



Danish Intelligence Oversight Board

# Annual report 2023

Danish Centre for Cyber Security (CFCS)





## TO THE MINISTER OF DEFENCE

The Danish Intelligence Oversight Board (TET) hereby submits its report on its activities concerning the Danish Centre for Cyber Security (CFCS) for 2023 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 review activities performed with regard to CFCS.

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

- ▶ interception of communications,
- ▶ processing of personal information at CFCS,
- ▶ analysis, disclosure and deletion 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 examine 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.

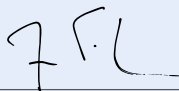
Copenhagen, May 2024



Pernille Christensen



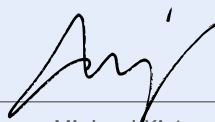
Henrik Udsen



Jesper Fisker



Rebecca Adler-Nissen



Michael Kistrup

# CONTENTS

<b>1. Introductory comments</b> .....	<b>3</b>
<b>2. Generally about TET's review activities</b> .....	<b>4</b>
2.1 General prerequisites for TET's reviews and its expectations from DSIS, DDIS, CFCS and PPNR ..	5
2.2 Scale for TET's comments .....	8
2.3 Review method .....	9
<b>3. TET's review in 2023</b> .....	<b>14</b>
3.1 Summary of TET's review in 2023 .....	14
3.2 Review of CFCS in 2023 .....	16
3.2.1 Review of CFCS' processing of information in its communication systems .....	16
3.2.2 Reviews of CFCS' processing of information in separate IT environments and analytical tools .....	16
3.2.3 Review of CFCS' processing of information on drives .....	17
3.2.4 Review of CFCS' processing of information in other systems .....	17
3.2.5 Review of CFCS' sharing of information with the other part of DDIS .....	17
3.2.6 Review of CFCS' internal compliance review .....	18
3.2.7 Follow-up on TET's reviews of CFCS in 2022 .....	18
3.2.8 TET's technical reviews and mapping of CFCS' IT landscape .....	18
3.3 CFCS' processing times in 2023 .....	19
3.4 Cases submitted to the Minister of Defence for a decision .....	19
<b>4. Examples of CFCS' handling of cyber attacks</b> .....	<b>23</b>
<b>5. Statistical data on CFCS' processing of information</b> .....	<b>25</b>

---

## APPENDIX

<b>1. About Danish Centre for Cyber Security</b> .....	<b>27</b>
<b>2. About Danish Intelligence Oversight Board (TET)</b> .....	<b>28</b>
2.1 TET's duties in relation to CFCS .....	29
2.2 TET's access to information held by CFCS .....	30
2.3 Responses available to TET .....	30
<b>3. Legal framework</b> .....	<b>32</b>
3.1 The CFCS Network Security Service .....	32
3.1.1 About the CFCS Network Security Service, see section 3 of the CFCS Act .....	32
3.2 Interception of communications and court-ordered disclosure .....	33
3.2.1 About interception of communications, see sections 4-6c of the CFCS Act .....	33
3.2.2 About court-ordered disclosure, see section 7 of the CFCS Act .....	34
3.3 Processing of personal information .....	34
3.3.1 About processing of personal information, see sections 9-14 of the CFCS Act .....	34
3.3.2 About security measures in connection with CFCS' processing of personal information, see section 18 of the CFCS Act .....	36
3.4 Analysis and deletion of data falling within the scope of Part 4 of the CFCS Act .....	36
3.4.1 About analysis of data, see section 15 of the CFCS Act .....	36
3.4.2 About deletion of data, see section 17 of the CFCS Act .....	37
3.5 Disclosure and sharing of information falling within the scope of Part 4 of the CFCS Act ...	39
3.5.1 About disclosure, see section 16 of the CFCS Act .....	39
3.5.2 About sharing of data with DDIS, see section 2 of the CFCS Circular .....	40

# 1. 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 deletion by CFCS of the information procured.

TET's review activities contribute to the legitimisation of CFCS' activities by strengthening public confidence in the lawfulness of CFCS' activities. It is a prerequisite for effective and accurate compliance reviews that TET is given full, complete and timely access to CFCS' material relevant to TET's activities.

As will appear from this report, TET has in 2023 carried out in-depth and intensive compliance reviews with regard to CFCS. TET's reviews focused on 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 addition, in 2023, TET has intensified its international cooperation. The publication of TET's standards for its review activities over the past year has resulted in increased international interest in its methods for planning and performance of its review of intelligence services. TET has thus continued its multilateral and bilateral partnerships with similar foreign authorities. In particular, TET would like to single out the consolidation of the close cooperation with the Canadian *National Security and Intelligence Review Agency (NSIRA)*, which in 2023 resulted in a visit to the Canadian sister organisation where the focus was on mutual competence building and optimisation of review methods.

