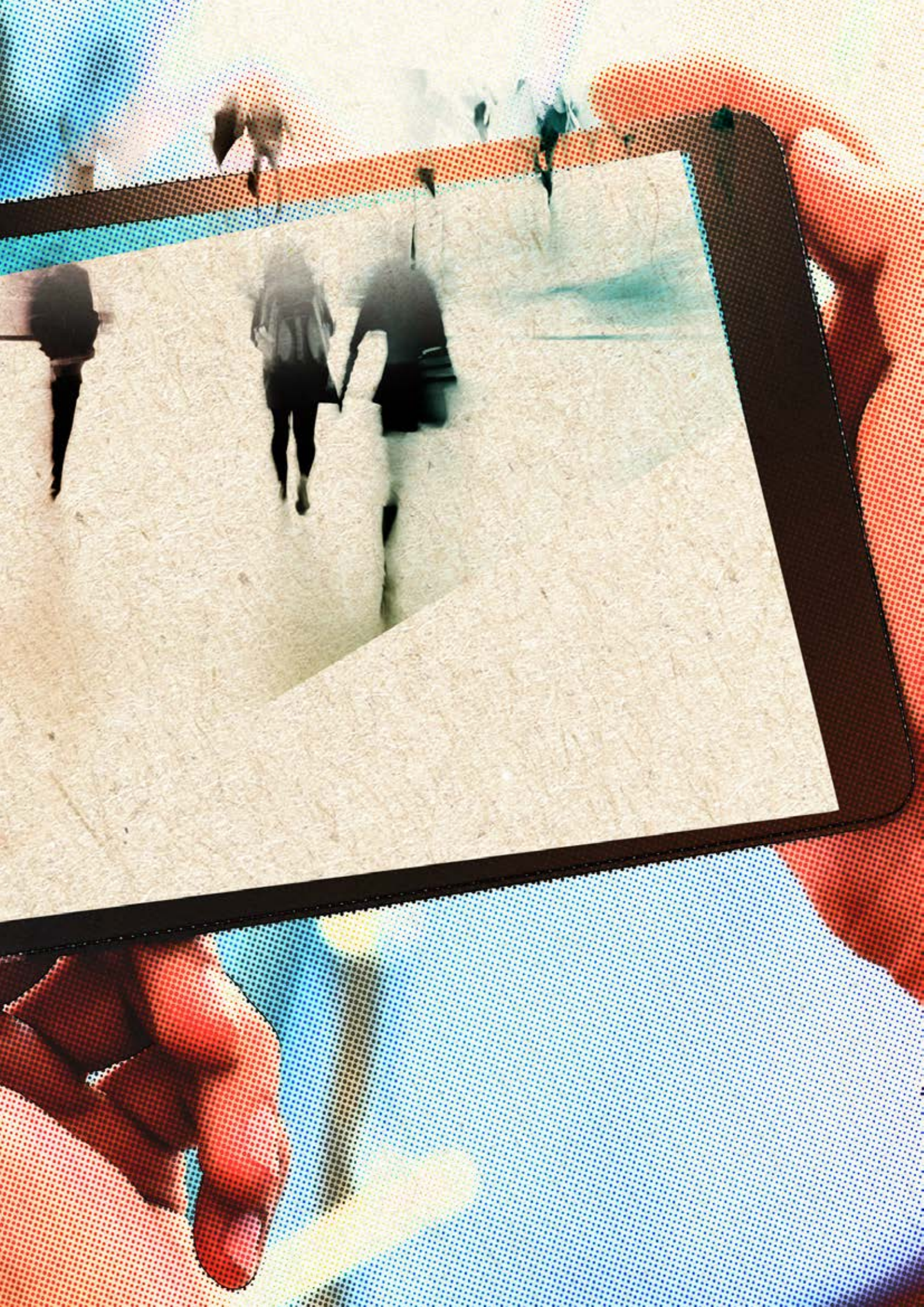
The Oversight Board is continuously notified by CFCS of its sharing with other parts of DDIS of data obtained by interception of communications. As regards 2018, the Oversight Board has received a total of 24 notifications in the form of completed data sharing forms. The details provided in the forms did not give rise to any questions from the Oversight Board to CFCS.

As a supplement to the check of the data sharing forms, the Oversight Board regularly performed random checks of CFCS's electronic incident management system in order to determine if the data shared were relevant in each case.

! **Comments by the Oversight Board**
The Oversight Board's check of CFCS's sharing with other parts of the Danish Defence Intelligence Service (*DDIS*) of data containing personal information obtained by interception of communications verified CFCS's compliance with the relevant provisions of the CFCS Guidelines, but that in one instance no legal approval had been obtained in advance, as prescribed by CFCS's internal guidelines.

On the basis of the check, the Oversight Board encouraged CFCS to ensure uniform documentation and registration of CFCS's sharing of data, including in order to perform efficient checks thereof.

