Report 2025

Danish Defence Intelligence Service

tet

Danish Intelligence Oversight Board

To the Minister of Defence

In accordance with section 19 of the Act on the Danish Defence Intelligence Service (DDIS) (Consolidated Act No. 1287 of 28 November 2017, as most recently amended by Act No. 1706 of 27 December 2018) and section 24 of the Act on the Danish Centre for Cyber Security (CFCS) (Consolidated Act No. 836 of 7 August 2019), the Danish Intelligence Oversight Board (TET) hereby submits its report on its activities concerning DDIS for 2025.

The report shall be submitted to the Parliamentary Intelligence Services Committee (UET) and shall subsequently be made public.

The purpose of the report is to provide general information about the nature of the review exercised over DDIS.

The report includes, inter alia, information about the matters which TET has chosen to focus on, and the number of cases in which TET has found that DDIS's processing of personal data was not in compliance with the rules.

TET also reviews the Danish National Police PNR Unit (the PNR Unit), including when the PNR Unit processes information on behalf of DDIS. TET's review of the PNR Unit is addressed in TET's report concerning the review of the Danish Security and Intelligence Service (DSIS) in 2025.

Danish Intelligence Oversight Board

Copenhagen, May 2026

Contents

1. Introductory comments

In 2025, following negotiations with the Minister of Defence and on the basis of discussions with the Parliamentary Intelligence Services Committee (UET), the Minister of Justice appointed five new members of the Danish Intelligence Oversight Board (TET) as a consequence of the entry into force of Act No. 666 of 11 June 2024 on strengthening oversight of the intelligence services.

In 2025, TET conducted a review of the Danish Defence Intelligence Service's (DDIS) processing of information concerning persons resident in Denmark within the framework set out in the applicable legislation.

TET has at the same time continued and strengthened its international cooperation with corresponding oversight authorities abroad. The international cooperation contributes to the exchange of experience and methodological development and supports TET's work to ensure that oversight of the Danish intelligence services is carried out in accordance with recognised international standards for oversight.

In 2025, TET has, among other things, hosted a meeting of the Intelligence Oversight Working Group (IOWG), which comprises oversight authorities in Belgium, Canada, the Netherlands, Norway, Switzerland, Sweden and the United Kingdom. Furthermore, in 2025, TET has further developed its close cooperation with the Canadian oversight body, the National Security and Intelligence Review Agency (NSIRA). In this connection, TET has had an employee seconded to the Canadian oversight body for a period in order to obtain experience and inspiration which can be used in the continued development of TET's working methods.

Of significance for TET's activities in 2025, it was determined by Royal Resolution of 28 August 2024 that the Danish Centre for Cyber Security (CFCS) - in addition to the Network Security Service and the other parts of CFCS which carry out the operational defensive cyber effort and tasks concerning the Danish Armed Forces - was transferred to the Ministry of Resilience and Preparedness (MSSB). The parts of CFCS which were transferred to MSSB became part of the Danish Resilience Agency (SAMSIK) at the beginning of 2025.

The Ministry of Defence and MSSB have decided that TET shall continue to review the application of the CFCS Act by DDIS, whereas TET will not review the processing of data by SAMSIK.

TET will therefore not submit a separate report to the Minister of Defence for 2025 concerning its review of CFCS, but will submit a consolidated report concerning TET's review of DDIS, covering the service's obligations under both the DDIS Act and the CFCS Act.

TET emphasises that effective intelligence activities and independent review are not opposites. A strong and independent review contributes to enabling the Danish Parliament and the public to have confidence that the activities of the intelligence services are conducted within the framework of the law and with respect for citizens' fundamental rights.

Lars Bay Larsen (Chair)

Gitte Lillelund Bech (Deputy Chair)

Anne Hedensted Steffensen (Member)

Pernille Knudsen (Member)

Rasmus Blaabjerg (Member)

2. TET's review activities in 2025

2.1 Summary of TET's reviews in 2025

In 2025, the Danish Intelligence Oversight Board (TET) completed 16 reviews of the Danish Defence Intelligence Service (DDIS). Of these, five reviews concerned DDIS's activities pursuant to the CFCS Act.

The results of TET's reviews are described in full in section 2.2. The following highlights central and principal elements of the report.

TET's review is risk-based, which means that TET directs its reviews at those parts of DDIS's activities where there is considered to be the greatest risk of errors, seen in relation to the degree of harm which possible errors are considered capable of causing to natural and legal persons, and whether possible errors are of a nature that may affect public confidence in the service. This also means that large parts of DDIS's activities have not been subject to review, as TET's assessment is that the service observes the provisions of the legislation in those areas. The report should be read in this light. It should also be emphasised that, in all the reviews in which non-compliance with the rules has been identified in the current year, DDIS has indicated that the service will initiate or has initiated measures to remedy the circumstances.

It should be noted that the references below constitute only a limited extract of TET's review of DDIS in 2025. For the full picture of TET's review of DDIS, the report should be read in its entirety.

- 12 out of 16 reviews of DDIS did not give rise to any comments. No reviews gave rise to comments concerning highly criticisable matters.

- TET found it criticisable that DDIS had not previously taken measures to ensure that information in a folder in one of the service's drive structures is deleted in accordance with section 6(1) of the DDIS Act. TET's assessment was based in particular on the volume of information in the folder concerned, the special nature of the information, the age of the information and the length of time for which the folder had been in use (section 2.2.5).

In connection with the review, TET found that DDIS was not currently able to ensure that information in the folder is deleted in accordance with section 6(1) of the DDIS Act.

TET found it positive that DDIS had initiated mitigating measures with a view to improving the possibilities of ensuring compliance with the rules of the DDIS Act, and that the service was working on a new technical solution for storing the information concerned.

- TET found it criticisable that, in 28 cases, DDIS processed information concerning persons resident in Denmark in a pre-production environment in contravention of section 6(1) of the DDIS Act (section 2.2.6).

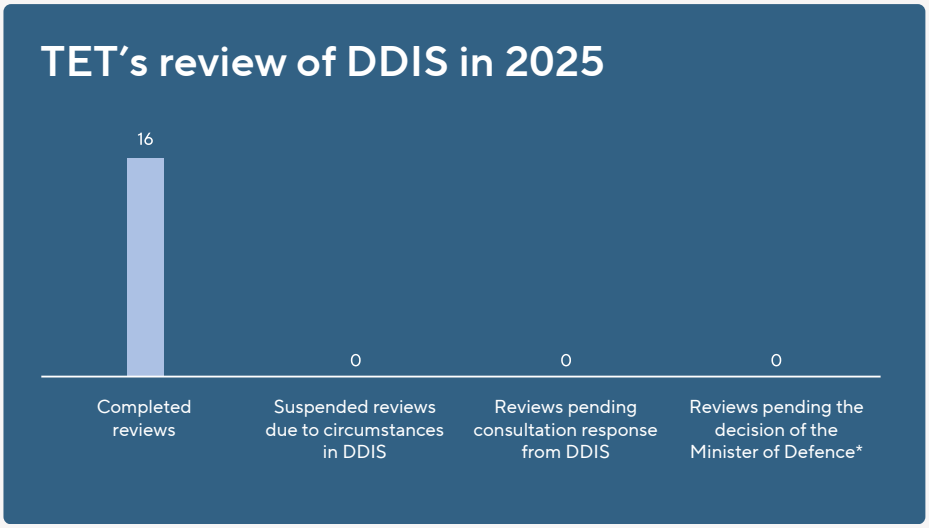
  The information was identical to information which DDIS had deleted on the basis of TET's review of the corresponding production environment in 2024. However, owing to an error in the deletion process, the deletion in the production environment had not been followed by a corresponding deletion in the pre-production environment.

- TET assessed that, in connection with the implementation of DDIS's decision to close the service's sensor network, there was an increased risk of non-compliance with section 17 of the CFCS Act. However, TET assessed that the implementation did not in itself entail non-compliance with the rules of the CFCS Act (section 2.2.9).

