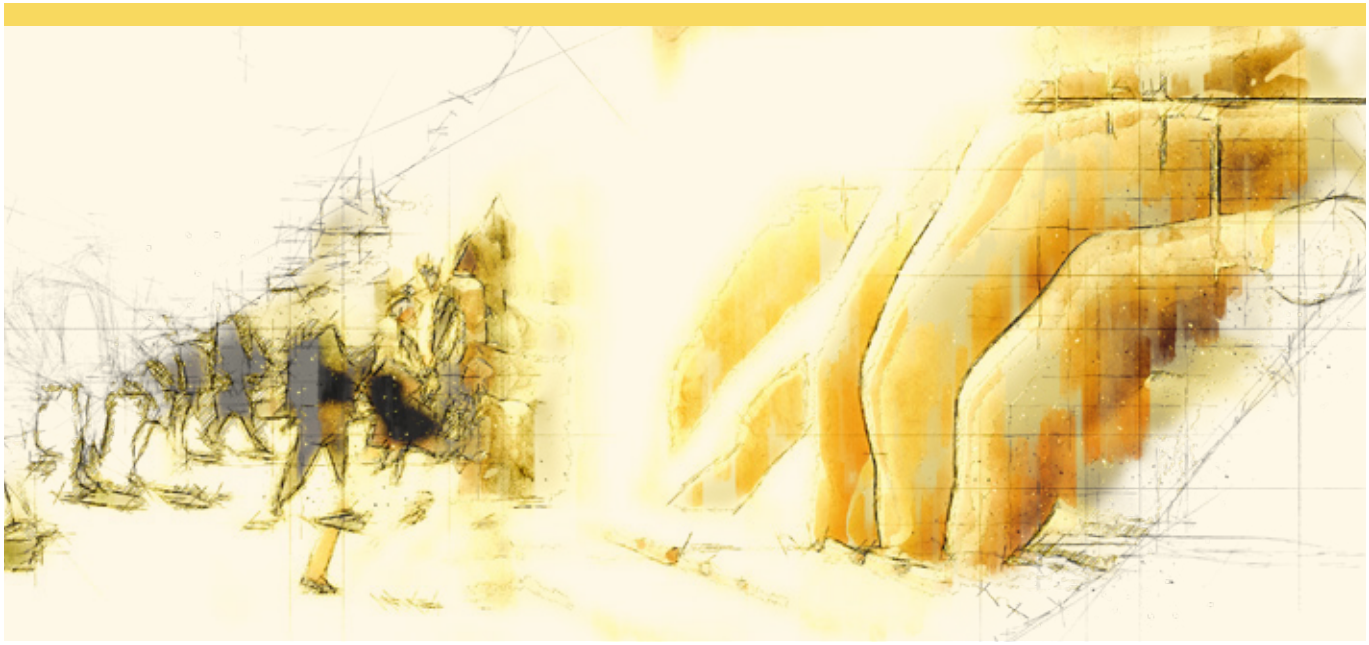
Danish Intelligence Oversight Board



Annual report 2022

Centre for Cyber Security (CFCS)

Contents

To the Minister of Defence

The Danish Intelligence Oversight Board (TET) hereby submits its report on its activities concerning the Centre for Cyber Security (CFCS) for 2022 in accordance with section 24 of the Centre for Cyber Security Act (Consolidated Act No. 836 of 7 August 2019). The annual report must be published.

The aim of this annual report is to provide general information about the nature of the oversight activities performed with regard to CFCS.

TET oversees CFCS' compliance with the provisions of the CFCS Act concerning:

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

The report includes information about the aspects, which TET has decided to review more closely as well as the number of instances where CFCS' processing of personal information has been found by TET to be in violation of CFCS legislation.

Copenhagen, June 2023

Michael Kistrup
Chair of the Danish Intelligence Oversight Board

Introductory comments

CFCS is tasked with the responsibility of assisting 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 is tasked with detecting, analysing and contributing to preventing advanced cyber security attacks against the Danish military as well as government authorities and businesses forming part of CFCS' sensor network.

In order to perform this nationally important function, CFCS has broad powers and capabilities under the law to intercept communications without a court order and to subsequently process information about citizens and businesses. In order to ensure due process protection for the individual citizen and business in Denmark, CFCS' wide powers are counterbalanced by a set of rules governing the subsequent erasure by CFCS of the information procured.

In 2022, TET has carried out in-depth and intensive compliance reviews with regard to CFCS, including with regard to CFCS' processing and disclosure of data from CFCS' sensor network to which Danish public authorities as well as private businesses performing nationally important functions are connected.

In connection with TET's compliance reviews in 2022, CFCS has generally made great efforts to assist TET by attending meetings, providing prior written clarification of factual and legal matters and responding to consultation questions concerning completed reviews.

TET and CFCS have ongoing discussions on the interpretation of the CFCS Act in relation to the obligations imposed on CFCS and TET's checks thereof. In accordance with the provisions of the CFCS Act, the Minister of Defence is involved to the extent necessary. This has been reflected, among other things, in TET's reviews of CFCS' security of processing in 2022.

In relation to TET's other activities in 2022, the publication of the compliance standards has resulted in increased national and international attention and – on this basis – cooperation and dialogue with similar authorities and think tanks in Denmark, the Nordic countries, Europe and Canada, as well as other international organisations. In addition, in 2022, TET has continued its cooperation with other Nordic and European bodies charged with overseeing intelligence or security services and initiated cooperation with the Independent Evidence Oversight Board (the Evidence Oversight Board) on the exchange of staff for shorter periods for sparring and mutual capacity building.

Scale of TET's comments

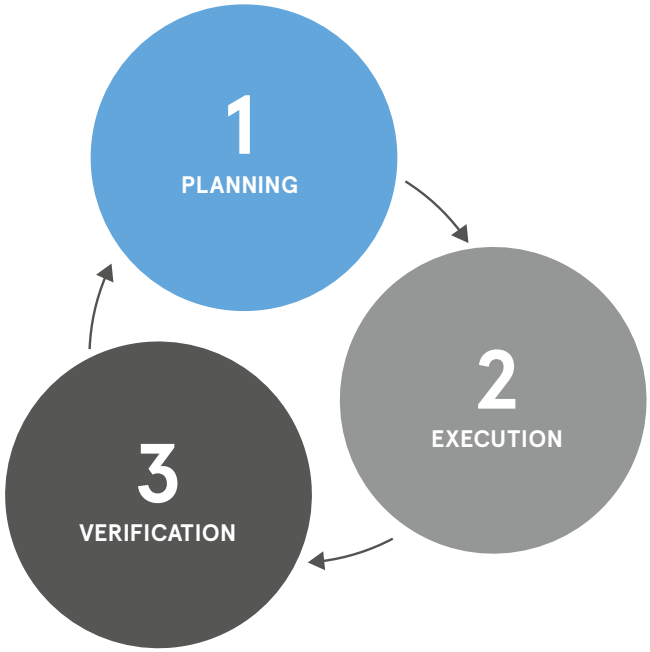
TET's comments are based on the following scale:

Comments	Background to comments
»[...] **does not give rise to any comments**«	Used when TET's review is limited by either factual or legal circumstances.
»On the information available, TET is **unable to assess** [...]«	Used for situations in CFCS or legislation which do not quite match the general or immediate impression of an outsider.
»TET finds it **striking** [...]«	Used for situations where no actual non-compliance with legislation has been established, but where there is considered to be a high risk that the situation could lead to non-compliance with legislation or where TET has been prevented from performing its activities for a certain period of time.
»TET finds it **problematic** [...]«	Used for situations where actual non-compliance with legislation of an isolated nature or non-compliance with internal guidelines has been identified.
»TET has **identified** [...]«	Used for situations where actual non-compliance with legislation of a not insignificant extent has been identified or where TET has been prevented from exercising its activities for a prolonged period.
»TET finds it **criticisable** [...]«	Anvendes om forhold, hvor der er konstateret egentlige lovbrud af et ikke uvæsentligt omfang eller hvor TET har været forhindret i at udøve sin virksomhed i en længere periode.
»TET finds it **highly criticisable** [...]«	Used for situations where serious non-compliance with legislation has been identified or where TET has been prevented from performing its activities for a prolonged period without CFCS having demonstrated a willingness to ensure the necessary remedial action.