Moreover, together with its Norwegian and Swedish sister organisations, TET organised and hosted the annual *European Intelligence Oversight Conference 2023 (EIOC)*, and contributed with presentations at the *International Intelligence Oversight Forum (IIOF)* held in Washington DC in 2023.

In December 2023, the Government (Socialdemokratiet, Venstre and Moderaterne) and Socialistisk Folkeparti entered into an Agreement on Strengthening the Danish Intelligence Oversight Board (TET) and on Investigating Certain Specific Cases, which, following the conclusion of a broad political agreement on strengthening TET in February 2024, has been implemented in a draft bill amending, among other things, the DSIS Act, which was sent for consultation with selected authorities and organisations by the Ministry of Justice on 11 March 2024. The Bill is expected to be adopted in the current parliamentary session.



# Generally about TET's review activities

## General prerequisites for TET's reviews and its expectations from DSIS, DDIS, CFCS and PPNR

The review activities of the Danish Intelligence Oversight Board (TET) contribute to the legitimisation of activities of the Danish Security and Intelligence Service (DSIS), the Danish Defence Intelligence Service (DDIS), the Danish Centre for Cyber Security (CFCS) and the Danish National Police PNR unit (PPNR) by strengthening public confidence in the lawfulness of these activities.

TET's activities are determined by law, including

- ▶ that TET, upon receipt of a complaint or of its own motion, reviews that DSIS, DDIS, CFCS and PPNR process personal information in compliance with applicable legislation,
- ▶ that TET may require DSIS, DDIS, CFCS and PPNR to provide any information and material of importance to its activities,
- ▶ that 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,
- ▶ that TET may require DSIS, DDIS, CFCS and PPNR to provide written statements on factual and legal matters of importance to TET's review activities,
- ▶ that DSIS, DDIS, CFCS or PPNR – if they decide not to comply with a recommendation issued by TET in exceptional cases – must without undue delay submit the matter to the Minister of Justice or the Minister of Defence for a decision,
- ▶ that TET must inform the Minister of Justice and the Minister of Defence of any matters which the Ministers ought to know in the opinion of TET, and
- ▶ that TET must submit annual reports on its activities, which must be published.

If DSIS, DDIS, CFCS or PPNR fail to fully comply with these basic prerequisites for effective and accurate reviews, it will significantly weaken TET's ability to review the legal compliance of DSIS, DDIS, CFCS and PPNR and thereby contribute to the agencies' legitimacy towards the public.

TET has the following expectations from DSIS, DDIS, CFCS and PPNR in the fulfilment of these requirements:

### TET's access to information

**TET expects** to be given unrestricted, full and timely access by DSIS, DDIS, CFCS and PPNR to all material that is relevant for TET to conduct a proper and effective compliance review.

**TET expects** DSIS, DDIS, CFCS and PPNR to ensure that TET has the right user access to the IT infrastructure of DSIS, DDIS, CFCS and PPNR, which ensures direct and unrestricted access to relevant information for TET's compliance reviews.

In the situations where, for technical reasons, full user rights cannot be given to selected parts of the IT infrastructure of DSIS, DDIS, CFCS or PPNR, TET expects to be informed about

- ▶ the nature and extent of the part of the IT infrastructure to which TET does not have direct access, and
- ▶ the nature and scope of data processed in the part of the IT infrastructure to which TET does not have direct access.

Unrestricted, full and timely access to material relevant to TET's activities is essential for effective and accurate compliance reviews.

DSIS, DDIS, CFCS or PPNR may in exceptional circumstances submit a statement on the omission of selected information from the compliance review. However, for purposes of compliance with TET's statutory right of access to information, only TET has the authority to decide whether selected information can be omitted from a review.

If TET is not able to verify that the information, which DSIS, DDIS, CFCS or PPNR wishes to omit from a compliance review, is not relevant to the review, this will constitute a significant risk of circumvention of the law.

## Response to TET's consultation questions

---

TET expects the responses from DSIS, DDIS, CFCS and PPNR to be complete, transparent and unqualified.

TET expects to be informed by DSIS, DDIS, CFCS and PPNR of the existence of any other information or material of relevance to the compliance review, which DSIS, DDIS, CFCS or PPNR may acknowledge that TET does not have access to.

TET expects the responses from DSIS, DDIS, CFCS and PPNR to be provided in a timely manner and within the timeframes set out in TET's process for consultation with DSIS, DDIS, CFCS and PPNR (see process for consultation with DSIS, DDIS, CFCS and PPNR in Standards for Danish intelligence review activities).

In order to ensure effective and accurate compliance reviews, TET issues targeted requests for statements on factual and legal matters of relevance to its review activities.

TET has the decision-making authority to decide whether selected information is relevant to the compliance review, for which reason the responses from DSIS, DDIS, CFCS and PPNR must be complete, transparent and unqualified.