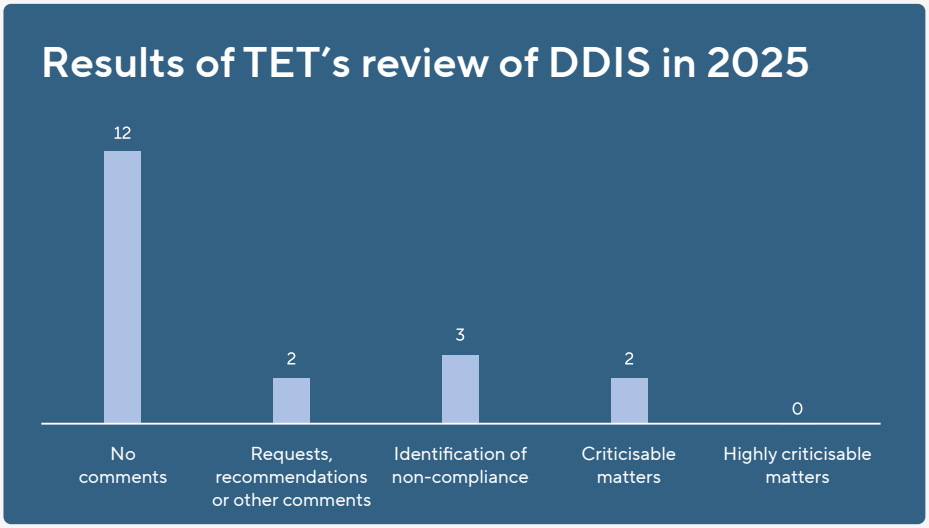
  TET recommended that DDIS ensure as quickly as possible that data on the sensor network probes was deleted in accordance with the rules of the CFCS Act.

- In 2025, TET processed requests from 20 natural or legal persons asking TET to examine whether DDIS was unlawfully processing information about them. In that connection, TET found that in 17 cases DDIS was not unlawfully processing information about the persons concerned.

  In three cases, DDIS processed information about the persons concerned which no longer met the conditions for processing in section 4(1) or section 5(1) of the DDIS Act. On that basis, DDIS deleted the information. In this connection, it should be noted that DDIS is not obliged, on its own initiative and on an ongoing basis, to review the service's cases and documents, etc., in order to assess whether the above-mentioned conditions for processing continue to be met (section 2.4).



*see section 2.6



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

2.2 Completed reviews of DDIS in 2025

For the purpose of reviewing whether DDIS, in connection with its processing of information concerning natural and legal persons resident in Denmark, complies with the rules set out in the DDIS Act, TET in 2025 reviewed the service's

- targeted intelligence obtaining using SIGINT (section 2.2.1),
- handling of raw data (section 2.2.2),
- searches in raw data (section 2.2.3),

- compliance with the rules on processing information concerning legal political activities (section 2.2.4),
- deletion of information (section 2.2.5),
- processing of information in pre-production environments (section 2.2.6),
- processing of information on workstations (section 2.2.7),
- disclosure of information (section 2.2.8),
- procurement and processing of information pursuant to the CFCS Act (section 2.2.9), and
- internal compliance review (section 2.2.10).

Furthermore, in 2025, TET performed

- follow-up on TET's review of DDIS and CFCS in 2024 (section 2.2.11), and
- technical investigations and mapping of the service's IT infrastructure (section 2.2.12).

2.2.1 Review of DDIS's targeted intelligence obtaining using SIGINT

TET carried out a review in 2025 of two of DDIS's systems for targeted intelligence obtaining. TET also reviewed whether DDIS has established sufficient measures to avoid inadvertently carrying out targeted intelligence obtaining directed at persons resident in Denmark.

What is SIGINT?

SIGINT stands for Signals Intelligence, which is electronic obtaining of data transfers between computer networks, telecommunications, etc. Electronic obtaining takes place, for example, from permanent intelligence obtaining facilities that obtain communications from satellites. It may also involve intelligence obtaining facilities set up abroad that can be controlled remotely from Denmark. Communications are obtained while they are in transit, without affecting the transmission and without the parties concerned discovering that their communication is being intercepted.

SIGINT requires large IT systems to process the material obtained and is technically complex. This is because the volume of communication is increasing at a very high rate while new technologies are constantly being developed.

Conditions for targeted obtaining using SIGINT
When carrying out targeted obtaining of information using SIGINT, DDIS must comply with the rules of the DDIS Act on obtaining information. Obtaining directed at a natural or legal person resident in Denmark must take place on

the basis of a court order obtained by DDIS, see section 3(3) of the DDIS Act, or at the request of the Danish Security and Intelligence Service (DSIS) on the basis of a court order obtained by DSIS. In these cases, the obtaining must always be carried out within the framework set out in the court order.

Obtaining under section 3(3) of the DDIS Act is conditional on the person concerned being located abroad and on there being specific reasons to believe that the person is participating in activities that may involve or increase a terrorist threat against Denmark and Danish interests.

Comments by TET

The review of DDIS's targeted intelligence obtaining in 2025 did not give rise to any comments.

2.2.2 Review of DDIS's handling of raw data

TET carried out a review in 2025 of a system used by DDIS for storing raw data and of the service's storage of raw data procured through two network operations (CNO) initiated by DDIS before 2011.

What is raw data?

Through electronic obtaining, DDIS procures very large quantities of unprocessed data (raw data).

Raw data is characterised by the fact that, until the data is processed, it is not possible to determine what information is contained therein.

DDIS has the possibility of extracting information from raw data by searching it, for example for information concerning specific selectors, such as telephone numbers and email addresses. The processing rules of the DDIS Act do not otherwise apply to raw data until such data has been processed and can therefore no longer be categorised as raw data.

Raw data must be deleted by DDIS no later than 15 years after the time of obtaining, see section 6(2) of the DDIS Act.

What is the significance of time stamping of raw data?

It is crucial that raw data, during and after obtaining, is handled in such a way

as to ensure the integrity of the information contained therein, including in particular that the time stamping of raw data is correct. Correct time stamping of raw data means that DDIS may search or delete raw data in accordance with section 3(3), cf. section 3a(3), and section 6(2) of the DDIS Act, respectively.

When DDIS obtains raw data, the data will typically contain a time stamp indicating when the raw data in question was procured.

Time stamping of raw data is relevant to how DDIS can ensure that the service complies with the rules of the DDIS Act on searches in raw data and deletion of raw data.

DDIS's activities are directed at conditions abroad, and, as a general rule, searches in raw data directed at persons resident in Denmark are therefore not carried out.

Where DDIS nevertheless, in certain cases, searches raw data directed at persons resident in Denmark, this must always take place on the basis of a court order obtained by DDIS or DSIS. Court orders will often contain a specific period within which the intervention may be carried out.

In order to comply with the content of the court orders, DDIS will impose a time limitation on searches carried out on the basis of the court order.

If there are errors in the time stamping of the raw data searched, there will, however, be a risk that the search will display data which in reality concerns a period other than the one for which DDIS is authorised by the court order to search.

The time stamp will naturally form the starting point for assessing when raw data must be deleted pursuant to section 6(2) of the DDIS Act. If raw data does not have a reliable time stamp, doubt may arise as to how long the raw data in question may be stored.

Depending on the circumstances, it may nevertheless be possible to demonstrate by other means that DDIS complies with the time limit for deletion of raw data.

Computer Network Operations (CNO)

DDIS's network intelligence obtaining - referred to as Computer Network Exploitation (CNE) - is active electronic intelligence obtaining directed at computer networks, which typically requires an employee of the service to obtain access to closed internet forums, IT systems and computers.

DDIS supports the Danish Armed Forces with offensive military cyber operations - referred to as cyberattacks or Computer Network Attacks (CNA) - the purpose of which is to attack an adversary's digital infrastructure.

TET does not review DDIS's offensive military cyber operations, as the operations are carried out under the provisions of the Defence Act. TET may, however, review any processing of information concerning persons resident in Denmark and any handling of raw data that may be carried out by DDIS before or after the operation.

DDIS's network intelligence obtaining and military cyber operations are collectively referred to as network operations or Computer Network Operations (CNO).

Data procured by DDIS through CNO will in many cases be stored as raw data.

Comments by TET

The review of DDIS's handling of raw data in 2025 did not give rise to any comments.

2.2.3 Review of DDIS's searches in raw data

TET carried out a review in 2025 of two of DDIS's systems for searches in raw data.

When may DDIS search raw data?