1. Oversight method

TET 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 the work of TET.

In general, the oversight of CFCS consists of the following parts:



TET's **1)** planning of next year's compliance reviews is based on an annual risk and materiality assessment of CFCS processes and systems. The purpose of the risk and materiality assessment is to assess the risk of non-compliance with legislation in relation to CFCS activities falling within TET's scope of competence. On that basis, TET prepares risk analyses, which form the basis of the selection of the reviews to be made in the coming year.

The purpose of the risk analyses is to ensure that the oversight activities are focused on the areas with the highest risk of errors and that other relevant factors are taken


GIN

into account, e.g. areas where TET's oversight activities are given special weight by the legislators such as the rules on disclosure and sharing of information.

Areas that are deemed to have a low risk of errors are generally reviewed 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.

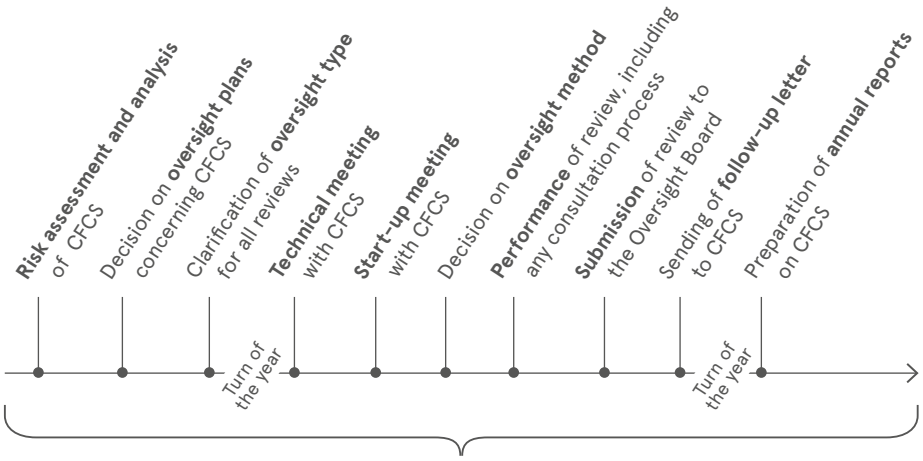
The reviews **2)** are conducted regularly throughout the year based on the CFCS oversight plan approved by TET. TET does not define the methods for the individual reviews in connection with the preparation of risk assessments and analyses, and the choice of method must thus be determined prior to initiating a specific review.

TET uses various methods to review the individual areas, including full reviews, random or targeted samplings, content screenings, inspections and interview-based reviews.

The choice of oversight method is based on a specific risk assessment of the oversight area, experience from previous reviews and findings in connection with the specific review. In that connection, prior to reviewing areas not previously reviewed, TET holds technical meetings and start-up meetings with relevant CFCS employees in order to ensure an adequate technical understanding of the area that will allow for the reviews to be adjusted and adequately performed.

Finally, TET **3)** performs verification by continuously mapping CFCS' IT infrastructures at the server, component and application level in order to be able to make complete risk assessments of all CFCS processes and systems. The purpose of the verification is to ensure that TET's reviews are based on data from CFCS the correctness of which has been verified by TET.

TET's activities include the following stages:



Continuous verification and mapping of IT landscapes with feedback to risk assessments and analyses as well as clarification of oversight method for the individual reviews

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

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

For further information on TET's oversight methods, reference is made to the relevant standards published by TET, which are available on TET's website.

2. TET's review

2.1 Summary of TET's reviews in 2022

In 2022, TET has completed 13 out of 14 planned reviews of CFCS.

The result of TET's reviews is described in full in section 2.2. The central and fundamentally important parts of the report are emphasised below.

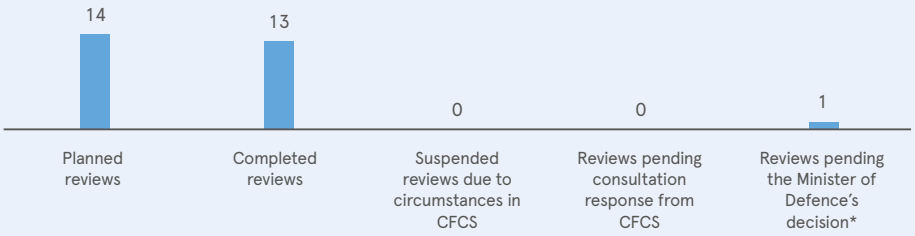
It is noted that the below references only represent a minor cross-section of TET's reviews of CFCS in 2022. For a full picture of TET's checks of CFCS, the report should be read in its entirety.

- 11 out of 13 reviews of CFCS did not give rise to any comments. Of the remaining two reviews, none gave rise to any comments on highly criticisable or criticisable matters.

- In one review, TET found that CFCS in three cases stored data falling within the scope of Part 4 of the CFCS Act which should have been erased as the purpose of the processing had been fulfilled, see section 17(1) of the CFCS Act, and that the data in three cases should in any case have been erased no later than in August and September 2021, see section 17(2)(i) of the CFCS Act (section 2.2.3).

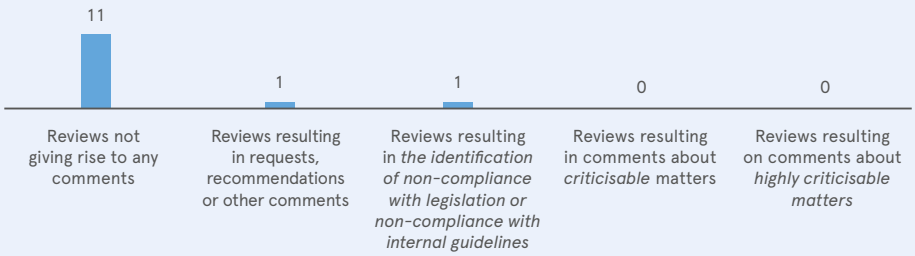
- On the information available, TET was unable to assess whether CFCS had taken the appropriate security measures in two systems in accordance with section 18 of the CFCS Act (section 2.2.7).

TET's reviews of CFCS in 2022



* See section 2.2.3.

Result of TET's review of CFCS in 2022



Note: If a review has had several different results, such as recommendations and findings of non-compliance with legislation or comments on highly criticisable or criticisable matters, these will be included under each category.

2.2 Review of CFCS in 2022

For the purpose of reviewing CFCS' compliance with the provisions of the CFCS Act when processing information about natural persons, TET has carried out reviews in 2022 of CFCS'

- processing of information on its sensor network (2.2.1),
- processing of information in separate IT environments and analytical tools (2.2.2),
- processing of information in other systems (2.2.3),
- use of court-ordered disclosure (2.2.4),
- disclosure of information to other public authorities, private businesses and partners (2.2.5),
- sharing of information with other parts of DDIS (2.2.6),
- security of processing (2.2.7),
- internal controls (2.2.8), and
- follow-up on TET's checks in 2021 (2.2.9).

Furthermore, in 2022, TET has completed

- technical reviews and mapping of CFCS' IT landscape (2.2.10).