> The Oversight Board's checks of CFCS's processing of information in relation to submitted media showed that at the time of the Oversight Board's first inspection, CFCS was not in compliance with the requirements under section 18(1) of the CFCS Act concerning security measures. The check also showed that CFCS's internal guidelines contained procedures that were not in accordance with the provisions of the CFCS Act.



1.2.5 Checks of CFCS work stations

In 2018, the Oversight Board performed a check of a number of staff work stations, focusing on the staff's processing of information about natural persons, including their knowledge of the rules in this area.

The Oversight Board checked a number of randomly chosen work stations, including their drives, email systems, external storage devices and documents in hard copy. In connection with the check performed of the information held on each of the work stations, the Oversight Board asked questions to the individual staff members in question about their knowledge of the rules on processing, including erasure, of information about natural persons.

! **Comments by the Oversight Board**

The Oversight Board's check of specific work stations verified all staff members' compliance with the CFCS Act in their processing of information about natural persons and their general awareness that the processing of such information must comply with the Act and CFCS's internal guidelines.

1.2.6 Checks of CFCS's internal controls

In the course of its oversight of CFCS in 2018, the Oversight Board performed a check of CFCS's internal controls. The check comprised all internal controls carried out by CFCS in 2018 and CFCS's planning of the same for 2019, and was carried out by reviewing documentation provided and engaging in discussions with CFCS

The Oversight Board performed similar checks of CFCS's internal controls in 2016 and 2017. The checks showed that CFCS's internal controls were not planned on the basis of a documented risk and materiality assessment. On this basis, the Oversight Board informed CFCS in 2016 and 2017 that it should plan its internal controls on the basis of an annual risk and materiality assessment.

At the time of completion of the check, the Oversight Board had not received reports on the internal controls nor had the Oversight Board received a documented risk and materiality assessment approved by management. However, in 2019, CFCS has submitted a status report on the internal controls performed in 2018.

! **Comments by the Oversight Board**

The Oversight Board finds it unacceptable that CFCS's internal controls – as announced in 2016 and 2017 – were not planned on the basis of a documented risk and materiality assessment approved by management.

In light of CFCS's failure to report on its internal controls in 2018, the Oversight Board has been unable to assess on the basis of the information available at the time of completion of the check whether CFCS's internal controls in 2018 were satisfactory.

However, the Oversight Board has noted that CFCS subsequently submitted a documented risk and materiality assessment approved by management as well as a report on internal controls performed in 2018.

2

Examples of CFCS's handling of cyber attacks

According to the legislative history of the CFCS Act, the annual report of the Oversight Board on its activities concerning CFCS must include a fully depersonalised description of one or more specific cyber attacks.

CFCS has provided the following description of cyber attacks in 2018:

The CFCS Network Security Service is tasked with detecting, analysing and contributing to preventing IT security incidents at the public authorities and private businesses forming part of the sensor network. This process is targeted primarily on the most sophisticated attacks that are usually carried out by government-backed groups.

The work of the CFCS Network Security Service is planned in close cooperation with CFCS's Cyber Situation Centre which, in addition to the connected organisations, also has particular focus on analysing and informing about current cyber attacks that impact on Danish critical infrastructure, including the six nationally critical sectors in Denmark.

In 2018, the CFCS Network Security Service and the Cyber Situation Centre have addressed a number of IT security incidents, the major part of which were dominated by various kinds of social engineering, including attacks via email in the form of phishing, and which are still considered a serious threat against the organisations connected with CFCS.

In addition to social engineering, a large number of reconnaissance attempts are generally observed against the organisations connected with CFCS where the attacker tries to gain knowledge about the IT systems of potential victims which may be used in subsequent attacks. Such knowledge may, for example, be obtained by the attackers scanning the internet-based services of the organisations.

Other examples include numerous cases where attackers successfully exploited the vulnerabilities in the software of organisations to infect the systems with malware. These cases included concrete examples of so-called coin-miner infections that exploit the calculating power of the infected machine to generate a virtual currency on behalf of the attacker.

Moreover, a number of brute force-related attempted attacks were observed against various organisations connected with CFCS. The attackers tried to force their way into the IT systems of organisations via a number of automated login requests against specific software services of theirs. However, in these specific cases the attackers were not successful in their attempts to access the systems.

3 Statistical data on CFCS's processing of information

As can be seen from the legislative history of the CFCS Act, the Oversight Board's annual report must provide statistical data on CFCS's processing of personal information, including data on the number of complaints received by CFCS as well as by the Oversight Board, data on the number of subject access requests received and their status (granted/refused) as well as data on the number of cases involving security incidents dealt with by CFCS.

The annual report must also provide statistical data on the number of cases where a CFCS analyst carried out an analysis of data obtained by interception of communications. These statistics must contain an overall categorisation of the severity of the incidents.