DDIS may not, on its own initiative, search raw data if the result must be expected predominantly to be information about identifiable persons resident in Denmark, unless the search is conducted on the basis of a court order obtained by DDIS, see section 3(3) of the DDIS Act.

DDIS may also conduct searches in raw data at the request of DSIS on the basis of a court order obtained by DSIS. In these cases, the search in raw data must always be carried out within the framework set out in the court order. Searches in raw data on the basis of court orders which relate only to a specific period must, for example, be limited in time to that period only.

If DDIS searches raw data where the result must be expected predominantly to contain information about persons resident in Denmark, without the service having a lawful basis for the search, the search in question will be unlawful. Reasons why searches in raw data may be carried out unlawfully include lack of time limitation in accordance with court orders, failure to filter out Denmark-related selectors (for example telephone numbers) from a combined search using a longer list of selectors, typing errors or searches using selectors that are no longer used by a target person.

Comments by TET

The review of DDIS's searches in raw data in 2025 did not give rise to any comments.

2.2.4 Review of DDIS's processing of information concerning legal political activities

TET carried out a review in 2025 of DDIS's processing of information concerning legal political activities in one of the service's central systems.

Processing of information concerning legal political activities

Section 8(1) of the DDIS Act provides that the participation by a natural person resident in Denmark in legal political activity does not in itself warrant processing of information about that person by DDIS.

The prohibition on processing information concerning the exercise of legal political activities is not absolute. This is indicated by the wording "not in itself". DDIS may therefore process information about a person's legal political activities where other circumstances mean that the person is of interest to the service.

If the person concerned is already the subject of attention in connection with the performance of DDIS's tasks, DDIS may also process information about the person's legal political activities if such information is relevant to the investigation. This may, for example, involve a person using the exercise of political activities as a pretext for planning, preparing or carrying out espionage, terrorism or violent extremist activities.

DDIS must therefore, in each individual case, assess whether processing of information concerning legal political activities is justified by circumstances other than the exercise of those activities itself, and such an assessment will necessarily involve discretion.

DDIS may also process information about a person's political activities in order to clarify whether the political activity is lawful. If DDIS's investigations show that the political activity is lawful, the information must be deleted. This applies irrespective of the fact that the general time limit for deletion of such information under section 6 of the DDIS Act has not yet been reached.

DDIS's processing of information about the persons concerned must in all circumstances comply with the other rules of the DDIS Act.

Comments by TET

The review of DDIS's processing of information concerning legal political activities in 2025 did not give rise to any comments.

2.2.5 Review of DDIS's deletion of information

TET carried out a review in 2025 of DDIS's compliance with section 6(1) of the DDIS Act by reviewing the service's processing of information in three drive structures.

TET's review focused on information procured more than 15 years before TET's review and which TET assessed contained information about persons resident in Denmark.

A complex deletion rule

Section 6(1) of the DDIS Act reads as follows:

> *"Unless otherwise prescribed by law or provisions laid down pursuant to law, the Danish Defence Intelligence Service shall delete information about natural and legal persons resident in Denmark which has been procured as part of the Danish Defence Intelligence Service's activities pursuant to section 1(1) where no new information relating in substance to the same case has been procured within the past 15 years."*

In TET's opinion, the time limit for deletion in section 6(1) of the DDIS Act may in practice be extremely difficult for DDIS to observe, as compliance with the provision for each item of information in the service's systems requires an independent assessment of

1) whether the information has been procured as part of the service's intelligence-related activities pursuant to section 1(1) of the DDIS Act;

2) whether the person concerned is currently resident in Denmark; and

3) whether new information has subsequently been procured which relates in substance to the same case.

In relation to the first criterion, it will not always be clear whether an item of information has been procured by DDIS as an intelligence service, as a national security service in the defence area or as part of the service's other activities. Systems may be used to process information that serves several different purposes and will not necessarily support marking or categorisation of such information. This applies in particular to information procured before the entry into force of the DDIS Act on 1 January 2014, when the same distinction between DDIS's different purposes did not exist.

In relation to the second criterion, a person's status as resident in Denmark may change over time. Even if DDIS allocates resources to marking information concerning persons resident in Denmark, it will be difficult for the service to ensure correct marking of all information concerning persons resident in Denmark.

In relation to the third criterion, DDIS's processing of information takes place across many different types of systems, and the work has an analytical and technical complexity which rarely makes it meaningful to divide the work into cases in the manner known from other public authorities. It is therefore difficult to establish whether new information concerns an already existing case, as DDIS does not, as a general rule, work with cases in the classical sense.

The practical challenges which, in TET's opinion, are associated with observing the time limit for deletion in section 6(1) of the DDIS Act may partly be addressed by DDIS by supporting compliance with the provision in its systems to the greatest extent possible, including by ensuring relevant metadata on the service's information and centrally managed review across the service's IT infrastructure.

Comments by TET

The review of DDIS's deletion of information in 2025 showed the following:

- TET found that in two cases DDIS stored information concerning persons resident in Denmark in a drive structure in contravention of section 6(1) of the DDIS Act. In connection with the review, TET also found that in two cases DDIS processed information concerning persons resident in Denmark in one of the service's analysis tools in contravention of section 6(1) of the DDIS Act.

- TET found it criticisable that DDIS had not previously implemented measures to ensure that information in a folder in one of the service's drive structures is deleted in accordance with section 6(1) of the DDIS Act.

  In connection with the review, TET found that DDIS was not currently able to ensure that information in the folder is deleted in accordance with section 6(1) of the DDIS Act.

  In connection with the review, DDIS stated that it was the service's assessment that by far the majority of the information in the folder did not concern persons resident in Denmark.

  DDIS also stated that, in cases where the time limit for deletion under section 6(1) of the DDIS Act may have been reached, it is the service's immediate assessment that, to a predominant extent, the information will be copies of documents where DDIS, in connection with storing the original (the physical document), has decided to refrain from deleting the original, see section 6(3) of the DDIS Act.

  TET's assessment was based in particular on the volume of information in the folder concerned, the special nature of the information, the age of the information and the length of time for which the folder had been in use.

  In this connection, it should be noted that TET selected the area for review on the basis of an initial assessment that non-compliance with section 6(1) of the DDIS Act may have a significant consequence for the legal rights of a

natural or legal person and/or a significant consequence for public confidence in DDIS.

In connection with the review, DDIS stated that the service had already initiated mitigating measures before the review and had decided that further measures should be initiated. As a consequence of the review, these further measures were prioritised and accelerated by DDIS.

TET found it positive that DDIS had initiated mitigating measures with a view to improving the possibilities of ensuring compliance with the rules of the DDIS Act, and that the service was working on a new technical solution for storing the information concerned.

TET's other review of DDIS's deletion of information in 2025 did not give rise to any comments.

2.2.6 Review of DDIS's processing of information in pre-production environments

TET carried out a review in 2025 of DDIS's processing of information in one of the service's pre-production environments.

What is a pre-production environment?

DDIS develops and tests new software in pre-production environments in order to identify errors and unintended consequences without affecting the production environment. In some cases, data is copied from a production environment to the pre-production environment for the purpose of developing and testing the software.

If data from DDIS's production environments is used in testing and development of software in pre-production environments, the rules of the DDIS legislation also apply to that information.

Comments by TET

The review of DDIS's processing of information in pre-production environments in 2025 showed the following:

- TET found it criticisable that in a pre-production environment information concerning persons resident in Denmark was processed in 28 cases in contravention of section 6(1) of the DDIS Act, as the information was more than 15 years old and as the service did not know whether new information had been procured which related in substance to the same cases within the past 15 years.

  TET's assessment was based on the fact that the information was identical to information in the production environment which, already in connection

with TET's review in 2024, DDIS became aware should have been deleted pursuant to section 6(1) of the DDIS Act. However, owing to a process error, the deletion in the production environment had not been followed by a corresponding deletion in the pre-production environment.

In this connection, it should be noted that TET selected the area for review on the basis of an initial assessment that non-compliance with section 6(1) of the DDIS Act may have a significant consequence for the legal rights of a natural or legal person and/or a significant consequence for public confidence in DDIS.

DDIS has stated that, on the basis of the review, all 28 documents have been deleted from the pre-production environment. DDIS has also, as a result of the review, initiated measures to ensure that deletion of information in the production environment is also carried out in the pre-production environment.