2.2.1 Reviews of CFCS' processing of information on its sensor network

CFCS operates a sensor network that monitors internet traffic at the public authorities and private businesses, which are connected to the network (so-called NSS sensors). The sensors contain a number of rules which are used to recognise attempted cyber-attacks. When the sensors detect potentially hostile traffic which matches a rule, CFCS will receive an alert. CFCS staff will then collect a relevant sample of the internet traffic to examine the cause of the traffic.

In addition to the NSS sensors, CFCS operates a sensor network to create a national situational picture that can form the basis for the CFCS' alert procedure for observed threats (so-called NCSO sensors).

Data obtained from CFCS' sensor network must not be held for more than 5 years, 3 years or 13 months, see section 17(2)(i)-(iii) of the CFCS Act. How long CFCS may hold sensor data is determined by whether the data is related to a security incident and whether it is sensor data originating from public authorities which are particularly involved in or whose activities are of special importance to foreign policy, national security policy and defence policy matters, as well as private businesses and organisations whose activities are of special importance to those matters.

In 2022, TET carried out reviews of CFCS' processing, including erasure, of information on both of its sensor networks.

Comments by TET

TET's reviews of CFCS' use of its sensor network did not give rise to any comments.

2.2.2 Reviews of CFCS' processing of information in separate IT environments and analytical tools

CFCS uses a number of separate IT environments and analytical tools for its technical analysis of, for example, cyber-attacks, malware and phishing. CFCS processes and stores information in these IT environments and analytical tools in connection with its analysis thereof. In some cases, the information will originate from CFCS' sensor network, but may also have been obtained from open sources, such as the internet.

In 2022, TET carried out compliance reviews with regard to CFCS' processing of information in two analytical tools.

Comments by TET

TET's reviews of CFCS' processing of information in separate IT environments and analytical tools did not give rise to any comments.

2.2.3 Reviews of CFCS' processing of information in other systems

In connection with its activities, CFCS uses a wide range of different systems to store and process data, e.g. file systems, file drives or email systems.

Processing may include general personal data as well as information obtained by interception of communications pursuant to Part 4 of the CFCS Act, such as information from CFCS' sensor network.

In 2022, TET carried out compliance reviews with regard to CFCS' processing of information in other systems by reviewing

- a file system
- a shared drive and
- CFCS work stations

Comments by TET

TET identified that CFCS in three cases stored data falling within the scope of Part 4 of the CFCS Act which should have been erased as the purpose of the processing had been fulfilled, see section 17(1) of the CFCS Act, and that the data in three cases should in any case have been erased no later than in August and September 2021, see section 17(2)(i) of the CFCS Act 3). The information was erased from the user-related part of the system, but could still be accessed by CFCS system administrators.

The time limit for erasure under section 17(2)(i) of the CFCS Act was extended from 3 to 5 years by Act no. 555 of 7 May 2019 (Act to amend the Centre for Cyber Security Act). However, as the information in question was obtained before 1 July 2019, it was the previous time limit for erasure of 3 years that applied to the information, see section 2(2) of the amending act.

On 1 November 2021, the Minister of Defence made a decision regarding the scope of application of section 17(1) of the CFCS Act in relation to sensor data based on TET's reviews of CFCS' sensor network in 2019 (see TET's annual report for 2021, section 2). In connection with the review of work stations in 2022, TET stated that, in its opinion, CFCS is obliged to erase sensor data processed on employees' work stations once the purpose of the processing has been fulfilled, see section 17(1) of the CFCS Act, as, in TET's opinion, the decision of the Minister of Defence only concerns sensor data stored centrally.

CFCS stated that, in its opinion, the decision of the Minister of Defence also applies to CFCS' processing of sensor data on work stations, and as according to the Minister's decision of 1 November 2021 section 17(1) of the CFCS Act has a very limited scope in relation to sensor data, and as the primary scope of the provision is the other types of data covered by chapter 4 of the CFCS Act. On this basis, CFCS will submit the matter to the Minister of Defence for a decision.

2.2.4 Review of CFCS' use of court-ordered disclosure

Court-ordered disclosure is a special legal remedy in Part 4a of the CFCS Act which grants CFCS the power to order third parties to produce information to CFCS about the user of an email address, IP address or domain name. The order is subject to CFCS having obtained a court order as a basis for the disclosure.

In a court-ordered disclosure, the court orders the person who has access to the information, typically a telecom provider, to produce the information to CFCS.

In 2022, TET carried out a compliance review with regard to CFCS' use of court-ordered disclosure.

Comments by TET

TET's review of CFCS' use of court-ordered disclosure did not give rise to any comments.

2.2.5 Review of CFCS' disclosure of information to other public authorities, private businesses and partners

As part of the performance of its activities, CFCS regularly discloses information to other public authorities, businesses and partners. By way of example, CFCS may in exceptional circumstances disclose information obtained from its sensor network in connection with a security incident to connected public authorities, see section 16 of the CFCS Act.

In 2022, TET carried out a review of CFCS' disclosure of information.

Comments by TET

TET's review of CFCS' disclosure of information did not give rise to any comments.

2.2.6 Review of CFCS' sharing of information with other parts of DDIS

Organisationally, CFCS forms part of DDIS, and internal sharing of information between CFCS and the other parts of DDIS therefore does not fall within the scope of the provisions

of the CFCS Act on disclosure. The Ministry of Defence's Circular No. 9741 of 21 August 2019 on the processing of data in and from the CFCS Network Security Service (the CFCS Circular) regulates the sharing of information from CFCS to DDIS.

In 2022, TET carried out a review of CFCS' sharing of information with other parts of DDIS. The particular focus of the review was on whether CFCS has ensured sufficient access restriction of information systems where information obtained by interception of communications is processed, see section 4 of the CFCS Circular.

Comments by TET

TET's review of CFCS' sharing of information with other parts of DDIS did not give rise to any comments.

2.2.7 Reviews of CFCS' compliance with the rules on security of processing

According to section 18 of the CFCS Act, CFCS must implement appropriate technical and organisational security measures to protect information against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in violation of the Act.

In relation to two reviews in 2022, TET has asked detailed questions about how CFCS ensures that the processing of data in the systems in question is in accordance with the requirements of section 18 of the CFCS Act.

In this regard, TET has asked CFCS to state:

- What measures CFCS has taken to ensure that the processing of data in the systems is in accordance with section 18 of the CFCS Act.
- Whether CFCS has conducted a risk assessment of the security of processing of data processed in the systems.

CFCS has referred to its initiatives in the ISO/IEC 27001 area regarding security of processing as well as Circular No. 10338 of 17 December 2014 of the Prime Minister's office and the military security regulations (FKOBST 358-1), which also contain a number of requirements for security of processing, as documentation for the measures taken by CFCS to ensure the level of security of processing.

Furthermore, CFCS has stated that in its opinion section 18 of the CFCS Act does not contain a legal obligation for CFCS to perform risk assessments at system level when establishing systems within the existing IT infrastructure. After the review, CFCS has stated that in its assessment, the measures implemented by CFCS across the system portfolio can generally be assumed to meet the requirements of section 18 of the CFCS Act.

Comments by TET

TET stated that it does not agree with CFCS' assessment that it was not the intention of section 18 of the CFCS Act to lay down specific legal requirements for CFCS' security of processing.

Furthermore, TET stated that, in its assessment, section 18 of the CFCS Act – like section 41(3) of the then current Data Protection Act – specifically imposes on CFCS an obliga-

tion to take any such appropriate technical and organisational measures which protect against the risks described in the provision. According to the specific explanatory notes to section 41(3) of the Data Protection Act, it is assumed that the measures, taking into account the current state of the art and the costs associated with their implementation, will provide an adequate level of security in relation to the risks posed by the processing and the nature of the data to be protected.