CFCS has provided the following data for 2018:

Table 1 Complaints received concerning CFCS's processing of personal information

Categories	2018
Complaints received by CFCS	0
Complaints received by the Oversight Board	0

Table 2 Subject access requests

Categories	2018
Full access requested	1
Partial access requested	0
Requests refused	7
No documents located to grant or refuse access	2
Total	**10**

Table 3 Security incidents* according to severity

Categories	2018
Serious cyber attacks	0
Major cyber attacks	1
Moderate cyber attacks	12
Minor cyber attacks	159
None**	740
Total	**912**

* Security incidents are defined in accordance with section 2(i) of the CFCS Act.

** The category has been renamed from "False positive" to "None" as a false positive incident has not impacted on the customer and did thus not give a true picture of this category. By naming this category "None" a more precise category is obtained as it will also include all of the security incidents that have not impacted on the customer.

In addition, CFCS has provided the following information about the number of cases where CFCS disclosed data to other public authorities, private companies and partners, including personal data, obtained by interception of communications, and the number of cases where CFCS shared similar data with other parts of the Danish Defence Intelligence Service (*DDIS*):

Table 4 CFCS's disclosure and sharing of data**

Categories	2018
Disclosure of data	109
Sharing of data	24

* The figures representing the number of instances where the CFCS Network Security Service has disclosed information, including information obtained by interception of communications, include all disclosed information, including about natural and legal persons as well as non-identifiable information. See also the Oversight Board's oversight activities in this regard, see section 1.2.3.

4 Publicity in 2018

CFCS's activities and the framework for such activities set by the Danish Parliament and Government, including the Oversight Board's oversight, have been the subject of regular comment by the Danish media.

The Oversight Board would like to contribute as much as possible to the press and thus the public getting the best possible insight into the Oversight Board's oversight of CFCS without compromising the need for secrecy following from CFCS's special function.

The Oversight Board makes sure that it is updated on the public debate about its oversight of CFCS in order to assess whether it can contribute to a better understanding of its role, oversight options as well as the results of its oversight.

1. About the Centre for Cyber Security

The Centre for Cyber Security ("*CFCS*") was established in 2012 as part of the Danish Defence Intelligence Service (*DDIS*) with the main responsibility of acting as:

- governmental and military cyber security alert service,
- national IT security authority (except for the areas under the Danish Ministry of Justice where this authority lies with the Danish Security and Intelligence Service (*DSIS*)), and
- cyber security and emergency response authority in telecommunications.

The responsibility of CFCS as the governmental and military cyber security alert service is to assist in securing a high level of cyber security in the information and communication technology infrastructure on which nationally important functions depend. In this connection, CFCS's cyber security service is responsible for detecting, analysing and contributing to preventing advanced cyber security attacks against the Danish military as well as government authorities and businesses which form part of CFCS's sensor network.

CFCS's task as the national IT security authority means that it must inform, guide and advise Danish authorities and businesses on cyber security and act as a national centre of competence within the area of cyber security. As the national IT security authority, CFCS is also tasked with security vetting and overseeing classified products, systems and installations within information and communications technology.

CFCS's responsibility for carrying out the function as the cyber security and emergency response authority in the area of telecommunications means, among other things, that CFCS oversees the area and advises the players in emergency response area in Denmark on telecommunications emergency responses. Further, by virtue of the powers vested in it under the Danish Network and Information Security Act (the "NIS Act"), CFCS issues executive orders and is tasked with overseeing the area and at a general level to coordinate the handling of special threats which may affect cyber security in the telecommunications sector.

On 1 July 2014, Consolidated Act No. 713 of 26 June 2014 on the Centre for Cyber Security (the "CFCS Act") entered into force. The Act strengthens CFCS's powers with regard to protecting Denmark from cyber attacks. CFCS's powers have been strengthened, among other things, by an extension of its mandate to investigate security incidents, including cyber attacks, in cooperation with public authorities and private businesses so as to enable CFCS to a larger degree than before to collect the information necessary to determine the tools and methods of attack which were employed in the security incidents. The Act also means that a number of the central data protection principles also apply to CFCS's activities.

With the Act, it is further established that the Oversight Board – which is an independent monitoring body charged with overseeing that the Danish Security and Intelligence Service (*DSIS*) processes personal information in compliance with DSIS legislation and that the Danish Defence Intelligence Service (*DDIS*) processes information about natural and legal persons resident in Denmark in compliance with the legislation regarding the Danish Defence Intelligence Service (*DDIS*) – is also charged with overseeing that CFCS processes information about natural persons in compliance with CFCS legislation.

> The responsibility of CFCS as the governmental and military cyber security alert service is to assist in securing a high level of cyber security in the information and communication technology infrastructure on which nationally important functions depend. In this connection, CFCS's cyber security service is responsible for detecting, analysing and contributing to preventing advanced cyber security attacks against the Danish military as well as government authorities and businesses which form part of CFCS's sensor network.

2. The Danish Intelligence Oversight Board

The Oversight Board is a special independent monitoring body charged with overseeing that the Danish Security and Intelligence Service (*DSIS*), the Danish Defence Intelligence Service (*DDIS*) and the Danish Centre for Cyber Security (*CFCS*) process personal information in compliance with the legislation.