2.2.7 Review of DDIS's processing of information on workstations

TET carried out a review in 2025 of a number of randomly selected workstations at DDIS.

Processing of information on workstations

TET's review of DDIS is primarily focused on the service's central systems for the procurement, processing and disclosure of information. However, DDIS employees may process information locally on individual employees' workstations, including on individual user accounts, devices and storage media, as well as on printouts or in handwritten form on paper.

Comments by TET

The review of workstations at DDIS in 2025 did not give rise to any comments.

2.2.8 Review of DDIS's disclosure of information

TET carried out a review in 2025 of DDIS's disclosure of information.

Disclosure of information

DDIS participates in bilateral and multilateral partnerships with foreign intelligence services, in which the services exchange information of an intelligence-related nature. The exchange of information on obtaining methods, technologies, capabilities and specific information takes place with a view

to DDIS ultimately receiving information from its partners which is widely included in the service's analyses and thereby in a significant proportion of the products prepared by the service.

DDIS also discloses information to national cooperation partners, for example DSIS and other authorities within the remit of the Ministry of Defence.

In connection with disclosure, DDIS uses various communication systems which often also enable processing of information, for example storage of incoming and outgoing communication in copy.

Comments by TET

The review of DDIS's disclosure of information in 2025 did not give rise to any comments.

2.2.9 Review of DDIS's procurement and processing of information pursuant to the CFCS Act

TET carried out a review in 2025 of DDIS's compliance with the CFCS Act in relation to the sensor network used by the service's Network Security Service. The review focused particularly on DDIS's plan for compliance with the rules of the CFCS Act in connection with implementation of the service's decision of 4 August 2025 to close the sensor network.

Furthermore, in 2025, TET reviewed DDIS's internal exchange of information covered by chapter 4 of the CFCS Act on interference with the secrecy of communications and reviewed DDIS's handling of external media which the service receives from external parties in connection with its activities pursuant to the CFCS Act.

The division of the former Danish Centre for Cyber Security

TET has previously carried out separate review of the Danish Centre for Cyber Security (CFCS). Until August 2024, CFCS was organisationally placed as part of DDIS, but the centre operated under a separate legal framework, the CFCS Act.

By Royal Resolution of 29 August 2024, CFCS was divided between the remits of the Ministry of Defence and the Ministry of Resilience and Preparedness, so that some of the centre's tasks were placed with the Danish Resilience Agency, while the Network Security Service and the parts of CFCS that carried out the defensive cyber effort and tasks concerning the Danish Armed Forces remained part of DDIS, where they are placed as part of the service's Cyber Sector.

The CFCS Act was not amended, and the Act regulates DDIS's performance of the tasks that remain with the service following the change of remit.

TET's review of DDIS's compliance with the rules of the CFCS Act is therefore included from 2025 as part of the consolidated report on the review of the service.

Comments by TET

The review of DDIS's procurement and processing of information pursuant to the CFCS Act showed the following:

- TET assessed that, in connection with the implementation of DDIS's decision to close the service's sensor network, there was an increased risk of non-compliance with section 17 of the CFCS Act. However, TET assessed that the implementation did not in itself entail non-compliance with the rules of the CFCS Act.
- TET recommended that DDIS ensure as quickly as possible that data on the sensor network probes was deleted in accordance with the rules of the CFCS Act.

In 2026, TET will continue to follow the implementation of DDIS's decision to close the sensor network.

TET's other review of DDIS's procurement and processing of information pursuant to the CFCS Act in 2025 did not give rise to any comments.

2.2.10 Review of DDIS's internal compliance review

TET carried out a review in 2025 of DDIS's internal compliance review in 2024 and the service's planning thereof for 2025, including the internal review of the parts of the service which are covered by the CFCS Act.

How does DDIS conduct internal compliance review?

DDIS carries out ongoing internal compliance review of the service's compliance with specific parts of the DDIS Act, etc. For the purpose of planning the internal compliance review, DDIS annually prepares a risk analysis of the service's compliance with statutory requirements and a plan for the internal compliance review in the following year.

DDIS regularly briefs TET on the planning of the internal compliance review and the results thereof, including by submitting the service's risk analysis and review plan.

Comments by TET

The review of DDIS's internal compliance review in 2025 did not give rise to any comments.

TET found that DDIS had planned and carried out the service's internal compliance review satisfactorily.

2.2.11 Follow-up on TET's review of DDIS in 2024

TET reviews annually whether DDIS has carried out the actions which, on the basis of TET's review in the preceding year, the service indicated that it would carry out.

In 2025, TET followed up on TET's review of DDIS in 2024, including TET's review in 2024 of the former CFCS.

TET reviewed the information which DDIS, in connection with TET's reviews in 2024, had agreed to delete, as well as the recommendations which TET, in connection with completed reviews, found it necessary to implement.

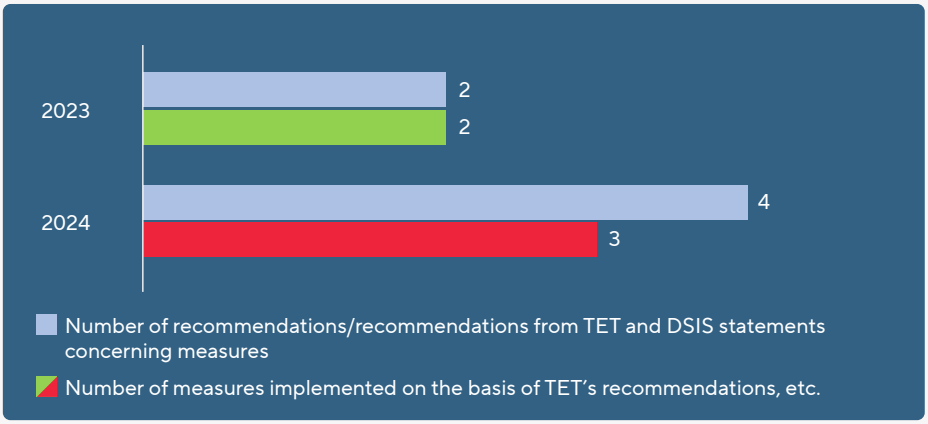
The review also aimed to determine whether DDIS had carried out the measures which, in connection with the reviews in 2024, the service had indicated to TET that it would carry out.

Comments by TET

The follow-up on TET's review of DDIS in 2024 showed the following:

- TET noted that in three cases DDIS had carried out the measures which TET had either recommended or which the service had stated that it would carry out.
- TET noted that in one case DDIS had not yet carried out measures which the service, on the basis of recommendations in connection with TET's review in 2024, had stated would be carried out.

  In connection with the review, DDIS stated that the measure is expected to be implemented in 2026.



2.2.12 TET's technical investigations and mapping of DDIS's IT infrastructure

In 2025, TET carried out verification reviews and mappings of DDIS's IT infrastructure by

- mapping the service's server infrastructure,
- mapping the service's network,
- mapping the service's use of artificial intelligence (AI), and
- mapping the service's use of container-based infrastructure.

Mapping as a prerequisite for risk management

DDIS's IT systems and underlying databases in which information is processed constitute a complex and dynamic landscape of different technologies and data types. In order to navigate this complex IT landscape and perform TET's primary tasks, in 2025 TET reviewed and verified extensive parts of DDIS's IT landscape and worked continuously to ensure up-to-date knowledge of the service's systems.

It is a prerequisite for meaningful review of DDIS that TET has knowledge of the service's overall IT infrastructure, so that the review can be targeted at those parts of the infrastructure which pose the greatest risk of processing in contravention of the DDIS legislation.

Comments by TET

The technical investigations and mapping of IT infrastructure in 2025 did not give rise to any comments.

2.3 DDIS's briefing of TET

In 2025, DDIS regularly briefed TET on significant matters concerning the service's processing of information about natural and legal persons resident in Denmark, including incidents detected through the service's internal compliance review.

Statutory duty to inform

According to the preparatory works to the DDIS Act, DDIS is required to keep the TET informed on an ongoing basis of the application of a number of provisions of the Act.