Thus, when responding to TET's consultation questions, DSIS, DDIS, CFCS or PPNR may not independently assess whether selected requests for information are relevant to TET's compliance reviews.



## Follow-up on TET's reviews

---

If DSIS, DDIS, CFCS or PPNR have comments on the results of TET's individual reviews, TET expects to be in receipt of such comments within the deadline stated in TET's follow-up letter.

If DSIS, DDIS, CFCS or PPNR in exceptional cases decide not to comply with a recommendation issued by TET, TET expects DSIS, DDIS, CFCS or PPNR to fulfil their duty of disclosure and without undue delay submit the matter to the Minister of Justice or the Minister of Defence for decision.

Practices which TET has found to be unlawful, and where DSIS, DDIS, CFCS or PPNR agree, must be dealt with immediately, and disagreements about the interpretation of the legal basis should be resolved without undue delay. It is therefore crucial that DSIS, DDIS, CFCS or PPNR respond to TET's recommendations in a timely manner, including, if necessary, by submitting a given case to the Minister of Justice or the Minister of Defence for a decision.

## 2.2

## Scale for TET's comments

TET's comments are based on the following scale:

COMMENTS	BACKGROUND TO COMMENTS
»[...] <b>does not give rise to any comments</b> «	Used when TET agrees with the authority on how they are generally or specifically administering the law.
»On the information available, TET is <b>unable to assess</b> [...]«	Used when TET's review is limited by either factual or legal circumstances.
»TET finds it <b>striking</b> [...]«	Used for situations in the authority or legislation which do not quite match the general or immediate impression of an outsider.
»TET finds it <b>problematic</b> [...]«	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 has <b>identified</b> [...]«	Used for situations where actual non-compliance with legislation of an isolated nature or non-compliance with internal guidelines has been identified.
»TET finds it <b>criticisable</b> [...]«	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 <b>highly criticisable</b> [...]«	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 the authority having demonstrated a willingness to ensure the necessary remedial action.

## 2.3

### Review method

TET continuously works to improve the methods it uses in the planning and performance of its review of DSIS, DDIS, CFCS and PPNR in order for the review to be as effective as possible within the framework set for the work of TET.

TET's compliance review of the DSIS, DDIS, CFCS and PPNR requires knowledge of the agencies' IT infrastructure, prioritisation of the oversight resources and effective methods for carrying out the review.

TET is only able to review the parts of DSIS, DDIS, CFCS and PPNR of which that is aware. Furthermore, TET does not have the resources to perform a full review of all parts of DSIS, DDIS, CFCS and PPNR. Finally, TET's reviews must be able to document the conditions in DSIS, DDIS, CFCS and PPNR using a limited amount of resources.

TET's standards aim to address these fundamental challenges. For this purpose, TET's work consists of three main elements:



TET's **1** mapping of IT infrastructure in DSIS, DDIS, CFCS and PPNR, respectively, aims to provide TET with the necessary knowledge of the procurement, the processing and the disclosure of information in DSIS, DDIS, CFCS and PPNR.

TET compiles and assesses information about relevant parts of the IT infrastructure in order to create the right basis for performing complete risk and materiality assessments of all processes and systems in DSIS, DDIS, CFCS and PPNR.

TET's methodology for mapping IT infrastructure is self-developed. The method is a further development of TET's initial mapping of IT systems in DSIS and DDIS in 2014-2015, which has prompted a need for both adjustment, structuring and formalisation of the methodology.

The selection of methodology reflects a trade-off between the need for technical detail in mapping to support TET's review activities, the extent of IT resources, and the IT governance maturity level within TET as well as DSIS, DDIS, CFCS and PPNR.

TET's **2** planning of compliance reviews for the coming year aims to prioritise TET's resources so that the reviews are directed at those parts of DSIS, DDIS, CFCS and PPNR assessed to pose the greatest risk of non-compliance with legislation.

The planning is based on an annual risk and materiality assessment of processes and systems (hereinafter referred to as "review subjects") in DSIS, DDIS, CFCS and PPNR for the purpose of assessing the risk of non-compliance with legislation. On this basis, TET prepares risk analyses that makes the foundation for the selection of reviews in the coming year. The selected reviews are summarised in review plans for DSIS, DDIS, CFCS and PPNR for the coming year.

The purpose of the risk analyses is to ensure that TET's reviews are focused on areas, which pose the greatest risk of non-compliance with legislation. In addition, other relevant factors are taken into account, for example, review areas given special weight by the legislature such as the rules on legitimate political activity.

Review areas assessed to pose a lower risk of non-compliance with legislation are generally reviewed every five years in order to ensure completeness in reviewing DSIS, DDIS, CFCS and PPNR. In addition, this measure intends to ensure that the assessment of the risk of non-compliance with legislation in the area remains accurate.