Against this background, TET assessed that CFCS, in the cases where CFCS processes data, is obliged to make an assessment of which measures can provide an adequate level of security. The assessment will need to take into account the risks presented by the processing and the nature of the data to be protected, taking into account the state of the art and the costs involved in their implementation. Once CFCS has completed the assessment, it will then be obliged to ensure that the relevant measures are implemented for the processing in question.

In TET's assessment, it is a prerequisite for its reviews of CFCS' compliance with section 18 of the CFCS Act that CFCS documents its assessment of which measures it finds necessary to implement in order to provide an adequate level of security in relation to the risks involved in the processing and the nature of the data to be protected.

On the information available, TET was unable to assess whether CFCS had taken the appropriate security measures in two systems in accordance with section 18 of the CFCS Act.

Based on the review, CFCS informed TET that it disagrees with TET's assessment and will therefore submit the matter to the Minister of Defence for a decision.

CFCS' compliance with the rules on security of processing will continue to be a focus point for TET.

2.2.8 Review of CFCS' internal review

CFCS carries out regular internal review of its compliance with specific parts of the CFCS Act. For the purpose of organising its own internal reviews, CFCS must prepare an annual risk assessment of its compliance with statutory requirements and a schedule for its internal review for the following year. CFCS must regularly inform TET of the organisation of its internal review and their results, including by submitting its risk analysis and oversight plan.

In May 2022, CFCS has informed TET about its

- risk analysis concerning compliance with statutory requirements and
- review plan for 2023.

In addition, CFCS has regularly informed TET about its internal reviews.

Comments by TET

TET's review of CFCS' internal review did not give rise to any comments.

2.2.9 Follow-up on TET's reviews of CFCS in 2021

Each year, TET review whether CFCS has initiated the measures which CFCS has stated that it would based on TET's reviews in the preceding year.

In 2022, TET has followed up on its reviews of CFCS in 2021.

Comments by TET

The follow-up on TET's review of CFCS in 2021 did not give rise to any comments.

2.2.10 TET's technical reviews and mapping of CFCS' IT landscape

CFCS' IT systems and underlying databases in which information is processed form a complex and dynamic landscape of different technologies and data types. In order to navigate this complex IT landscape and fulfil TET's primary tasks, TET has in 2022 reviewed and verified extensive parts of CFCS' IT landscape and continuously works to ensure up-to-date knowledge of CFCS' systems.

It is a prerequisite for meaningful oversight of CFCS that TET has knowledge of CFCS' overall IT infrastructure so that its reviews can be targeted at the parts of the infrastructure which pose the greatest risk of processing in violation of CFCS legislation.

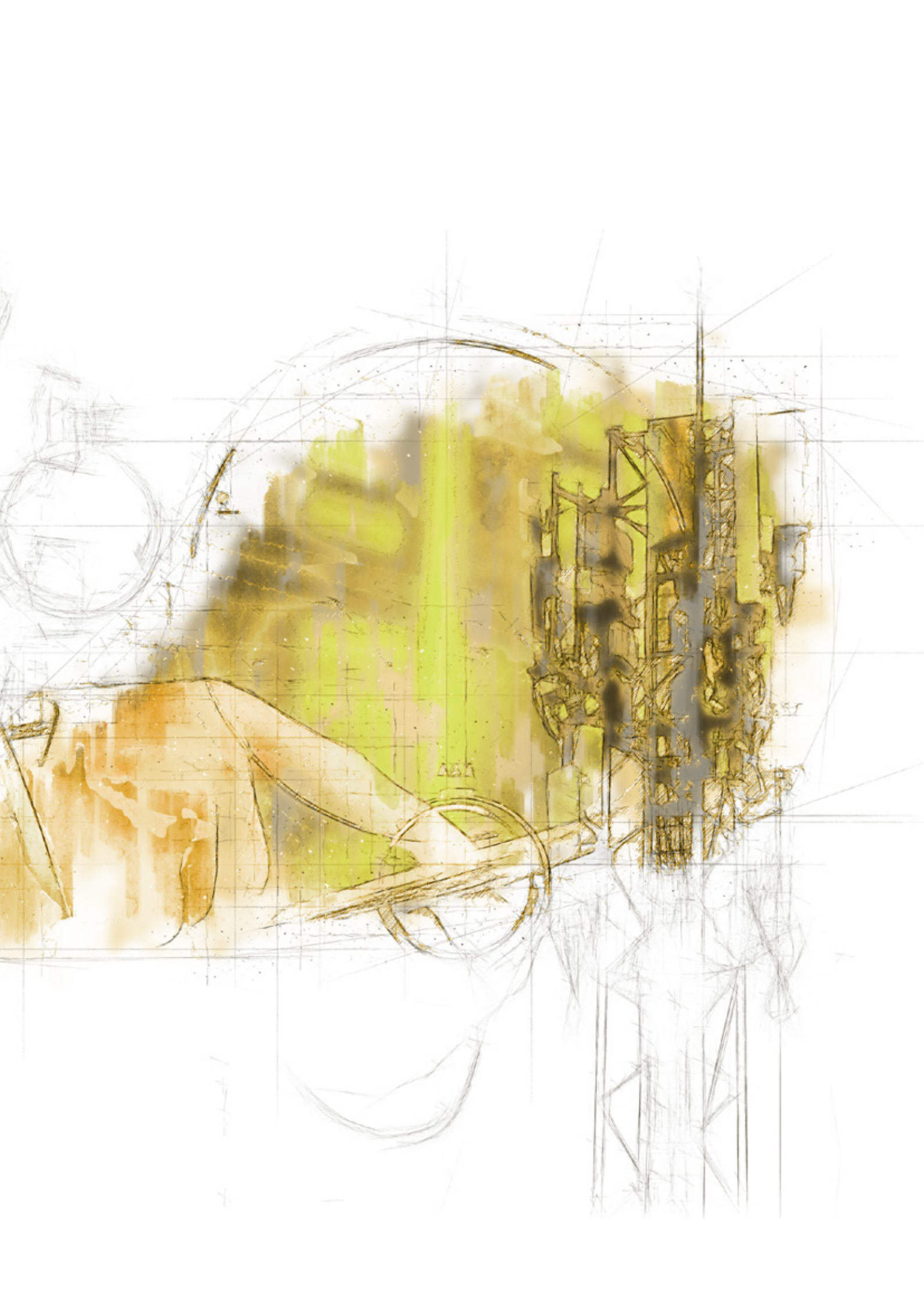
In 2022, TET has performed validation reviews and inspections of CFCS' IT infrastructure by inspecting a number of systems, which, in TET's immediate assessment, should not form part of TET's general reviews, in order to clarify whether the immediate assessment thereof was correct.

In 2022, TET has also initiated a mapping of CFCS' handling of the erasure of data from its sensor network. The mapping is expected to be finalised during 2023.

2.3 CFCS' processing times in 2022

In 2022, TET submitted seven legal consultations to CFCS in connection with its review activities. CFCS has responded to five of TET's consultation questions within the specified deadline and two after the specified deadline. CFCS' average processing time for responding to consultation questions that were responded to after the deadline was 30 working days.

In 2022, TET has been in dialogue with CFCS and developed a new consultation handling process.



3. Examples of CFCS' handling of cyber-attacks

According to the legislative history of the CFCS Act, the annual report of TET 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 2022:

CFCS is tasked with protecting the important parts of Danish society against cyber-attacks. In practice, this task is carried out by the Network Security Service detecting, analysing and contributing to preventing IT security incidents at public authorities and private businesses which are vital to society forming part of the CFCS sensor network or which request CFCS' assistance. The Network Security Service consists of several organisational units within CFCS.

In 2022, the Network Security Service handled a large number of IT security incidents for public authorities and private business in and outside the sensor network. The majority of these incidents involved reconnaissance, social engineering and compromises in the form of data espionage and data theft. CFCS has observed attacks and attempted attacks from both state-sponsored and criminal cyber players also in 2022.