The Oversight Board is completely autonomous and is thus not subject to the directions of the Ministry of Defence or any other administrative authority with respect to the performance of its activities.

The Oversight Board is composed of five members who are appointed by the Minister of Justice following consultation with the Minister of Defence. The chairman, who must be a High Court judge, is appointed on the recommendation of the Presidents of the Danish Eastern and Western High Courts, while the remaining four members are appointed following consultation with the Parliamentary Intelligence Services Committee.

The members are:

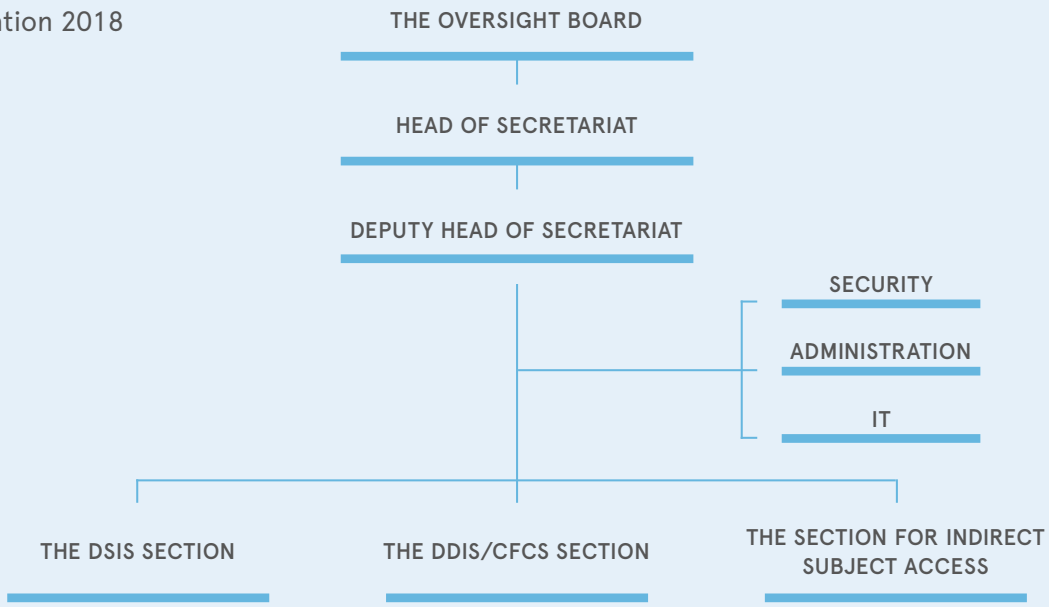
- Michael Kistrup, High Court Judge, the Danish Eastern High Court (chairman)
- Professor Jørgen Grønnegård Christensen, Aarhus University
- Erik Jacobsen, Chairman of the Board of Directors, Roskilde University
- Pernille Christensen, Legal Chief, Local Government Denmark
- Professor Henrik Udsen, Copenhagen University

The members are appointed for a term of four years each, and all members are eligible for reappointment for an additional term of four years. When the Oversight Board was set up in October 2014, two of its members were appointed for a term of two years and they were eligible for reappointment for an additional term of four years for the purpose of preventing a situation where all members were to be replaced at the same time, as the subsequent terms are staggered by two years.

The Oversight Board is supported by a secretariat which is subject solely to the instructions from the Oversight Board in the performance of its duties. The Oversight Board recruits its own secretariat staff and also decides which educational and other qualifications the relevant candidates must have. At the end of 2018, the secretariat consisted of a head of secretariat, who is in charge of the day-to-day management of the secretariat, a deputy, three lawyers, an IT consultant and an administrative employee.

The secretariat is divided into departments which are concerned with DSIS, DDIS/CFCS and indirect subject access requests. In order to ensure subject-matter coordination and experience sharing, the Oversight Board's staff works across the departments.

Organisation 2018



2.1 The Oversight Board's duties in relation to CFCS

The CFCS Act provides that upon receipt of a complaint or of its own motion, the Oversight Board must oversee CFCS's compliance with the relevant provisions of the CFCS Act and the statutory regulations issued thereunder in its processing of information about natural persons. The Oversight Board oversees CFCS's compliance with the provisions of the Act concerning:

- interception of communications,
- processing of personal information in CFCS,
- analysis, disclosure and erasure of data, and
- the requirements to security measures in connection with CFCS's processing of personal information.

The Oversight Board must oversee by way of compliance checks that CFCS processes information about natural persons in compliance with CFCS legislation, and the Oversight Board thus has no mandate to oversee whether CFCS carries out its activities in an appropriate manner.

The Oversight Board itself decides the intensity of oversight, including whether to perform full oversight or random checks, which aspects of the activities are to be given special priority and the extent to which the Oversight Board wishes to raise a matter of its own motion. No specific guidelines have been provided for the Oversight Board's performance of its oversight functions.