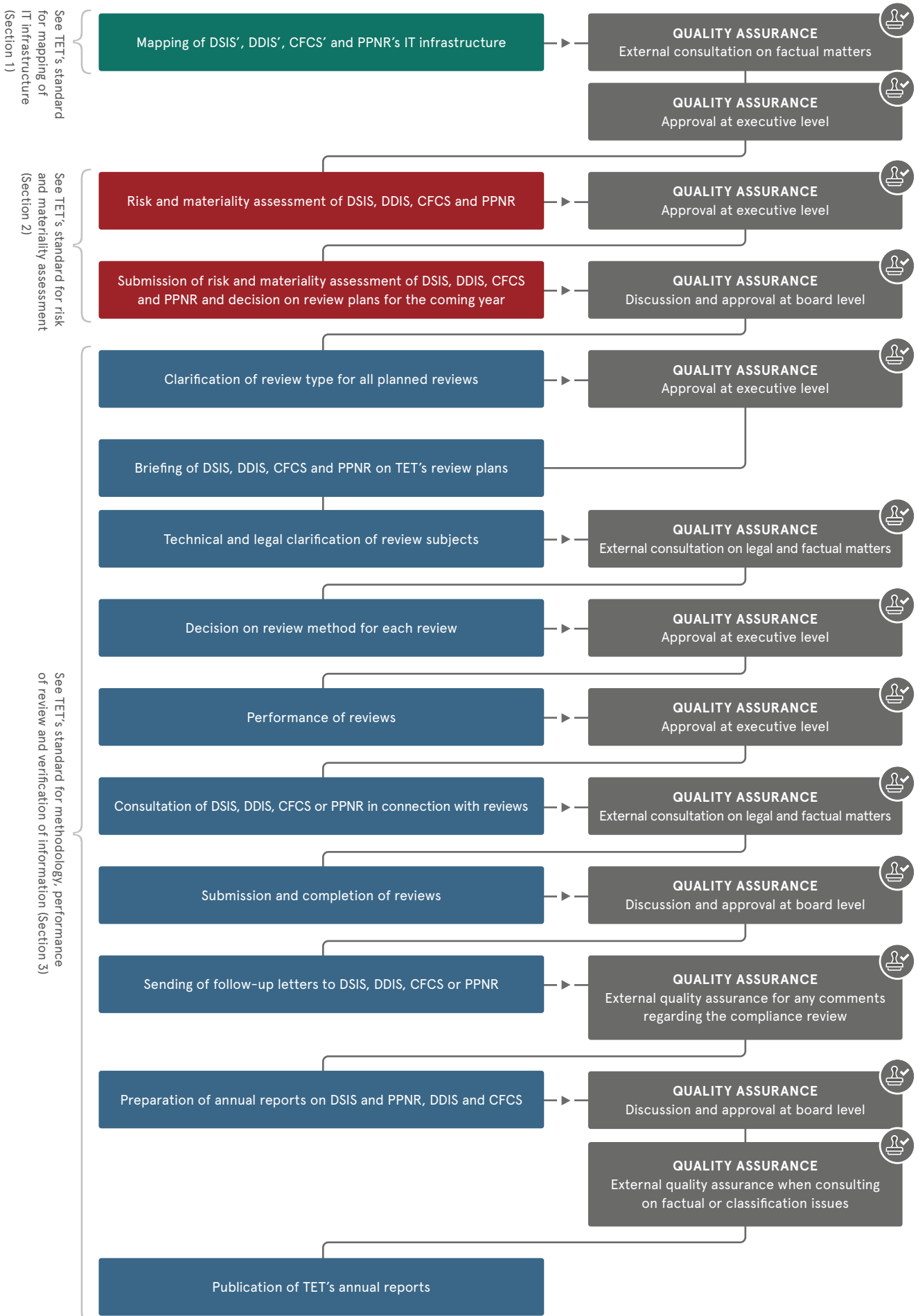
TET's reviews **3** are carried out throughout the year based on the review plans applicable to DSIS, DDIS, CFCS and PPNR, respectively. TET does not determine methods for individual reviews in connection with the preparation of risk assessments and analyses. As such, the selection of method is determined prior to initiating a specific review.

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

TET's selection methodology of review is based on a specific risk assessment of the review subject, experience from previous reviews and TET's findings in connection with the specific review. In that connection, prior to reviewing subjects not previously reviewed, TET holds a start-up meeting with relevant DSIS, DDIS, CFCS and PPNR employees in order to ensure an adequate police and/or intelligence professional and technical understanding of the subject, which will enable the reviews to be adjusted and adequately performed.

As part of TET's performance of reviews, verification reviews are also carried out on the IT infrastructure of DSIS, DDIS, CFCS and PPNR. The purpose of the verification is to ensure that TET's reviews are based on data from DSIS, DDIS, CFCS and PPNR the accuracy of which has been verified by TET.