Based on CFCS' observations, phishing attacks continue to be considered a serious threat to connected public authorities and private businesses. Such threats include emails from a malicious player that tries to trick a recipient into activating or accessing content in the email that can either lead to infections or steal login information from the victim.

In addition, CFCS has observed various types of attempts to exploit misconfigurations and vulnerabilities in software services that are exposed to the internet. This also includes brute force-related attempted attacks targeting exposed IT systems which the attacker is trying to gain access to.

4. Statistical data on CFCS' processing of information

As can be seen from the legislative history of the CFCS Act, TET's annual report must provide statistical data on CFCS' processing of personal information, including data on the number of complaints received by CFCS as well as by TET, 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 report must also include statistical data on the number of instances 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 2022:

TABLE 1

Disclosure and sharing of information

Categories	2022
Disclosure of information	46
Sharing of information	6

TABLE 2

Security incidents* according to severity

Categories	2022
Serious cyber-attacks	3
Major cyber-attacks	2
Moderate cyber-attacks	23
Minor cyber-attacks	328
No/limited effect**	1,468
False positives***	1,253
Total	**3,077**

* Security incidents are defined in accordance with section 2(i) of the CFCS Act.
** The category "No/limited effect" includes all the security incidents that have not had an impact on the customer
*** The category "False positives" covers suspicions of a security incident that turns out not to be the case based on closer analysis.

TABLE 3

Subject access requests

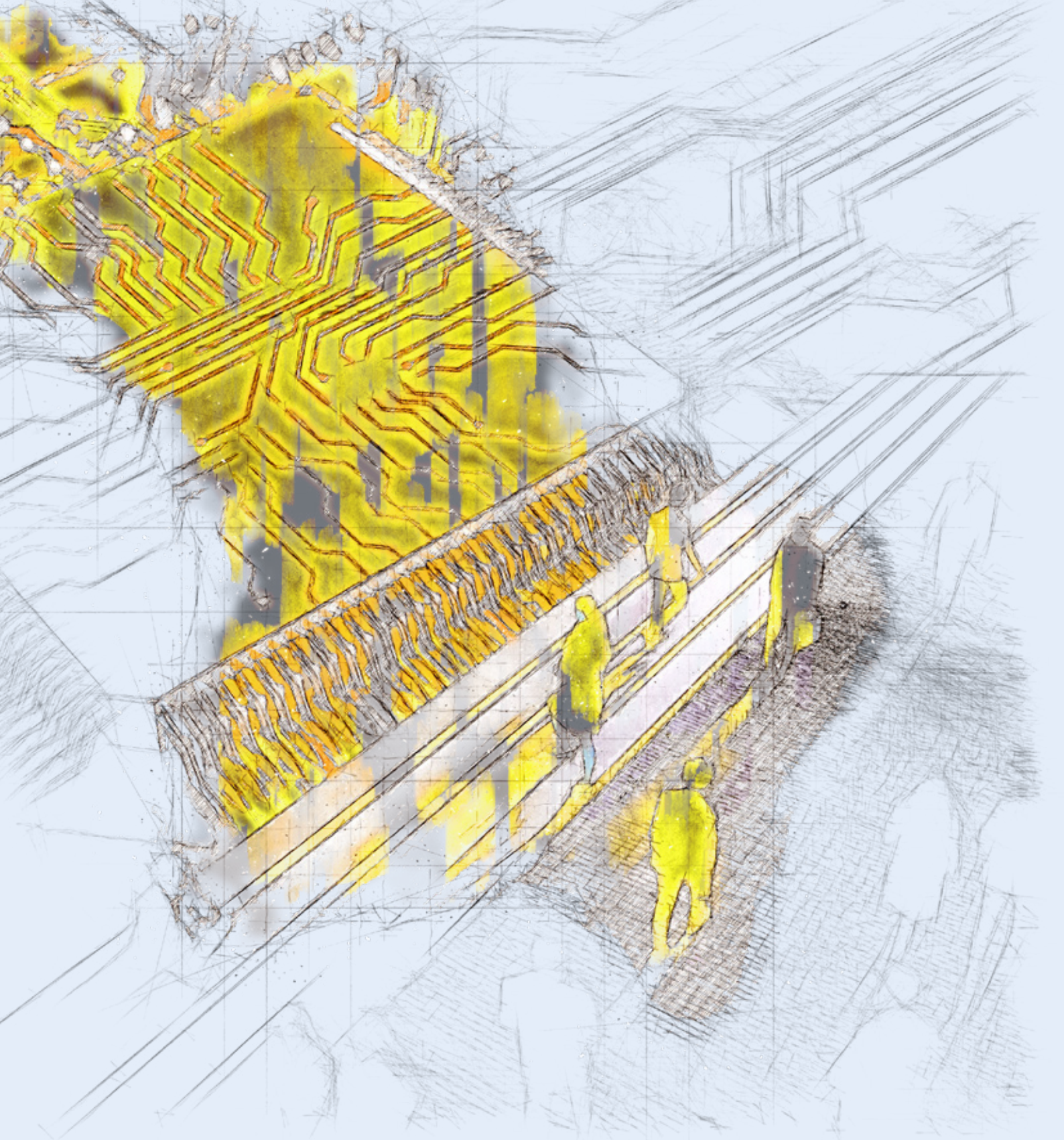
Categories	2022
Full access requested	3
Partial access requested	1
Requests refused	6
No documents located to grant or refuse access	0
Total	**10**

TABLE 4

Processing of personal information

Categories	2022
Complaints to CFCS about the processing of personal data	0*
Complaints received by TET	0

* CFCS is not aware of any complaints received



Appendix

1. About Centre for Cyber Security (CFCS)

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 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' 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' sensor network.

CFCS' 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' 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 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.

The legal framework within which CFCS operates essentially follows from the CFCS Act and the Executive Order and CFCS Circular issued under the CFCS Act as well as the NIS Act.

Among other things, the CFCS Act governs CFCS' duties as well as interception of communications, processing, analysis, disclosure and erasure of personal information. With the Act, it is further established that TET – which is an independent monitoring body charged with overseeing DSIS and DDIS – is also charged with overseeing that CFCS processes information about natural persons in compliance with CFCS legislation.

CFCS is also subject to external control by the Ministry of Defence, the courts and the Parliamentary Ombudsman.

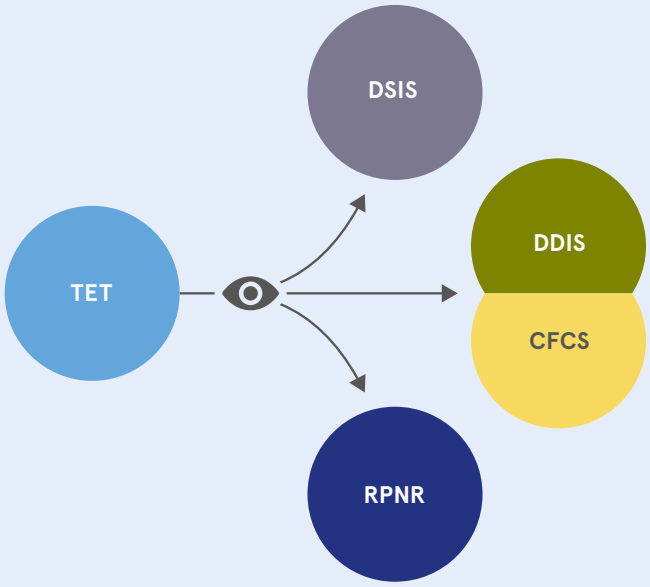
Appendix

2. Danish Intelligence Oversight Board (TET)

TET's activities

Staffing in 2022 (employees)	8
Budget appropriation in 2022 (DKK million)	9,9

The Danish Intelligence Oversight Board (TET) is an independent monitoring body charged with overseeing that DSIS, DDIS, CFCS and the PNR Unit of the Danish National Police (RPNR) process personal information in compliance with DSIS, DDIS, CFCS and RPNR legislation.