2.2 The Oversight Board's access to information held by CFCS

The Oversight Board may require CFCS to provide any information and material of importance to the Oversight Board's activities, and the Oversight Board is entitled at any time to access any

premises where the information being processed may be accessed or where technical facilities are being used. The Oversight Board may furthermore require CFCS to provide written statements on factual and legal matters of importance to the Oversight Board's oversight activities and request the presence of a CFCS representative to give an account of current processing activities.

CFCS has made office premises available to the Oversight Board for the Oversight Board to make its own searches in CFCS's IT systems.

2.3 Responses available to the Oversight Board

The Oversight Board has no authority to order CFCS to implement specific measures in relation to data processing. However, the Oversight Board may issue statements to CFCS providing its opinion on matters such as whether CFCS complies with the rules on processing of personal information. If CFCS decides not to comply with a recommendation issued by the Oversight Board in exceptional cases, CFCS must notify the Oversight Board and immediately submit the matter to the Minister of Defence for a decision.

The Oversight Board must inform the Minister of Defence of any matters which the Minister ought to know in the opinion of the Oversight Board.

Each year, the Oversight Board submits a report on its activities to the Minister of Defence. The report, which is also made available to the public, provides general information about the nature of the oversight activities performed with regard to CFCS. According to the legislative history of the Act, the aim of the annual report is to provide general information about the nature of the oversight activities performed with regard to CFCS, including a general description of the aspects having attracted the Oversight Board's interest. The reports must provide statistical data on CFCS's processing of personal information, including data on the number of complaints received by CFCS as well as by the Oversight Board, data on the number of subject access requests and their status (granted/refused) as well as data on the number of cases involving security incidents that have been dealt with by CFCS. The Oversight Board must also provide data on the number of instances where personal information has been found by the Oversight Board to be processed by CFCS in violation of CFCS legislation. The report must also contain a fully depersonalised description of one or more specific cyber-attacks as well as statistical data on the number of instances where a CFCS analyst carried out an analysis of data obtained by interception of communications. The statistics must also contain an overall categorisation of the severity of the incidents.

The Oversight Board issued its most recent annual report on its activities to the Minister of Defence in May 2018. The annual report was published in June 2018.

> The Oversight Board must oversee by way of compliance checks that CFCS processes information about natural persons in compliance with CFCS legislation, and the Oversight Board thus has no mandate to oversee whether CFCS carries out its activities in an appropriate manner.

3. Legal Framework

1) Consolidated Act No. 713 of 25 June 2014 on the Centre for Cyber Security (*CFCS*) (the "CFCS Act"), as amended (most recently by Act No. 443 of 8 May 2018).

2) Guidelines issued by the Danish Ministry of Defence concerning processing of data in and from the CFCS Network Security Service (the "CFCS Guidelines"), issued on 30 June 2014.

3.1 About the CFCS Network Security Service, see section 3 of the CFCS Act

According to section 3 of the CFCS Act, the CFCS Network Security Service is charged with detecting, analysing and contributing to preventing security incidents in public authorities under the Danish Ministry of Defence as well as in other public authorities and private businesses which are members of the Network Security Service. Membership is available to supreme government bodies and public authorities on request, while membership is available on request for regions and municipalities as well as private businesses performing nationally important functions provided that CFCS decides in each individual case that membership may contribute to maintaining a high level of national cyber security.

The CFCS Network Security Service is the name of CFCS's total activities in connection with detecting, analysing and contributing to preventing security incidents, including the CERT activities in the civil area (GovCERT), the CERT activities in the military area (MILCERT), security technical activities (e.g. malware analysis) and support functions. In the same way as before, when public authorities and private businesses become a member of the Network Security Service, the parties will conclude a membership agreement to govern the details of the relationship between the Network Security Service and the individual member. The public authorities under the Danish Ministry of Defence will be ordered by the military IT security authority to join the Network Security Service, and for those members no membership agreement will be concluded.

The security services provided to public authorities and private businesses having joined the Network Security Service are tailored to the needs of the individual members. By way of example, the services may include monitoring of the access point of the member to the Internet in order for the Network Security Service to detect and analyse security incidents, e.g. by way of a locally placed alarm device. Against that background – and against the background of similar analyses conducted for the other members – the Network Security Service may alert the member to any security incidents detected and also send out more general warnings. Furthermore, members may receive warnings based on information received by CFCS from the foreign section of the

Danish Defence Intelligence Service (*DDIS*), other network security services and other foreign partners. The Network Security Service will also advise members on cyber security and provide assistance if one of the members is the target of a serious security incident.

3.2 About interception of communications, see sections 4-7 of the CFCS Act

Under the provisions of sections 4 and 5 of the CFCS Act, which are identical in terms of contents, the CFCS Network Security Service is entitled without a court order to process content data and intercept related information derived from the networks of its members and from public authorities under the Danish Ministry of Defence with a view to maintaining a high level of national cyber security. *Content data* means the contents of communications which are transmitted through digital networks or services, see section 2(ii) of the Act, and *intercept related information* means data which are processed for the purpose of transmitting content data, see section 2(iii) of the Act.