Accordingly, DDIS must inform TET of the following:

- DDIS's decisions pursuant to section 6(3) of the DDIS Act not to delete infor-mation that has reached the 15-year deletion deadline laid down in section 6(1) and (2).
- All material issues concerning DDIS's processing of information relating to natural and legal persons domiciled in Denmark.
- New administrative guidelines issued pursuant to section 1(5), section 4(3) and section 5(3) of the DDIS Act.

2.4 Requests for access under sections 9 and 10 of the DDIS Act

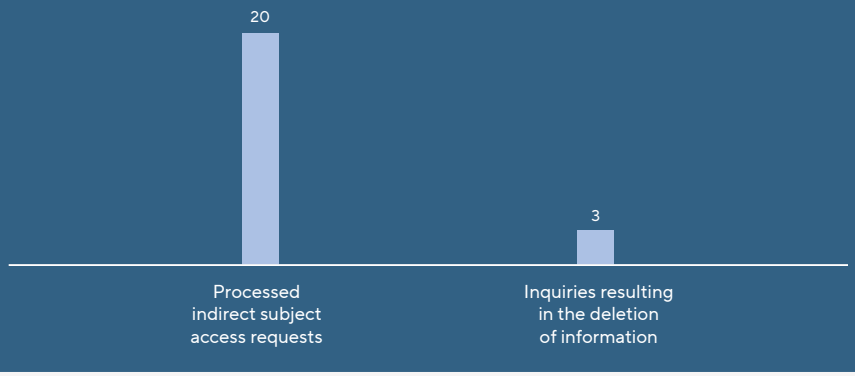
In 2025, TET processed requests from 20 natural or legal persons asking TET to examine whether DDIS was unlawfully processing information about them. In that connection, TET found that in 17 cases DDIS was not unlawfully processing information about the persons concerned.

In three cases, DDIS processed information about the persons concerned which no longer met the conditions for processing in section 4(1) or section 5(1) of the DDIS Act. On that basis, DDIS deleted the information. In this connection, it should be noted that DDIS is not obliged, on its own initiative and on an ongoing basis, to review the service's cases and documents, etc., in order to assess whether the above-mentioned conditions for processing continue to be met.

The average case processing time for the completed requests in 2025 was 85 working days, of which 16 days constituted case processing time at DDIS.

TET aims to respond to requests for access as quickly as possible, but the investigations may be both resource-intensive and complicated. The results of the investigations are submitted to TET at monthly meetings, at which TET decides on the response to the requests.

Requests for indirect subject access



It should be noted that a prerequisite for TET's performance of its task in connection with the indirect subject access scheme is that DDIS's information about natural and legal persons resident in Denmark is stored in IT systems in which effective searches can be carried out.

Processing of requests for access

When a natural or legal person resident in Denmark asks TET to examine whether DDIS is unlawfully processing information about that person, TET conducts an investigation at DDIS, where TET has access to any information and all material of importance to TET's activities.

It may be both resource-intensive and complicated to identify all information that DDIS may process about a person, but TET endeavours to find all information that the service may process about a person who requests indirect subject access.

When the investigations have been completed, TET assesses whether, in TET's opinion, DDIS is unlawfully processing information about the person concerned. If TET finds that this is the case, TET orders DDIS to delete the information. Once TET has ensured that information about the person concerned is no longer being processed unlawfully, TET replies to the request.

Where special circumstances warrant it, TET may order DDIS to give a natural or legal person resident in Denmark access to information which the service processes about that person, or access to whether the service processes information about that person.

In cases where TET receives a request for access to information, TET investigates what information DDIS may process about the person concerned and obtains the service's comments before TET makes a decision under the provision. In connection with requests for indirect subject access, TET examines of its own motion whether special circumstances may warrant ordering DDIS to provide full or partial access to the information mentioned.

Which systems are covered by TET's investigations?

TET annually prepares a separate risk assessment and analysis for TET's tasks in relation to DDIS under the indirect subject access scheme, including with a view to ensuring that TET's investigations in connection with requests for indirect subject access are effective and relevant.

TET's investigations cover a number of central systems at DDIS. TET has assessed, however, that the investigations should cover an additional system which is not currently covered, as it has not been technically possible to carry out content-based searches in that system.

TET and DDIS remain in dialogue concerning the search function in the central system. In this connection, in 2025 TET began testing a solution for searching the system made available to TET by DDIS.

Systems which should be covered by TET's examinations, but which are not currently covered

0
systems in which it is not technically possible to carry out an effective search

0
systems out of operation

1
system regarding which DDIS and TET are in dialogue

2.5 DDIS's case processing times in 2025

DDIS's case processing times in 2025

Number of legal consultations of DDIS	14 consultations
Number of legal consultations answered within the deadline	3 consultations
Average number of days for overdue consultations	8 days

2.6 Cases submitted to the Minister of Defence for decision

Since 2014, TET and DDIS have submitted seven questions of interpretation to the Minister of Defence.

On 28 March 2025, the Ministry of Defence asked DDIS to resume discussions with TET concerning four questions of interpretation which had been submitted to the Minister of Defence but not yet decided, so that the new Board could have an opportunity to consider the questions. In dialogue with DDIS throughout 2025, TET has considered whether the returned questions of interpretation should be resubmitted to the Minister of Defence. The dialogue with DDIS is expected to continue in 2026.

Submission of questions to the Minister of Defence

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

At the conclusion of each review, TET issues a statement to DDIS describing the result of TET's review. The statement may also contain a description of one or more measures which TET assesses DDIS should take. If DDIS, in exceptional cases, decides not to comply with a recommendation in a statement from TET, the service must notify TET thereof and submit the matter to the Minister of Defence for decision without undue delay. If the Minister of Defence decides not to comply with TET's recommendation, the Government must inform the Parliamentary Intelligence Services Committee (UET) accordingly. TET's response options in relation to DDIS are described in further detail in section 16 of the DDIS Act and section 16 of the CFCS Act.

As a general rule, TET does not review matters which are covered by questions submitted to the Minister of Defence in the period from the submission until the Minister's decision. TET plans its subsequent review in accordance with the Minister of Defence's decision.

The following table provides an overview of cases submitted to the Minister of Defence since the establishment of TET in 2014.

Question	Date of submission	Status
Whether DDIS may carry out targeted searching for information about persons resident in Denmark in data procured from open sources and considered by the service to be collected raw data. Further addressed in TET's report on DDIS for 2024 (section 3.6).	20 June 2024	On 28 March 2025, the Minister of Defence asked DDIS to resume discussions with TET so that the new Board could have an opportunity to consider the question. TET has not yet taken a position on the question.
Whether news articles collected by DDIS, without a more detailed review of the content of the news article having first been carried out, must be regarded as raw data. Further addressed in TET's report on DDIS for 2023 (section 3.6).	23 October 2023	Decided on 20 February 2024. The Minister of Defence found that unread news articles received through news subscriptions cannot be categorised as raw data within the meaning of the DDIS Act.
Whether DDIS, in connection with compliance with section 3 of the DDIS Executive Order on Security Measures and section 18 of the CFCS Act, is required for each of the service's systems to assess which measures can provide a sufficient level of security. Further addressed in TET's reports on DDIS and CFCS for 2022, respectively (sections 2.2.9 and 2.2.7).	4 August 2023	On 28 March 2025, the Minister of Defence asked DDIS to resume discussions with TET so that the new Board could have an opportunity to consider the question. TET has not yet taken a position on the question.
Whether the Minister of Defence's decision of 11 August 2021 concerning deletion of data from DDIS's sensor network applies only when sensor data is stored in the alarm units and the service's central analysis platform, or applies in all cases where the service stores sensor data in relevant processing systems, for example locally on an employee's workstation. Further addressed in TET's report on CFCS for 2022 (section 2.2.3).	1 August 2023	On 28 March 2025, the Minister of Defence asked DDIS to resume discussions with TET so that the new Board could have an opportunity to consider the question. In 2025, TET decided that the question should not be resubmitted to the Minister of Defence.
Whether TET, when interpreting section 3 of the DDIS Executive Order on Security Measures, may use the ISO 27001 standard, which has been chosen as the government security standard, to elaborate the general obligations for DDIS in relation to security of processing set out in the Executive Order. Further addressed in TET's report on DDIS for 2021 (section 1.2.8).	2 May 2022	On 28 March 2025, the Minister of Defence asked DDIS to resume discussions with TET so that the new Board could have an opportunity to consider the question. On 26 March 2026, TET informed DDIS that TET wished the matter to be submitted to the Minister of Defence again if the service continued to disagree with TET's interpretation. TET and DDIS remain in dialogue on the matter.