TET 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.

TET is composed of five members who are appointed by the Minister of Justice following consultation with the Minister of Defence. The chair, 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.

TET had the following members as at the end of 2022:

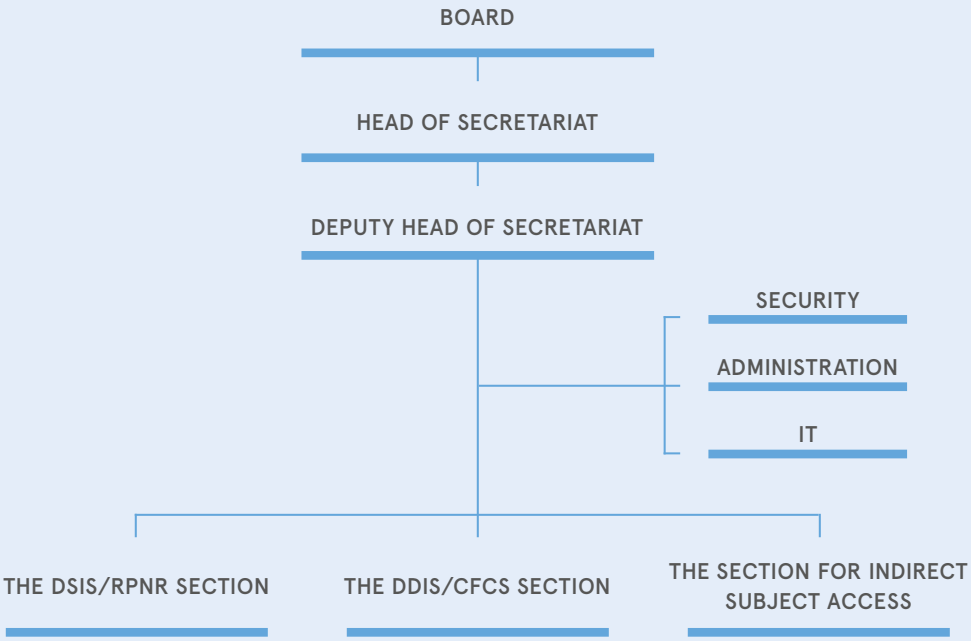
- High Court Judge Michael Kistrup, High Court of Eastern Denmark (Chair)
- Legal Chief Pernille Christensen, Local Government Denmark
- Professor Henrik Udsen, University of Copenhagen
- Professor Rebecca Adler-Nissen, University of Copenhagen
- Director Jesper Fisker, Danish Cancer Society

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 TET was set up in 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.

TET is supported by a secretariat, which is subject solely to the instructions from TET in the performance of its duties. TET recruits its own secretariat staff and decides which educational and other qualifications the relevant candidates must have. At the end of 2022, the secretariat consisted of a Head of Secretariat, who is in charge of the day-to-day management, a deputy, three lawyers, two IT consultants and an administrative employee.

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

Organisation 2022



2.1 TET's duties in relation to CFCS

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

- interception of communications,
- processing of personal information at CFCS,
- analysis, disclosure and erasure of data, and

- the requirements to security measures in connection with CFCS' processing of personal information.

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

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

2.2 TET's access to information held by CFCS

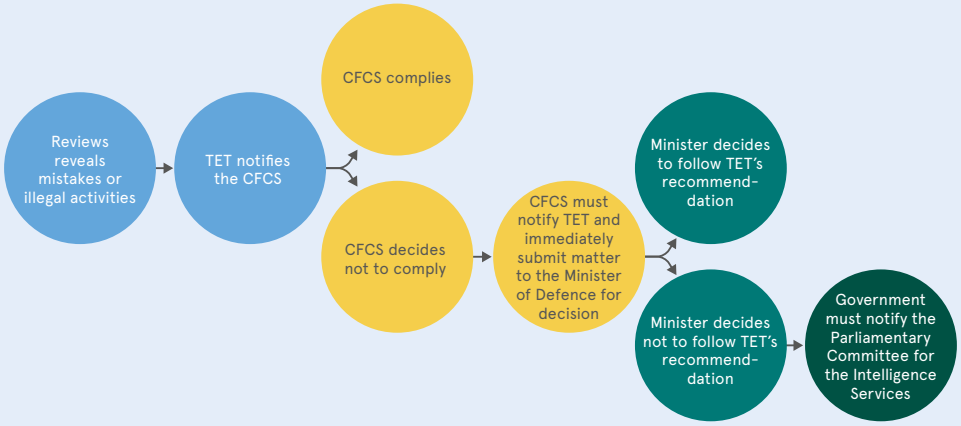
TET may require CFCS to provide any information and material of importance to TET's activities, and TET is entitled at any time to access any premises where the information being processed may be accessed or where technical facilities are being used. TET may furthermore require CFCS to provide written statements on factual and legal matters of importance to TET'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 TET for TET to make its own searches in CFCS' IT systems.

2.3 Responses available to TET

TET has no authority to order CFCS to implement specific measures in relation to data processing. However, TET 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 TET in exceptional cases, CFCS must notify TET and immediately submit the matter to the Minister of Defence for a decision.

Responses available for TET



TET must inform the Minister of Defence of any matters which the Minister ought to know in the opinion of TET.

Each year, TET 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 TET's interest. The reports must provide statistical data on CFCS' processing of personal information, including data on the number of complaints received by CFCS as well as by TET, 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. TET must also provide data on the number of instances where personal information has been found by TET 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.

TET submitted its most recent report on its activities to the Minister of Defence in May 2022. The report was published in June 2022.

Appendix

3. Legal framework

1) The Centre for Cyber Security Act (Consolidated Act No. 836 of 7 August 2019 (the CFCS Act)

2) The Ministry of Defence's Circular on processing of data in and from the CFCS Network Security Service (Circular No. 9741 of 21 August 2019) (the CFCS Circular)

3) Decree No. 1658 of 20 November 2020 on the entry into force for Greenland of the Centre for Cyber Security Act

3.1 The CFCS Network Security Service

3.1.1 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 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. In special cases, CFCS may order private businesses, which are vital to society as well as regional authorities and municipalities to join the Network Security Service.

The CFCS Network Security Service is the name of CFCS' 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. 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 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.

3.2 Interception of communications and court-ordered disclosure

3.2.1 About interception of communications, see sections 4-6c of the CFCS Act

Section 4 of the CFCS Act means that the CFCS Network Security Service is entitled, without a court order, to process content data, intercept related data and stationary data originating from connected public authorities and private businesses for the purpose of maintaining a high level of cyber security in Denmark. *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. Stationary data means data held on servers, cloud services, PCs, storage devices, network devices, mobile devices and the like, see section 2(iii) of the Act.

It follows from section 5 of the Act that on reasonable suspicion of a security incident, CFCS is entitled, without a court order, to process stationary data from a public authority or private business which is not connected to the Network Security Service when:

1) the public authority or private business has requested assistance from CFCS, made the stationary data available and given its written consent to processing, and

2) the processing is deemed to contribute to maintaining a high level of cyber security in Denmark.

It follows from section 6 of the Act that if so agreed with a public authority or private business which is connected to the CFCS Network Security Service, CFCS is entitled, on reasonable suspicion of a security incident and without a court order, to block, convert or redirect intercept related data, content data and stationary data originating from networks at the public authority or private business in order to maintain a high level of cyber security in Denmark. In case of a security incident that has been found to exist, CFCS is entitled to erase stationary data that have caused the security incident.