The regulation of the Network Security Service's power to intercept communications in the civil and military areas is divided into two provisions as there are some areas where special rules apply in the military area in order to thereby ensure that no restrictions are imposed in relation to the monitoring that MILCERT was previously allowed to carry out. In the areas under the Danish Ministry of Defence where classified information is subject to significant processing, there will thus still be a need for greater power to analyse monitored data and to disclose data to relevant partners.

According to section 6 of the Act, a public authority or private business which is not a member of the CFCS Network Security Service may become a *temporary member of the Network Security Service* on reasonable suspicion of a security incident, and the Network Security Service will then be entitled without a court order to process content data and intercept related information derived from networks in the public authority or private business where:

(i) the public authority or private business has submitted a request to CFCS for temporary membership and given its written consent to the processing,
(ii) the processing is deemed to contribute significantly to CFCS's effort to secure the information communication technology infrastructure on which nationally important functions depend, and
(iii) the temporary membership is for a maximum period of two months.

Temporary membership may be available to public authorities and private businesses which are not usually the target of a threat scenario that is sufficiently serious to render a regular membership of the Network Security Service advisable, but which due to current events are the target of a threat scenario for a short period of time which is sufficiently tangible to require the extra security provided by membership. Temporary membership may also be available if private businesses which do not perform nationally important functions are the target of particularly serious cyber attacks.

On reasonable suspicion of a security incident, the Network Security Service is entitled under section 7 of the Act without a court order to *process data* contained in or derived from an information system used by a public authority or a private business where:

(i) the public authority or private business has requested assistance from CFCS, made the information system or its data available to the Network Security Service, and given its written consent for the Network Security Service to process the data, and
(ii) the processing is deemed to contribute significantly to CFCS's effort to secure the information communication technology infrastructure on which nationally important functions depend.

3.3 About processing of personal information, see sections 9-14 of the CFCS Act

Under section 9 of the CFCS Act, CFCS's collection of personal information must be for specified, explicit and legitimate purposes, and any subsequent processing must not be incompatible with those purposes. Subsequent processing of personal information which is made only for historical, statistical or scientific purposes will not be deemed to be incompatible with the purposes for which the personal information is collected. Any personal information to be processed must be adequate, relevant and not excessive in relation to the purposes for which the information is collected and the purposes for which the information is to be processed.

Under section 10 of the CFCS Act, processing of personal information may take place only if:

(i) the data subject has given his or her explicit consent,
(ii) the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the data subject's request prior to the conclusion of such a contract,
(iii) the processing is necessary for the performance of a task carried out in the public interest,
(iv) the processing is necessary to protect important aspects of national security or defence policy,
(v) the processing is necessary for the performance of a task carried out in the exercise of official authority vested in CFCS or a third party to whom the data are disclosed,
(vi) the processing is necessary to safeguard legitimate interests pursued by CFCS or by the third party to whom the data are disclosed, and these interests are not overridden by the interests of the data subject, or
(vii) the processing concerns personal information falling within the scope of Part 4 (interception of communications).

If linguistically adjusted, paras (i), (ii), (iii), (v) and (vi) of the provision are identical to the corresponding provisions in article 6 of Regulation (EU) 2016/679 of the European Parliament and of the Council and must be interpreted in accordance with the legislative history of those provisions and relevant administrative practice. For para. (iv) to be applicable, there must be a risk of national security or defence policy being compromised, which may be the case in connection with cyber attacks against the information systems of Danish public authorities. The important aspects of national security and defence policy must be interpreted in accordance with the corresponding expression in section 31 of the Danish Freedom of Information Act (*offentlighedsloven*). Para. (vii) of the provision establishes the general statutory basis for the processing of personal information if the information falls within Part 4 (interception of communications), in which connection it is noted that section 15 of the Act establishes a framework for the analysis of content data (*pakkedata*) falling within the scope of sections 4, 6 and 7 of the Act, while section 17 of the Act establishes a set of rules to govern the erasure of such data.

No processing may take place if the personal information concerns racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or personal information concerning health or sex life, see section 11(1) of the Act. Under subsection (2), however, this does not apply where:

(i) the data subject has given his or her explicit consent to such information being processed,
(ii) the processing concerns personal information which has been made public by the data subject,
(iii) the processing is necessary to establish, enforce or defend a legal claim,
(iv) the processing is necessary to protect important aspects of national security or defence policy, or
(v) the processing concerns personal information falling within the scope of Part 4 (interception of communications).