The process for TET's **1** mapping, **2** planning **3** performance and verification of its reviews is illustrated in the below figure. The processes are supported by ongoing quality assurance by approval at executive and board levels, respectively, and by consultation with external parties on legal, factual or classification related matters.



TET's direct access to DSIS', DDIS', CFCS' and PPNR's systems prevents the agencies from predicting which files and data will be subjected to reviews by TET. However, TET may sometimes have to notify DSIS, DDIS, CFCS or PPNR 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 analyses and review plans with DSIS, DDIS, CFCS and PPNR for the purpose of ensuring, among other things, openness about TET's assessment of the situation at each of the agencies. The openness also allows DSIS, DDIS, CFCS and PPNR to take into account TET's reviews in the organisation of the agencies' own internal compliance reviews, which contributes to TET's reviews and their internal compliance reviews collectively covering a larger part of the agencies' activities. Finally, the openness allows DSIS, DDIS, CFCS and PPNR to dedicate sufficient resources to serve TET.

Furthermore, TET prepares separate risk assessments and analyses specifically for TET's reviews in relation to DSIS and DDIS under the indirect subject access request system, among other things for the purpose of ensuring that TET's reviews in connection with indirect subject access requests are effective and relevant.

For further information on TET's review methods, please consult the published standards on Danish intelligence review activities available on TET's website.





# TET's review in 2023



## 3.1

### Summary of TET's review in 2023

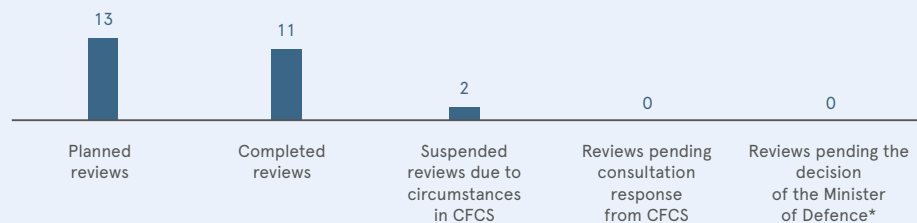
In 2023, the Danish Intelligence Oversight Board (TET) has completed 11 out of 13 planned reviews of the Danish Centre for Cyber Security (CFCS).

The result of TET's reviews is described in full in section 3.2. The central and fundamentally important parts of the report are emphasised below.

- ▶ None of the 11 reviews of CFCS gave rise to any comments.
- ▶ TET decided to suspend two planned reviews of CFCS' drive structures in 2023, as a solution enabling searches in the content of the drive structures was still not in place.

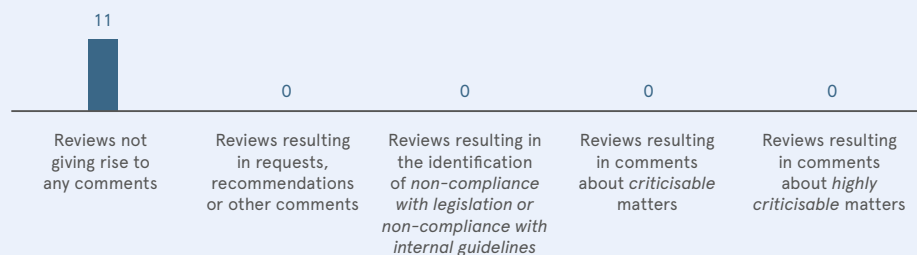
In TET's assessment, CFCS had in 2023 taken any possible steps to promote the establishment of the solution and that the delay was due to challenges with external deliverables (section 3.2.3).

#### TET's review of CFCS in 2023



\* But see section 3.4

#### Results of TET's review of CFCS in 2023



---

## 3.2

### Review of CFCS in 2023

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 2023 of CFCS':

- ▶ processing of information in communication systems (section 3.2.1),
- ▶ processing of information in separate IT environments and analytical tools (section 3.2.2),
- ▶ processing of information on drives (section 3.2.3),
- ▶ processing of information in other systems (section 3.2.4),
- ▶ sharing of information with other parts of DDIS (section 3.2.5), and
- ▶ internal compliance review (3.2.6).

Furthermore, in 2023, TET has

- ▶ followed up on TET's reviews of CFCS in 2022 (section 3.2.7), and
- ▶ completed technical reviews and mapping of CFCS' IT landscape (section 3.2.8).

#### 3.2.1

---

##### Review of CFCS' processing of information in its communication systems

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.

CFCS uses communication systems to disclose information to relevant external partners, as well as government authorities and businesses forming part of CFCS' sensor network.

CFCS also uses various communication or email systems that enable employees in different parts of CFCS to exchange information.