Question	Date of submission	Status
Whether TET's remit under section 15 of the DDIS Act includes DDIS's obtaining and disclosure of raw data, and whether the rules of the DDIS Executive Order on Security Measures apply to raw data. On the basis of the report of the DDIS Commission, TET independently asked the Minister of Defence to take a position on the interpretation of the DDIS Act. The submission was therefore not made pursuant to section 16 of the DDIS Act. Further addressed in TET's report on DDIS for 2022 (section 3).	2 February 2022	Decided on 16 January 2023. The Minister of Defence found that TET shall not review whether DDIS's obtaining and disclosure of raw data complies with the requirements of the DDIS Act, and that DDIS is not obliged to secure raw data in accordance with the DDIS Executive Order on Security Measures, as the Executive Order does not apply to raw data.
Whether data from CFCS's sensor network must, pursuant to section 17(1) of the CFCS Act, be deleted immediately after the investigation of the specific incident that caused the obtaining has been completed. Further addressed in TET's report on CFCS for 2021 (section 2).	11 August 2020	Decided on 11 August 2021. The Minister of Defence found that section 17(1) of the CFCS Act has a very limited scope of application in relation to sensor data. The primary scope of application of the provision is the other forms of data covered by chapter 4 of the CFCS Act, for example stationary data procured pursuant to section 5 of the CFCS Act. Stationary data includes data stored on, among other things, servers, storage devices, mobile devices or the like and which, unlike sensor data, does not constitute communication between networks.

2.7 Statistics concerning DDIS's processing of information pursuant to the CFCS Act

DDIS's activities pursuant to the CFCS Act are performed as part of the tasks of the service's Cyber Sector.

It follows from the legislative history of the CFCS Act that TET's annual report on its activities shall contain statistical information on DDIS's processing of personal data pursuant to the Act, including information on the number of complaints received by both the service and TET, information on the number of access-to-documents cases and the outcome of those cases, and information on the number of cases related to security incidents processed by the service.

TET's report shall also contain statistics on the number of cases in which an analyst at DDIS has, pursuant to the CFCS Act, performed an analysis

of data on the basis of interference with the secrecy of communications. These statistics shall include an overall categorisation of how serious those cases have been.

Finally, TET's report shall contain a fully anonymised description of one or more specific cyberattacks.

DDIS has contributed the following description and data for 2025:

Examples of DDIS's Cyber Sector's handling of cyberattacks in 2025

In 2025, DDIS's Cyber Sector handled a large number of security incidents for public authorities and businesses. The incidents included, among other things, systematic exploitation of known or previously unknown vulnerabilities, data leaks, reconnaissance, spear phishing and attempts at brute forcing. Some of the incidents also involved attempted compromises in the form of espionage and data theft as well as ransomware attacks involving encryption, data theft, extortion and leakage of data.

Attempted attacks by phishing remain a serious threat to public authorities and businesses. These may, for example, be emails or messages from a malicious actor seeking to induce a recipient to activate links or access content that may either lead to infections or deceive the victim into disclosing login credentials. In addition, DDIS's Cyber Sector continuously observes different types of attempts to exploit misconfigurations and publicly known vulnerabilities in software services exposed to the internet.

It should be noted that Table 2 below states the number of identified security incidents, while threats also include potential events which have therefore not materialised or been recognised by DDIS. The threat from phishing may therefore be serious even if DDIS has not identified any major or serious security incidents in 2025.

Table 1 - Disclosures and exchanges*	**2025**
Disclosures	137
Exchanges	23

* Disclosure includes sharing of data, typically on the basis of a security incident, with other authorities or businesses, for example an authority or business connected to DDIS's sensor network. Exchange includes internal sharing of data between the Network Security Service and the other parts of DDIS.

Table 2 - Security incidents* by severity	2025
Serious cyberattacks	0
Major cyberattacks	0
Moderate cyberattacks	9
Minor cyberattacks	20
No/limited impact**	838
Total	**867**

* Security incidents are defined in accordance with section 2, no. 1, of the Act on the Danish Centre for Cyber Security.

** The category "No/limited impact" includes all security incidents which have not had an impact on the customer or which, on closer analysis, prove not to be a security incident.

Table 3 - Access-to-documents cases 2025	2025
Full access to documents	1
Partial access to documents	6
Refusal of access to documents	4
No documents covered by the request located	2
Total	**13**

Table 4 - Complaints concerning processing of personal data	2025
Complaints concerning DDIS's Cyber Sector's processing of personal data	0*
Complaints received by TET	0

* DDIS is not aware of any complaints having been received.

3. About TET's review activities

3.1 Prerequisites for TET's review

The review activities of the Danish Intelligence Oversight Board (TET) contribute to the legitimisation of the activities of the Danish Security and Intelligence Service (DSIS), the Danish Defence Intelligence Service (DDIS) and the Danish National Police PNR Unit (the PNR Unit) by strengthening public confidence that these activities are lawful.

TET's activities are determined by law, including

- that, upon receipt of a complaint or of its own motion, TET reviews that DSIS, DDIS and the PNR Unit process personal data in compliance with legislation,
- that, by ex post legality review, TET reviews that DSIS's operational tasks are carried out in accordance with applicable legislation, international obligations and internal guidelines,
- that, upon request from the Parliamentary Intelligence Services Committee (UET), TET may examine specific cases, courses of events, issues, etc., in DSIS and/or DDIS,
- that TET is responsible for the external whistleblower scheme for DSIS,
- that TET may require DSIS, DDIS and the PNR Unit to provide any information and all material of significance to TET's activities,
- that TET is entitled at any time to access all premises from which the information being processed may be accessed or where technical facilities are used,
- that TET may require DSIS, DDIS and the PNR Unit to provide written statements on factual and legal matters of significance to TET's review activities,
- that DSIS, DDIS or the PNR Unit - if they exceptionally decide not to comply with a recommendation in a statement from TET - must without undue de-

lay submit the matter to the Minister of Justice or the Minister of Defence, respectively, for decision,

- that TET informs the Minister of Justice and the Minister of Defence, respectively, of matters of which, in TET's opinion, the Ministers ought to have knowledge, and

- that TET must submit annual reports on its activities, which must be presented orally to UET and subsequently made public.

TET's access to information

TET expects DSIS, DDIS and the PNR Unit, within the framework of the law, to give TET unrestricted, full and timely access to all material relevant for TET to perform a proper and effective review.

TET expects DSIS, DDIS and the PNR Unit to ensure that TET has the right user access to the authorities' IT infrastructure, ensuring direct and unrestricted access to relevant information for TET's review.

In cases where, for technical reasons, full user rights cannot be given to selected parts of DSIS's, DDIS's or the PNR Unit's IT infrastructure, **TET expects** to be informed of:

- the nature and scope of the part of the IT infrastructure to which TET does not itself have access, and

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

Unrestricted, full and timely access to material of significance to TET's activities is crucial to effective and accurate review.

DSIS, DDIS and the PNR Unit may exceptionally submit a statement concerning the omission of selected information from a review. In order for TET's statutory right of access to information to be observed, however, only TET has the decision-making authority as to whether selected information may be omitted in connection with a review.

In this connection, TET must be able to verify that the information which DSIS, DDIS or the PNR Unit wishes to omit in connection with a review is not relevant to TET's review.

Response to TET's consultations

TET expects the consultation responses from DSIS, DDIS and the PNR Unit to be complete, transparent and unqualified.

TET expects DSIS, DDIS and the PNR Unit to inform TET of the existence of any other relevant information or material of significance to the review which the authority may acknowledge that TET does not have insight into.

TET expects the consultation responses from DSIS, DDIS and the PNR Unit to be provided in a timely manner and within the timeframes set out in TET's process for consultation with the authority.

With a view to ensuring effective and accurate review, TET sends targeted requests for statements on factual and legal matters of significance to TET's review activities.

TET has the decision-making authority to decide whether selected information is relevant to the review, and the consultation responses from DSIS, DDIS and the PNR Unit must therefore be complete, transparent and unqualified.