According to section 12(1) of the Act, no processing may take place if the personal information concerns criminal offences, serious social problems and purely private matters other than those mentioned in section 11(1), unless such processing is necessary for the performance of CFCS's responsibilities. Under subsection (2) of section 12, the personal information mentioned in subsection (1) may not be disclosed to any third party, unless:

(i) the data subject has given his or her explicit consent to such disclosure,
(ii) the disclosure takes place for the purpose of pursuing private or public interests which clearly override the interests of secrecy, including the interests of the data subject,
(iii) the disclosure is necessary for the performance of the activities of a public authority or required for a decision to be made by that authority,
(iv) the disclosure is necessary for the performance of tasks for an official authority by a person or a company, or
(v) the disclosure includes personal information falling within the scope of Part 4 (interception of communications).

The processing of information must be organised in a way which ensures the required updating of the information, see section 13 of the Act. Furthermore, the necessary checks must be made to ensure that no inaccurate or misleading information is processed. Personal information which turns out to be inaccurate or misleading must be erased or corrected without delay.

The personal information collected may not be held in identifiable form longer than necessary to fulfil the purposes for which the information is processed, see section 14 of the Act. In this connection it should be noted that section 17 of the Act contains special provisions on erasure of data falling within the scope of Part 4 of the Act (interception of communications).

3.4 About analysis, disclosure and erasure of data, see sections 15-17 of the CFCS Act and articles 2 and 4-6 of the CFCS Guidelines

According to section 15 of the Act, *analysis of content data* falling within the scope of sections 4, 6 and 7 of the Act (interception of communications) may take place only on reasonable suspicion of a security incident and only to the extent necessary to clarify the circumstances of the incident. The provision establishes the framework for the power of the CFCS Network Security Service to analyse content data falling within the scope of the provisions mentioned.

As part of the operation of the Network Security Service, data from the members' network communications are subjected to fully automated processing at regular intervals for the purpose of identifying possible security incidents. The provision means that the security analysts of the Network Security Service are only allowed to analyse content data on reasonable suspicion of a security incident and only to the extent necessary to clarify the circumstances of the incident.

The activities of the Network Security Service in the military area, see section 5 of the Act, fall outside the scope of section 15 of the Act, but are governed by administrative guidelines. Under article 4.1 of the CFCS Guidelines, analysis of content data derived from the networks of the public authorities under the Danish Ministry of Defence, see section 5 of the Act, may take place only in the following cases:

(i) On reasonable suspicion of a security incident.
(ii) During the process of the ongoing effort to maintain a high level of cyber security in the areas under the Danish Ministry of Defence, including by monitoring communications to see if they contain classified material.

Under subsection (2) of the provision, the analysis under subsection (1) may take place only to the extent necessary to clarify the circumstances of the incident or maintain a high level of cyber security in the areas under the Danish Ministry of Defence.

Under section 16 of the Act, data falling within the scope of sections 4, 6 and 7 of the Act (interception of communications) may be disclosed only in the following cases:

(i) On reasonable suspicion of a security incident, data may be disclosed to the police.
(ii) On reasonable suspicion of a security incident and if necessary for the performance by the Network Security Service of its responsibilities, intercept related information may be disclosed to Danish public authorities, providers of public electronic communication networks and services, other network security services and private businesses which are covered by sections 4, 6 and 7, as well as to public authorities and private businesses in other contexts in connection with CFCS sending out security warnings.

The provision governs CFCS's power to disclose data which fall within sections 4, 6 and 7 of the Act and are thus processed based on interception of communications. Section 16(i) of the Act ensures that CFCS is allowed to disclose all relevant information to the police in cases where it may be relevant for the police to conduct a criminal investigation. The requirement of reasonable suspicion of a security incident means that CFCS may disclose the data in question only if there are specific indications that a security incident may have taken place or may take place in future.

Section 16(ii) of the Act concerning the disclosure of intercept related information to providers of public electronic communication networks and services and others means that particularly telecoms companies may improve their security systems so as to further strengthen the information communication technology infrastructure on which nationally important functions largely depend, e.g. by the telecoms companies being informed of IP addresses that are used for cyber attacks. One of CFCS's most important preventive activities is to send out security warnings to inform public authorities, private businesses, other network security services, etc. of particularly serious security incidents. The security warnings allow the recipients to strengthen their own measures to prevent attacks (e.g. by blocking traffic from IP addresses that form part of hackers'

attack infrastructure) and investigate if they have been the target of attack (e.g. by analysing log files for e-mails from senders who have attacked other public authorities or private businesses). The provision in para. (ii) therefore enables CFCS to send out security warnings containing intercept related information which may strengthen the recipients' cyber security. Disclosure of intercept related information under para. (ii) requires reasonable suspicion of a security incident, and also requires a specific assessment that the disclosure is necessary for the performance of the tasks of the Network Security Service. If the disclosure involves personal information, the principles of relevance and proportionality, see section 9(2) of the Act, must also be observed so that the disclosure only involves personal information which is relevant and adequate to achieve the purpose of the disclosure in question.

Section 16 of the Act should further be seen in the context of section 12 of the Act, which generally governs CFCS's access to disclose personal information on criminal offences, serious social problems and purely private matters other than those mentioned in section 11(1). Based on experience CFCS has very rarely a need to disclose such personal information, but in connection with serious cyber attacks there may be a need to disclose personal information about criminal offences to the police. Section 12(2)(v) authorises CFCS to disclose such types of personal information if the information falls within Part 4 (interception of communications). The issue of disclosure must then be considered in accordance with section 16 of the Act.