In 2023, TET carried out a review of CFCS' processing of data in three communication systems. TET's review focused on information falling within the scope of Part 4 of the CFCS Act and which should have been deleted at the time of TET's review, see section 17(2) of the CFCS Act.

##### Comments by TET

TET's review of CFCS' processing of information in its communication systems did not give rise to any comments.

#### 3.2.2

---

##### 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 2023, TET carried out compliance reviews with regard to CFCS' processing of information in three analytical tools.

#### Comments by TET

TET's review of CFCS' processing of information in separate IT environments and analytical tools in 2023 did not give rise to any comments.

### 3.2.3

#### Review of CFCS' processing of information on drives

---

CFCS uses drives to store information for many different parts of its operations.

In 2023, TET planned to perform two compliance reviews of different CFCS drive structures.

#### Comments by TET

TET decided to suspend two planned reviews of CFCS' drive structures in 2023, as there was still no solution in place to enable searching the content of the drive structures.

In TET's assessment, CFCS had in 2023 taken any possible steps to promote the establishment of the solution and that the delay was due to challenges with external deliverables.

TET's other reviews of CFCS' processing of information on drives in 2023 did not give rise to any comments.

### 3.2.4

#### Review 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, work stations, etc.

In 2023, TET carried out compliance reviews with regard to CFCS' processing of information in other systems by reviewing CFCS workstations.

#### Comments by TET

TET's review of CFCS' processing of information in other systems in 2023 did not give rise to any comments.

### 3.2.5

#### Review of CFCS' sharing of information with the other part of DDIS

---

Organisationally, CFCS forms part of DDIS, and internal sharing between CFCS and the other part of DDIS of information falling within the scope of Part 4 of the CFCS Act 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 from CFCS to DDIS of information falling within the scope of Part 4 of the CFCS Act.

In 2023, TET carried out a review of CFCS' sharing of information with the other part of DDIS.

## Comments by TET

The review carried out by TET of CFCS' sharing in 2023 with the other part of DDIS of information falling within the scope of Part 4 of the CFCS Act did not give rise to any comments.

### 3.2.6

#### Review of CFCS' internal compliance review

---

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

In 2023, TET carried out a review of CFCS' internal compliance review. The review comprised CFCS' internal compliance reviews in 2022 and CFCS' planning thereof for 2023.

In September 2023, CFCS informed TET about its

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

In addition, in 2023, CFCS regularly informed TET about its internal compliance review.

## Comments by TET

TET's review of CFCS' internal compliance review in 2023 does not give rise to any comments.

### 3.2.7

#### Follow-up on TET's reviews of CFCS in 2022

---

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

In 2023, TET followed up on its reviews of CFCS in 2022.

TET reviewed the information, which CFCS agreed to delete in connection with TET's reviews in 2022 as well as CFCS' follow-up on the requests and recommendations made by TET to CFCS on the basis of TET's reviews in 2022. The review was also carried out with a view to determining whether CFCS had made the changes that it had informed TET it would in connection with the reviews in 2022.

## Comments by TET

TET's follow-up on its reviews of CFCS in 2022 did not rise to any comments.

### 3.2.8

#### 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 2023 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 review of CFCS that TET has knowledge of CFCS' overall IT infrastructure so that its review can be targeted at the parts of the infrastructure, which pose the greatest risk of processing in violation of CFCS legislation.

In 2023, TET performed validation reviews and inspections of CFCS' IT infrastructure by mapping CFCS' server infrastructure.

#### Comments by TET

TET's mapping of CFCS' server infrastructure in 2023 did not rise to any comments..

---

### 3.3

#### CFCS' processing times in 2023

In 2023, TET submitted seven consultation questions 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 five working days.

---

### 3.4

#### Cases submitted to the Minister of Defence for decision

As part of its review of CFCS, TET may issue statements to CFCS in which TET may, among other things, express its opinion on whether CFCS complies with the rules of the CFCS Act.

At the end of each compliance review, TET issues a statement to CFCS describing the results of the review. The statement may also contain a description of one or more measures, which CFCS should take in TET's opinion. If CFCS decides not to comply with a recommendation issued by TET in exceptional cases, CFCS must notify TET and without undue delay submit the matter to the Minister of Defence for a decision. The responses available to TET towards CFCS are described in more detail in section 2.3 of the Appendix and in section 21 of the CFCS Act.