When responding to TET's consultations, DSIS, DDIS or the PNR Unit may therefore not independently assess whether selected requests for information are relevant to TET's review.

Follow-up on TET's review

TET expects - that if DSIS, DDIS or the PNR Unit have comments on the results of TET's individual review - such comments to be forwarded to TET within the deadline stated in TET's follow-up letter.

TET expects – that if DSIS, DDIS or the PNR Unit exceptionally decide not to comply with a recommendation from TET - the authority to fulfil its duty of disclosure and, without undue delay, submit the matter to the Minister of Justice or the Minister of Defence, respectively, for decision.

Practices which TET has assessed to be unlawful, and with which DSIS, DDIS or the PNR Unit agree, must be dealt with, and disagreement on the interpretation of the legal basis must be resolved without undue delay. It is therefore crucial that DSIS, DDIS and the PNR Unit respond to TET's recommendations in a timely manner, including, where necessary, by submitting a given case to the Minister of Justice or the Minister of Defence, respectively, for decision.

3.2 Scale for TET's comments in 2025

TET's remarks are based on the following scale:

Comments	Background to comments
*»[...] **does not give rise to any comments«***	Used when TET agrees with the authority on how they are generally or specifically administering the law.
*»On the information available, TET is **unable to assess** [...]«*	Used when TET's review is limited by either factual or legal circumstances.
*»TET finds it **striking** [...]«*	Used for situations in the authority or legislation which do not quite match the general or immediate impression of an outsider.
*»TET finds it **problematic** [...]«*	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 **identified** [...]«*	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 **criticisable** [...]«*	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 **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 the authority having demonstrated a willingness to ensure the necessary remedial action.

3.3 Review methodology

TET continuously works to improve the methods it uses in planning and performing the review of DSIS, DDIS and the PNR Unit so that the review has the greatest possible effect within the framework set for TET's activities.

TET's review of DSIS, DDIS and the PNR Unit requires knowledge of the authorities' operational tasks and IT infrastructure, prioritisation of TET's resources and effective methods for performing the review.

TET can review only those parts of DSIS, DDIS and the PNR Unit of which TET is aware. Furthermore, TET does not have the resources to perform a complete review of all parts of DSIS, DDIS and the PNR Unit. Finally, TET's reviews must be able to document the circumstances in DSIS, DDIS and the PNR Unit with limited resource use.

TET's standards are intended to address these fundamental challenges. TET's work therefore consists overall of three elements:

TET's ❶ mapping of both operational tasks in DSIS and IT infrastructure in DSIS, DDIS and the PNR Unit, respectively, is intended to provide TET with the necessary knowledge of the authority's handling of operational activities and of procurement, processing and disclosure of information.

TET compiles and assesses information about relevant parts of DSIS's, DDIS's and the PNR Unit's IT infrastructure and DSIS's operational tasks in order to create

the appropriate basis for performing complete risk and materiality assessments of all operational tasks in DSIS and of processes and systems at the authorities.

TET's method 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 gave rise to a need for adaptation, structuring and formalisation of the method.

The choice of method reflects a balancing of the need for technical detail in the mapping to support TET's review activities, the amount of IT resources and the level of IT governance maturity both within TET and within DSIS, DDIS and the PNR Unit.

TET's ❷ planning of reviews for the coming year is intended to prioritise TET's resources so that the review is directed at the parts of DSIS, DDIS and the PNR Unit where the risk of non-compliance with legislation is assessed to be greatest.

The planning is based on annual risk and materiality assessments of operational tasks in DSIS and of processes and systems (hereinafter referred to as review subjects) in DSIS, DDIS and the PNR Unit, for the purpose of assessing risks of non-compliance with legislation in the authorities' activities. On this basis, TET prepares risk analyses which form the basis for the selection of reviews in the coming year. The selected reviews are compiled in review plans for DSIS, DDIS and the PNR Unit for the coming year.

The purpose of the risk analyses is to ensure that TET's review is focused on areas where the risk of non-compliance with legislation is greatest when compared with the degree of harm that possible errors are assessed to entail for natural and legal persons, as well as whether possible errors are of a nature which may affect public confidence in the service. In addition, other relevant factors are taken into account, such as areas where TET's review has been given special weight by the legislature, including the rules on lawful political activities.

Areas where the risk of non-compliance with legislation is assessed to be lower will also be subject to review with a view to ensuring completeness in TET's review of DSIS, DDIS and the PNR Unit and ensuring that the assessment of the risk of non-compliance with legislation in these areas remains accurate. However, review of these areas is performed less regularly.

TET's reviews ❸ are performed continuously throughout the year on the basis of the review plans for DSIS, DDIS and the PNR Unit, respectively. TET does not determine methods for the individual reviews in connection with the preparation of risk assessments and analyses, but only after a prior technical and legal scoping of the individual review subject.

TET uses a number of different methods in the review of individual review subjects, including full review, random or targeted sampling, content screening, inspections and interview- and consultation-based reviews.

TET's choice of review method is based on a specific risk assessment of the review subject, experience from previous reviews and the factual circumstances which TET identifies in connection with the specific review. In this connection, before reviewing areas not previously reviewed, TET holds a start-up meeting with relevant employees of DSIS, DDIS or the PNR Unit in order to ensure


See standard for TET's IT infrastructure mapping (section 1)
Mapping of IT infrastructure of the DSIS, DDIS, and PNR Unit
QUALITY ASSURANCE
External consultation on factual matters
QUALITY ASSURANCE
Approval at managerial level
See standard for TET's risk and materiality assessment (section 2)
Risk and materiality assessment of the DSIS, DDIS, and PNR Unit
QUALITY ASSURANCE
Approval at managerial level
Presentation of risk and materiality assessment of the DSIS, DDIS, and PNR Unit and decision on review plans for the coming year
QUALITY ASSURANCE
Discussion and approval at Oversight Board level
See standard for TET's choice of method, performance of checks and verification (section 3)
Clarification of review type for all planned reviews
QUALITY ASSURANCE
Approval at managerial level
Briefing of DSIS, DDIS, and PNR Unit on TET's planned reviews
Technical and legal assessment of review subjects
QUALITY ASSURANCE
External consultation on legal and factual matters
Decision on method for the individual reviews
QUALITY ASSURANCE
Approval at managerial level
Performance of reviews
QUALITY ASSURANCE
Approval at managerial level
Consultation of DSIS, DDIS, or PNR Unit in connection with reviews
QUALITY ASSURANCE
External consultation on legal and factual matters
Presentation and conclusion of reviews
QUALITY ASSURANCE
Discussion and approval at Oversight Board level
Submission of follow-up letters to DSIS, DDIS, or PNR Unit
QUALITY ASSURANCE
External quality assurance in case of any comments concerning the control
Preparation of annual reports on DSIS, DDIS, and PNR Unit
QUALITY ASSURANCE
Discussion and approval at Oversight Board level
QUALITY ASSURANCE
External quality assurance in case of consultation on factual or classification-related matters
Publication of TET's annual reports

sufficient police and/or intelligence professional as well as technical and legal understanding of the area, so that the review can be adapted and performed appropriately and in a resource-optimised manner.

As part of TET's performance of reviews, verification reviews are also carried out of DSIS's, DDIS's and the PNR Unit's IT infrastructure. The purpose is to ensure that TET's review is based on information from DSIS, DDIS and the PNR Unit, the accuracy of which TET has verified.

The processes for TET's ❶ mapping, ❷ risk assessment and planninng and ❸ performance and verification are shown in the figure on page 39. The processes are supported by ongoing quality assurance through approval at chief level and Board level, respectively, and by consultations with external parties on legal, factual or classification-related matters.

TET's direct access to DSIS's, DDIS's and the PNR Unit's systems ensures that the authorities cannot predict which cases and information will be subject to review. In some cases, however, it is necessary for TET to notify DSIS, DDIS or the PNR Unit of the time and method of a review, for example if TET needs access to special physical premises or needs to interview specific employees.

Before commencing the reviews for the year, TET shares its risk analyses and review plans with DSIS, DDIS and the PNR Unit, respectively, in order to ensure openness about TET's assessment of the circumstances at the authorities. This openness also enables DSIS, DDIS and the PNR Unit to take TET's review into account in the organisation of the authorities' internal review, which contributes to TET's review and the authorities' internal review collectively covering a larger part of their activities. Finally, the openness ensures that DSIS, DDIS and the PNR Unit can allocate sufficient resources to serve TET.