Under section 6a of the Act, CFCS is entitled to carry out security-technical investigations in order to be able to advise public authorities and private businesses on the prevention of security incidents when a public authority or private business has requested CFCS to do so. In connection with a security-technical investigation, CFCS is entitled, without a court order, to process intercept related data, content data and stationary data at the public authority or private business, process publicly accessible data about the public authority or private business and its employees and initiate preventive activities directed at selected employees or entities of the public authority or private business.

Under section 6b of the Act, CFCS is entitled – for the purpose of gathering knowledge about the methods and tools used by hacker groups – to set up fictitious targets of attack if the set-up is deemed to contribute significantly to CFCS' possibilities of maintaining a high level of cyber security in Denmark. If hacker groups use a fictitious target of attack to deposit data, CFCS is entitled, without a court order, to process the deposited data for the purpose of detecting, analysing and contributing to preventing security incidents occurring to public authorities and private businesses or informing citizens, public authorities and private businesses that a security incident has occurred to them.

It follows from section 6c of the Act that in order to prevent, stop or mitigate an imminent or current security incident, CFCS may use domain names and similar IT infrastructure which are or have used been by a hacker group, provided that they are available for registration. If CFCS receives data from a third party in connection with the use of IT infrastructure, CFCS is entitled, without a court order, to process the data received for the purpose of detecting, analysing and contributing to preventing security incidents occurring to public authorities and private businesses or informing citizens, public authorities and private businesses that a security incident has occurred to them.

3.2.2 About court-ordered disclosure, see section 7 of the CFCS Act

For the purpose of investigating security incidents, a legal or natural person may be ordered under section 7 of the Act to present or provide information about the user of an email account, an IP address or a domain name if the information is available to the person in question, unless the measure is disproportionate in relation to the importance of the case and the loss or inconvenience which the measure can be assumed to inflict.

3.3 Processing of personal information

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

Under section 9 of the CFCS Act, CFCS' 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 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:

1) the data subject has given his or her explicit consent,

2) 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,

3) the processing is necessary for the performance of a task carried out in the public interest,

4) the processing is necessary to protect important aspects of national security or defence policy,

5) 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 information is disclosed,

6) the processing is necessary to safeguard legitimate interests pursued by CFCS or by the third party to whom the information is disclosed, and these interests are not overridden by the interests of the data subject, or

7) the processing concerns personal information falling within the scope of Part 4 (interception of communications).

If linguistically adjusted, section 10(i), (ii), (iii), (v) and (vi) of the Act 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. 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 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:

1) the data subject has given his or her explicit consent to such information being processed,

2) the processing concerns personal information which has been made public by the data subject,

3) the processing is necessary to establish, enforce or defend a legal claim,

4) the processing is necessary to protect important aspects of national security or defence policy, or

5) 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' responsibilities. Under subsection (2) of section 12, the personal information mentioned in subsection (1) may not be disclosed to any third party, unless:

1) the data subject has given his or her explicit consent to such disclosure,

2) 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,

3) 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,

4) the disclosure is necessary for the performance of tasks for an official authority by a person or a company, or

5) 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).

3.3.2 About security measures in connection with CFCS' 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.

3.4 Analysis and erasure of data falling within the scope of Part 4 of the CFCS Act

3.4.1 About analysis of data, see section 15 of the CFCS Act

It follows from section 15 of the Act that CFCS may perform automated analysis of intercept related data, content data and stationary data falling within the scope of Part 4 of the Act on interception of communications (sections 4-6c). CFCS may perform manual analyses of Part 4 data in the following cases only:

1) To detect, analyse and contribute to preventing security incidents, intercept related data may be analysed to the extent necessary.

2) On reasonable suspicion of a security incident, content data and stationary data may be analysed to the extent necessary to clarify matters concerning the incident.

3) In the course of preventive security-technical investigations under section 6a, intercept related data, content data and stationary data may be analysed to the extent necessary to complete the investigations.

4) During the process of the ongoing effort to maintain a high level of cyber security in the areas under the Ministry of Defence, including by monitoring communications to check if they contain classified material, intercept related data and content data originating from public authorities under the Ministry of Defence may be analysed.

5) In the course of technical testing and configuration of the alarm devices of the Network Security Service, intercept related data and content data may be analysed to the extent necessary to complete testing. Testing must be completed as soon as the purpose of testing has been fulfilled. The analysis must be performed by staff members performing technical operational management and development responsibilities for CFCS only. Other staff members are not allowed to access information originating from testing. However, any malware which is accidentally detected in the course of technical testing may be analysed by other CFCS staff under para. (ii).

3.4.2 About erasure of data, see section 17 of the CFCS Act

Under section 17(1) of the Act, any data processed pursuant to Part 4 of the Act on interception of communications (sections 4-6c) must be erased once the purpose of the processing is fulfilled. The provision should be seen in the context of section 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 all 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 the provision for the purpose of ensuring immediate erasure of any data that are no longer relevant in relation to the objectives and activities of the Network Security Service.

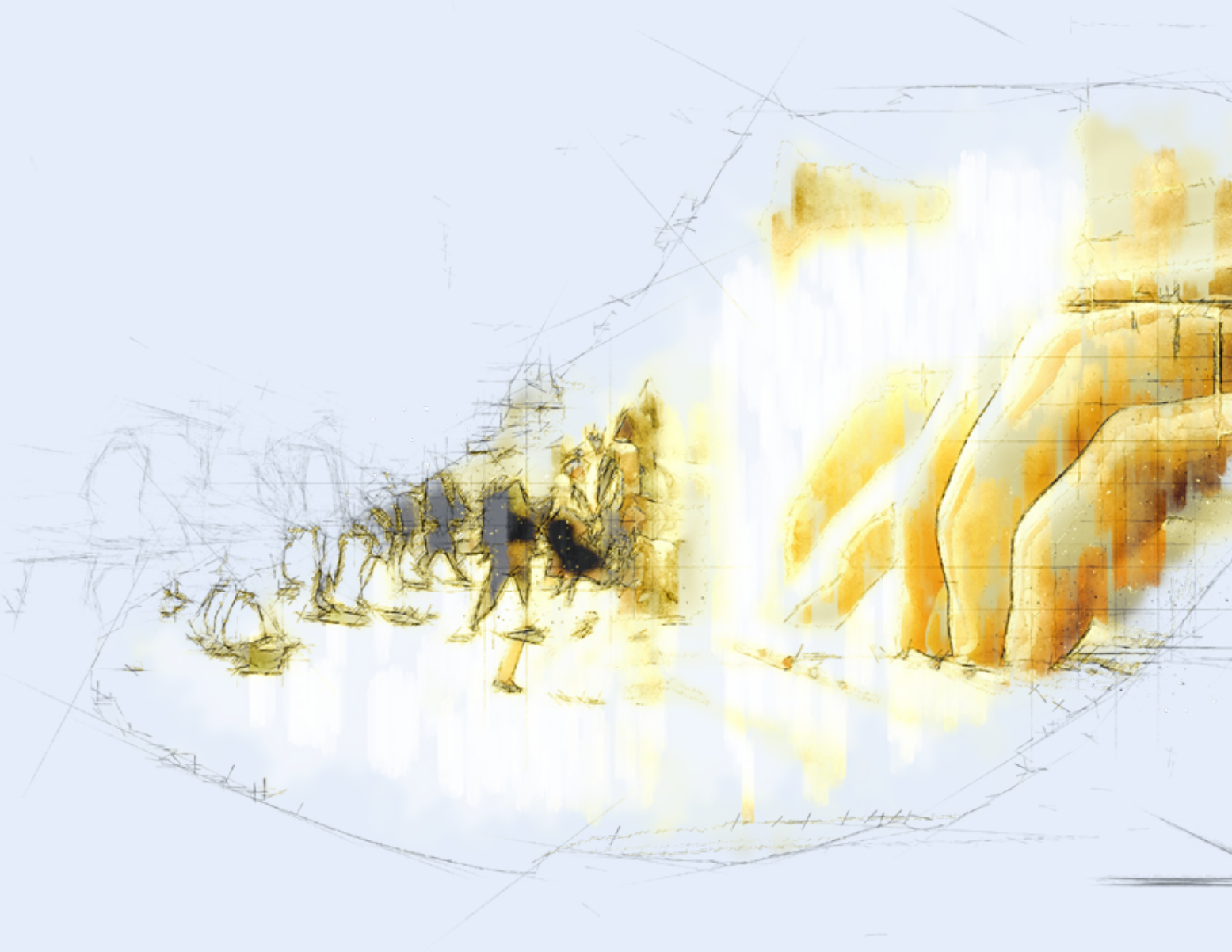
Furthermore, according to section 17(2) of the Act, even if the purpose of the processing has not been fulfilled, see subsection (1):