The activities of the Network Security Service in the military area, see section 5 of the Act, fall outside the scope of section 16 of the Act, but are governed by administrative guidelines. Under article 6 of the CFCS Guidelines, data falling within the scope of section 5 of the Act may be disclosed by CFCS only where:

(i) the disclosure is necessary to maintain a high level of cyber security, and
(ii) the disclosure is for specified, explicit and legitimate purposes and each such disclosure must be recorded by CFCS.

It is stated in the general part of the explanatory notes to the Bill concerning sharing of data internally in the Danish Defence Intelligence Service (*DDIS*) that in accordance with general principles of administrative law such sharing of data is not regulated by law.

This means that, as a general rule, the Danish Defence Intelligence Service is free to share data internally, including between CFCS and the other parts of the intelligence service, if necessary to fulfil the responsibilities of the public authority and the purpose is legitimate. This ensures that all of the relevant resources available in the Danish Defence Intelligence Service (*DDIS*) may be deployed swiftly and efficiently in connection with the very large number of cyber attacks against Denmark which are orchestrated from abroad and where the Danish Defence Intelligence Service (*DDIS*) as the foreign intelligence service can contribute with a large amount of valuable information.

In accordance with the above, article 2 of the CFCS Guidelines provides that CFCS is allowed to *share* data falling within the scope of sections 4, 6 and 7 of the Act with other parts of the Danish Defence Intelligence Service (*DDIS*) only:

(i) if the sharing of data is necessary to maintain a high level of cyber security,
(ii) if the sharing of data is for specified, explicit and legitimate purposes, and
(iii) on reasonable suspicion of a security incident,
as each such instance of sharing must be recorded by CFCS.

Similarly, article 5 of the CFCS Guidelines provides that CFCS is allowed to share data falling within the scope of section 5 of the Act with other parts of the Danish Defence Intelligence Service (*DDIS*) only where:

(i) the sharing of data is necessary to maintain a high level of cyber security, and
(ii) the sharing of data is for specified, explicit and legitimate purposes,

as each such instance of sharing must be recorded by CFCS.

According to section 17(1) of the Act, data falling within the scope of Part 4 of the Act (interception of communications) must be erased once the purpose of the processing has been fulfilled. The provision should be seen in the context of Part 14 of the Act, which provides that the personal information collected may generally not be held in identifiable form longer than necessary to fulfil the purposes for which the information is processed. While section 14 of the Act applies to all processing of personal information by CFCS, the special rules in section 17 of the Act only apply to the processing of data obtained by interception of communications. According to the explanatory notes to section 17, a continuous assessment of the processed data will be made based on this provision for the purpose of ensuring that any data that are no longer relevant in relation to the objectives and activities of the Network Security Service will be erased immediately.

According to section 17(2) of the Act, even if the purpose of the processing has not been fulfilled, see subsection (1):

(i) information relating to a security incident must not be held for more than three years, and
(ii) information which does not relate to a security incident must not be held for more than 13 months.

The provision imposes a cap on how long information which has not been erased in accordance with section 17(1) of the Act may be held, and the provision thus applies to information which is still deemed to be in need of processing by the Network Security Service. Even if the purpose of the processing has not yet been fulfilled in those cases, the information must be erased within the absolute time limits laid down in the provision. If information relating to a security incident within the three-year period is found to be used again in connection with a security incident, a new three-year period will begin to run. With regard to the time limits in subsection (2), time begins to run from the date when CFCS records the information in question, see subsection (3).

Section 17(1) and (2) of the Act does not apply to information which has been disclosed in accordance with section 16 of the Act, see section 17(4) of the Act.

3.5 About security measures in connection with CFCS's processing of personal information, see section 18 of the CFCS Act

According to section 18 of the Act, CFCS must implement appropriate technical and organisational security measures to protect the information against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in violation of the Act. For information which is of particular interest to foreign powers, CFCS must implement measures which allow for disposal or destruction in case of war or the like.

Annual report 2018
Danish Centre for Cyber Security
Published by the Danish Intelligence Oversight Board, June 2019

Layout + illustrations: Eckardt ApS
Portrait photographs: Lars Engelgaar

The publication is available on the Oversight Board's website at www.tet.dk

Members of the Danish Intelligence Oversight Board

Michael Kistrup, High Court Judge, the Danish Eastern High Court (chairman)
Pernille Christensen, Legal Chief, Local Government Denmark
Professor Henrik Udsen, Copenhagen University
Professor Jørgen Grønnegård Christensen, Aarhus University
Erik Jacobsen, Chairman of the Board of Directors, Roskilde University

The Danish Intelligence Oversight Board
Borgergade 28, 1st floor, 1300 Copenhagen K
www.tet.dk