TET also prepares separate risk assessments and analyses specifically for TET's tasks in relation to DSIS and DDIS under the indirect subject access scheme, among other things to ensure that TET's examinations in connection with requests for indirect subject access are effective and relevant.

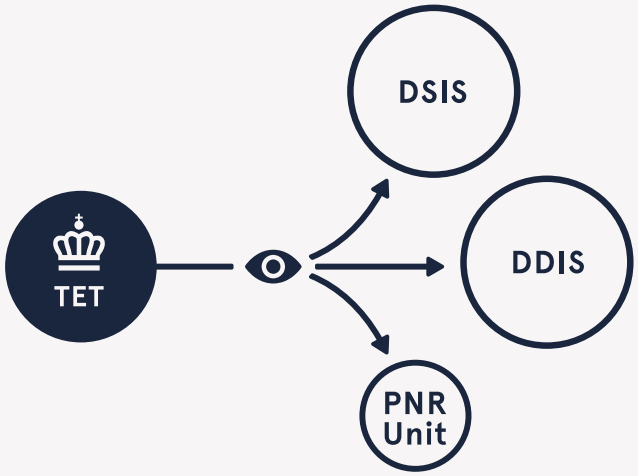
For further information on TET's review methodology, reference is made to TET's published standards, which are available on TET's website.

3.4 Organisation

Table - Resources and Staffing

Staff in 2025 (*employees*)	9
Budget appropriation in 2025 (*DKK million*)	10,6

TET is an independent oversight body which reviews whether DSIS, DDIS and the PNR Unit process personal data in accordance with legislation. TET also performs ex post legality review of DSIS's operational tasks.



TET performs its functions in full independence and is therefore not subject to instructions from the Ministry of Justice, the Ministry of Defence or other administrative authorities with respect to the performance of its activities.

TET consists of a chair and four additional members appointed by the Minister of Justice following negotiations with the Minister of Defence. The appointment of the members of TET takes place after discussion with UET.

TET is composed in such a way that TET collectively possesses the necessary competencies, including insight into and experience with foreign policy, security and intelligence matters, strong legal competencies, experience with oversight activities in a broader sense, and insight into and experience with intelligence activities.

The members of TET are generally appointed for a period of four years, and each member may be reappointed for a further four years.

Lars Bay Larsen (Chair)

Senior consultant at the law firm Gorrissen Feder-spiel.

Retired Vice-President and Judge of the Court of Justice of the European Union (2006-2024) and retired Justice of the Danish Supreme Court (2003-2006).

Gitte Lillelund Bech (Deputy Chair)

Independent adviser at LillelundBech ApS.

Former Danish Minister of Defence (2010-2011) and member of the Danish Parliament (1999-2013).

Anne Hedensted Steffensen (Member)

Director General and CEO of Danish Shipping.

Previously 23 years in the Foreign Service, most recently as Denmark's Ambassador to the United Kingdom (2011-2013).

Pernille Knudsen (Member)

Director for Employment Law and Collective Agreements, Danish Chamber of Commerce.

Previously 25 years at the Confederation of Danish Employers (2000-2025), most recently as Deputy CEO.

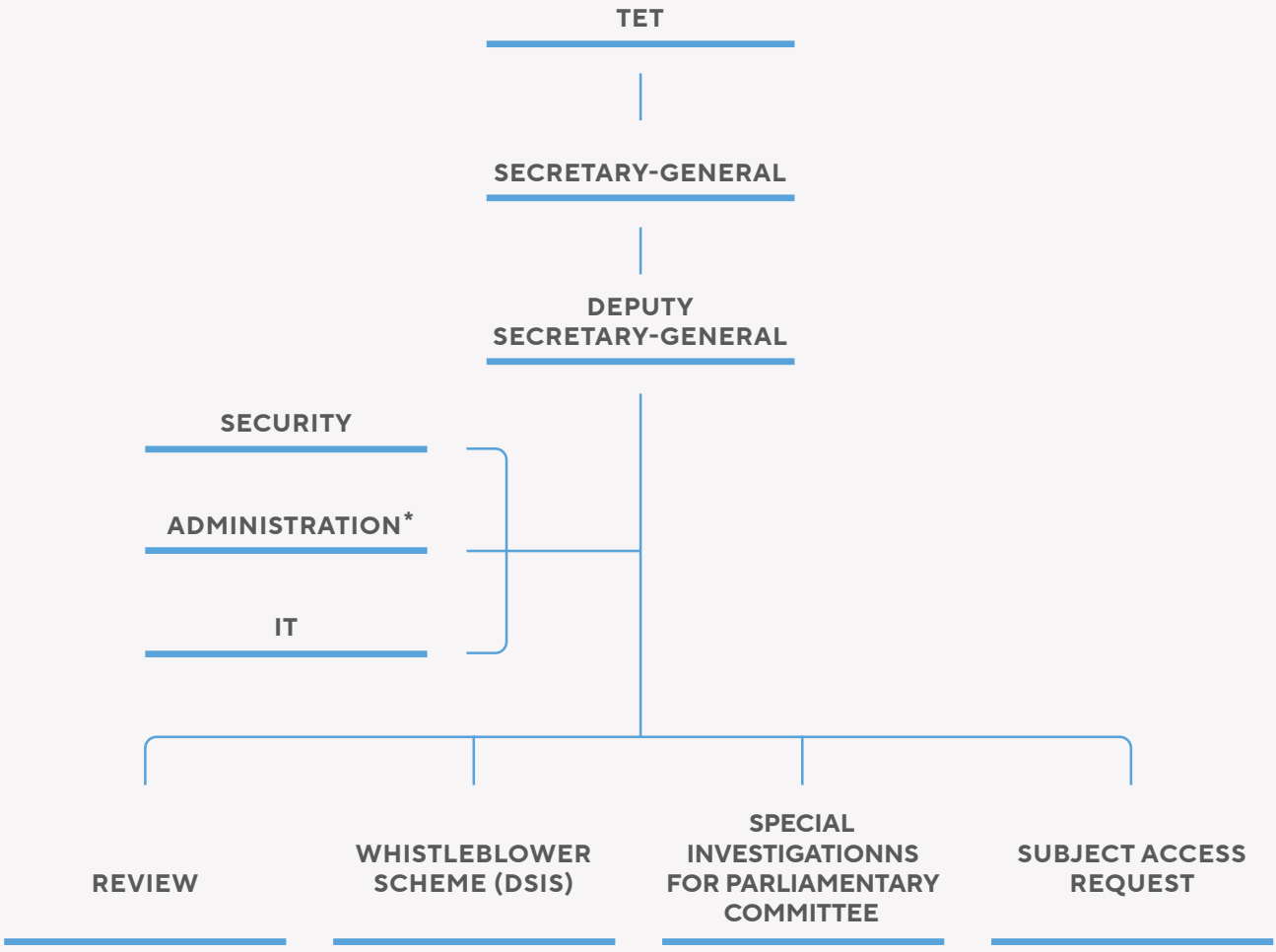
Rasmus Blaabjerg (Member)

Attorney-at-law and partner at the law firm Civitas Advokater.

Former Head of Division at the Independent Police Complaints Authority, acting High Court Judge at the High Court of Western Denmark, Head of Secretariat at East Jutland Police and employee at the Ministry of Justice.

TET is served by a separate unit at the Danish Data Protection Agency (TET Unit), which in professional matters reports directly to the members of TET. At the end of 2025, TET Unit consisted of a legal head of office responsible for day-to-day management, a political science deputy head, two legal officers, one political scientist, two IT specialists and an administrative employee.

The TET Unit is divided into functions concerned with TET's review activities, examinations on behalf of UET, the external whistleblower scheme for DSIS and requests for indirect subject access.



* Certain administrative functions are handled by the Danish Data Protection Agency.

Report 2025
Danish Defence Intelligence Service
Published by the Danish Intelligence Oversight Board, May 2026
Layout and illustrations: Eckardt ApS
Portrait photos: Helene Hallager Photography
The publication can be downloaded from TET's website (www.tet.dk)

tet

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