The following table provides an overview of cases submitted to the Minister of Defence since TET was established in 2014:

QUESTION	DATE OF SUBMISSION	STATUS
<p>Whether CFCS, in connection with its compliance with section 18 of the CFCS Act, is obliged to assess for each of its systems which measures can provide an adequate level of security.</p> <p>Discussed in more detail in TET's annual report for 2022 (section 2.2.7).</p>	4 August 2023	Awaiting the decision of the Minister of Defence.
<p>Whether the Minister of Defence's decision of 11 August 2021 regarding deletion of data from CFCS' sensor network only applies when sensor data is stored in the alarm devices and CFCS' central analysis platform, or applies in all cases where CFCS stores sensor data in relevant processing systems, for example locally on an employee's workstation.</p> <p>Discussed in more detail in TET's annual report for 2022 (section 2.2.3).</p>	1 August 2023	Awaiting the decision of the Minister of Defence.
<p>Whether data from CFCS' sensor network must be deleted immediately after the review of the specific incident that caused the obtaining has been completed in accordance with section 17(1) of the CFCS Act.</p> <p>Discussed in more detail in TET's annual report for 2021 (section 2).</p>	11 August 2020	<p>Decided on 11 August 2021.</p> <p>The Minister of Defence found that section 17(1) of the CFCS Act has a very limited scope in relation to sensor data. The primary scope of the provision is, however, the other types of data covered by Part 4 of the CFCS Act, such as stationary data obtained in accordance with section 5 of the CFCS Act. Stationary data includes data that is stored on servers, storage devices, mobile devices, etc., and which, unlike sensor data, does not constitute communication between networks.</p>



# 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 2023:

CFCS is tasked with protecting the important parts of Danish society against cyber attacks. In practice, this task is carried out by CFCS 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. In addition to data from the sensor network and commercially procured and openly available data, CFCS also makes use of information generated through DDIS' international intelligence activities.

In 2023, CFCS handled a large number of IT security incidents for public authorities and private business in and outside the sensor network. Incidents included systematic exploitation of known or previously unknown vulnerabilities, data leaks, reconnaissance, spear phishing and brute forcing attempts. Some of the events also included compromises in the form of espionage and data theft as well as ransomware attacks resulting in data encryption. In 2023, CFCS has observed attacks and attempted attacks from both state-sponsored and criminal cyber players.

Attempted phishing attacks continue to be 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 continuously observes various types of attempts to exploit misconfigurations and publicly known vulnerabilities in software services exposed to the internet.

# 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 2023:

<b>TABLE 1. DISCLOSURE AND SHARING OF INFORMATION</b>	<b>2023</b>
Disclosure of information	29
Sharing of information	16
<b>Total</b>	<b>45</b>

<b>TABLE 2 CONFIRMED SECURITY INCIDENTS* ACCORDING TO SEVERITY</b>	<b>2023</b>
Serious	2
Major	8
Moderate	12
Minor	193
None**	993
False positives***	1.256
<b>Total</b>	<b>2.464</b>

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

\*\* The category "None" includes all the security incidents that have not had an impact on the customer

\*\*\* False positives are suspected security incidents which, upon further analysis, turn out not to be a security incident.

<b>TABLE 3 SUBJECT ACCESS REQUESTS</b>	<b>2023</b>
Full access requested	10
Partial access requested	5
Requests refused	3
No documents located to grant or refuse access	4
<b>Total</b>	<b>22</b>

<b>TABLE 4 COMPLAINTS ABOUT PERSONAL INFORMATION PROCESSING</b>	<b>2023</b>
Complaints to CFCS about the processing of personal data	0*
Complaints received by TET	0

\* CFCS is not aware of any complaints received about its personal information processing.

# Appendix

# 1. ABOUT DANISH CENTRE FOR CYBER SECURITY (CFCS)

Danish 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 reviewing 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 reviews 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 reviewing 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 deletion of personal information. With the Act, it is further established that the Danish Intelligence Oversight Board (TET) – which is an independent monitoring body charged with reviewing DSIS and DDIS – is also charged with reviewing 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.

## 2. ABOUT DANISH INTELLIGENCE OVERSIGHT BOARD (TET)

### TET'S ACTIVITIES

Staffing in 2023 (employees)	8
Budget appropriation in 2023 (DKK million)	10,1

The Danish Intelligence Oversight Board (TET) is an independent monitoring body charged with reviewing that the Danish Security and Intelligence Service (DSIS), the Danish Defence Intelligence Service (DDIS), the Danish Centre for Cyber Security (CFCS) and the Danish National Police PNR unit (PPNR) process personal information in compliance with DSIS, DDIS, CFCS and PPNR legislation.

TET is completely autonomous and is thus not subject to the directions of the Ministry of Justice, 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.