1) data which relates to a security incident must not be held for more than five years,

2) data which does not relate to a security incident, but originates from public authorities which are particularly involved in foreign policy, national security policy and defence policy matters as well as private businesses and organisations whose activities are of special importance to those matters must not be held for more than three years, and

3) data 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 data which has not been erased in accordance with section 17(1) of the Act may be held, and the provision thus applies to data 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 data must be erased within the absolute time limits laid down in the provision. If data relating to a security incident within the five-year period is found to be used again in connection with a security incident, a new five-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 data in question, see subsection (3).

In 2021, the Minister of Defence – based on TET's check – assessed the bearing of section 17(1) of the CFCS Act on CFCS' obligation to erase data obtained via CFCS' sensor network. In the assessment of the Minister of Defence, sensor data which CFCS has assessed, on the basis of an analysis, is not related to a security incident, is not required to be erased pursuant to section 17(1) of the CFCS Act.

The reason for this is that CFCS needs to be able to search historical data when it acquires new knowledge or tools. The purpose of the processing of sensor data can therefore not be said to be fulfilled under section 17(1) of the CFCS Act, but is merely erased under the absolute time limits for erasure in section 17(2) of the CFCS Act.

Even where it can be definitively concluded that the data are benign and could not later be linked to a cyber-attack, sensor data will need to be stored for the full period set out in section 17(2) of the CFCS Act, as erasure of this type of data could potentially impair the ability of CFCS to draw a precise picture of the normal internet activity of the organisation concerned.

However, in the opinion of the Minister of Defence, sensor data that in CFCS' assessment are linked to a security incident should be erased in accordance with section 17(1) of the CFCS Act, to the extent that, in CFCS' assessment, the specific data will not be relevant to CFCS' future ability to detect, analyse and contribute to countering cyber-attacks. In this connection, the Minister of Defence emphasises that CFCS is vested with a considerable degree of discretion as to when the purpose of the processing in these cases is fulfilled.

Section 17(1) and (2) of the Act does not apply to data which have been disclosed to parties other than the public authority or private business from which the data originate, see section 17(5) of the Act.

Personal information contained in data accessed by CFCS in the course of preventive security-technical investigations under section 6a must be erased or depersonalised under section 17(6) of the Act when the security-technical investigation is completed. If CFCS finds out that the data in question contain sensitive personal information, they must be erased without undue delay.

In exceptional circumstances, the above erasure periods may be briefly suspended if necessary to safeguard important interests with regard to the performance of CFCS' duties, see section 17(7). CFCS must immediately inform TET of the suspension and the background to it.

Section 17a of the Act provides that section 17 of the Act does not apply to data which are deposited on fictitious targets of attack under section 6b or received via infrastructure falling within the scope of section 6c if CFCS does not select those data for closer inspection. Instead, those data must be erased as soon as possible.

3.5 Disclosure and sharing of information falling within the scope of Part 4 of the CFCS Act

3.5.1 About disclosure, see section 16 of the CFCS Act

Under section 16 of the Act, CFCS is entitled in a number of specified instances to disclose data, which fall within the scope of Part 4 of the Act on interception of communications (sections 4-6c). The requirements for such disclosure depend on the identity of the intended recipient of the data and on the type of data disclosed.

Under section 16(1) of the Act, CFCS may disclose intercept related data falling within the scope of Part 4 to:

1) The police, on reasonable suspicion of a security incident.

2) The connected public authority or private business from which the data in question originate, on reasonable suspicion of a security incident and if necessary for the performance of CFCS' duties.

3) Danish authorities, providers of public electronic communication networks and services and other network security services as well as other public authorities and private businesses in connection with CFCS' circulation of security warnings, on reasonable suspicion of a security incident and if necessary for the performance of CFCS' duties.

Under section 16(2) of the Act, CFCS may disclose content data falling within the scope of Part 4 to:

1) The police, on reasonable suspicion of a security incident.

2) The connected public authority or private business from which the data in question originate, on reasonable suspicion of a security incident.

Under section 16(3) of the Act, CFCS may disclose stationary data falling within the scope of Part 4 to:

1) The police, on reasonable suspicion of a security incident.

2) The connected public authority, private business or citizen from which the data in question originate, on reasonable suspicion of a security incident.

3) Other network security services if CFCS has received the data in question pursuant to section 6b or section 6c.

Under section 16(4) of the Act, CFCS may disclose malware falling within the scope of Part 4 to:

1) The police.

2) The public authority or private business from which the data in question originate.

3) Danish authorities, providers of public electronic communication networks and services and other network security services as well as other public authorities and private businesses in connection with CFCS' circulation of security warnings.

Under section 16(5) of the Act, CFCS may disclose data originating from technical testing and configuration of the alarm devices of the Network Security Service in the following cases only:

1) Accidentally detected malware may be disclosed to the police, to the public authority or private business from which the data in question originate, to Danish authorities, to providers of public electronic communication networks and services and to other network security services as well as to other public authorities and private businesses in connection with CFCS' circulation of security warnings.

2) Content data may be disclosed to the connected public authority or private business from which the data in question originate.

Under section 16(6) of the Act, in connection with preventive security-technical investigations under section 6a, CFCS may disclose information about the employees of the public authority or the private business only in depersonalised form.

3.5.2 About sharing of data with DDIS, see section 2 of the CFCS Circular

It is stated in the general part of the explanatory notes to the CFCS Act concerning sharing of data internally in 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 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 DDIS as the foreign intelligence service can contribute with a large amount of valuable information.

In accordance with the above, article 2(1) of the CFCS Circular provides that CFCS is allowed to share data falling within the scope of Part 4 of the Act with other parts of DDIS only:

1) if the sharing of data is necessary to maintain a high level of cyber security,

2) if the sharing of data is for specified, explicit and legitimate purposes, and

3) on reasonable suspicion of a security incident.

Under subsection (2) of the provision, subsection (1)(iii) does not apply to data originating from public authorities under the Ministry of Defence.

It follows from subsection (3) of the provision that any sharing of data must be recorded by CFCS.

Annual report 2022
Centre for Cyber Security
Published by the Danish Intelligence Oversight Board, June 2023

Layout + illustrations: Eckardt ApS
Portrait photographs: Lars Engelgaar / Sophie Kalckar

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

Members of the Danish Intelligence Oversight Board

High Court Judge Michael Kistrup, High Court of Eastern Denmark (Chair)
Legal Chief Pernille Christensen, Local Government Denmark
Professor Henrik Udsen, University of Copenhagen
Professor Rebecca Adler-Nissen, University of Copenhagen
Director Jesper Fisker, Danish Cancer Society

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