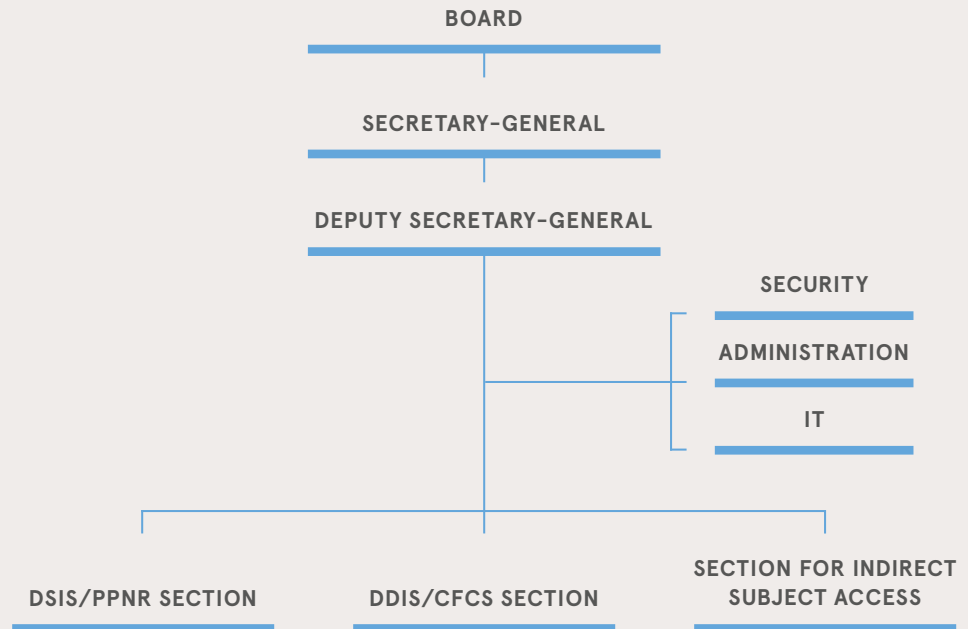
TET had the following members as at the end of 2023:

- ▶ 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 established 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 2023, 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.

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



## 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 deletion of data, and
- ▶ the requirements to security measures in connection with CFCS' processing of personal information.

TET must review 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 review, including whether to perform full review or random reviews, 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 review functions.

---

## 2.2 TET's access to information held by CFCS

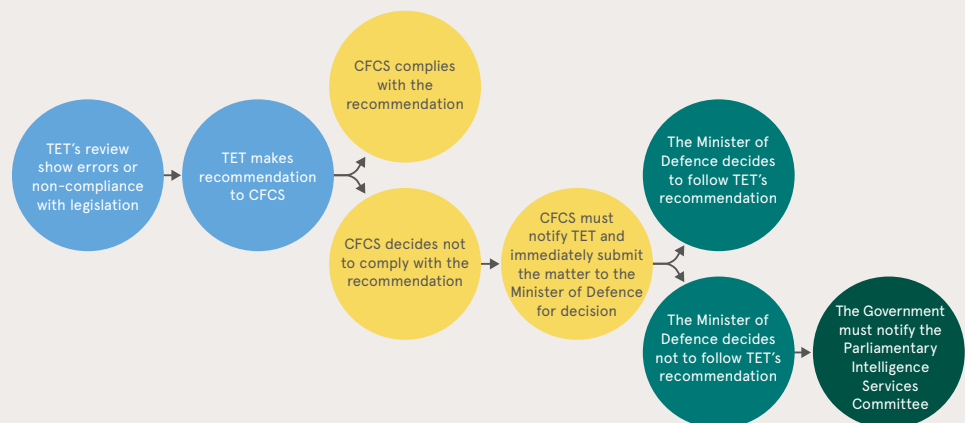
TET may require CFCS to provide any information and material of importance to TET's activities, and TET is entitled at any time to access any premises where the information being processed may be accessed or where technical facilities are being used. TET may furthermore require CFCS to provide written statements on factual and legal matters of importance to TET's review 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 information. At the end of each compliance review, TET submits a statement to CFCS describing the results of the review. The statement may also contain a description of one or more measures, which CFCS should take in TET's opinion. If CFCS decides not to comply with a recommendation issued by TET in exceptional cases, CFCS must notify TET and without undue delay submit the matter to the Minister of Defence for a decision.



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 made available to the public, provides general information about the nature of the review 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 review 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 annual report on its activities to the Minister of Defence in June 2023. The annual report was published in November 2023.

## 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 delete 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 deletion 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 reviews 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 deleted 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 deletion 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 deletion 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 review 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 deletion 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 deleted 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 deletion 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 deleted 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 deleted 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 review – assessed the bearing of section 17(1) of the CFCS Act on CFCS’ obligation to delete 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 deleted 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 deleted under the absolute time limits for deletion 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 deletion 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 deleted 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 deleted 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 deleted without undue delay.

In exceptional circumstances, the above deletion 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 deleted 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 2023**

Danish Centre for Cyber Security

Published by the Danish Intelligence Oversight Board, May 2024

Layout + illustrations: Eckardt ApS

Portrait photographs: Lars Engelgaard / Sophie Kalckar

The publication is available on TET's website at [www.tet.dk](http://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](http://www.tet.dk)