Report 2025

Danish Security and Intelligence Service

tet

Danish Intelligence Oversight Board

To the Minister of Justice

Pursuant to section 22 of the Act on the Danish Security and Intelligence Service (DSIS) (Consolidation Act no. 231 of 7 March 2017, as most recently amended by Act no. 666 of 11 June 2025), the Danish Intelligence Oversight Board (TET) hereby submits its report on its activities concerning DSIS for 2025.

The report also contains a description of TET's activities concerning the Danish National Police PNR Unit (the PNR Unit) in 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 DSIS.

The report includes, inter alia, information about the matters which TET has chosen to focus on, including DSIS's operational tasks. The report also describes the number of instances in which TET has found that DSIS's and the PNR Unit's processing of personal data was not in compliance with the applicable rules.

Danish Intelligence Oversight Board

Copenhagen, May 2026

Contents

1. Introductory comments

The Danish Intelligence Oversight Board (TET) has, with the entry into force on 1 January 2025 of Act no. 666 of 11 June 2024 on strengthening oversight of the intelligence services, had its responsibilities expanded, which is intended to help support effective and qualified review of the Danish Security and Intelligence Service (DSIS).

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 TET as a consequence of the amendment to the DSIS Act.

In 2025, TET has prioritised work to implement the amendments to the DSIS Act and has, against that background, had three primary focus areas:

1) Initiating the review of DSIS's operational tasks and further developing TET's standards for review with a view to ensuring transparency, systematic working methods and consistency in TET's work across review areas.

2) Establishing an effective and structured process for TET's performance of examinations on the basis of requests from UET. In this connection, TET has worked purposefully to organise workflows which ensure that TET's examinations can be performed in a timely manner and on an informed basis, so that the parliamentary review of the intelligence services is supported as effectively as possible. TET received its first request from UET for an examination of specific matters on 13 November 2025.

3) Establishing an external whistleblower scheme concerning DSIS, which constitutes an important supplement to the existing review mechanisms.

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.

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 28 reviews of the Danish Security and Intelligence Service (DSIS) and one review of the Danish National Police PNR Unit (the PNR Unit).

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

TET's review is risk-based, which means that TET directs its reviews at the parts of DSIS's) activities where the risk of errors is assessed to be 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. This also means that large parts of DSIS's activities have not been subject to review, as TET assesses that the service observes the statutory provisions in these areas. The report should be read in light of this. It should also be emphasised that, in most of the reviews in which non-compliance with the rules was identified during the current year, DSIS has stated that the service will initiate or has initiated measures to remedy the circumstances.

It should be noted that the references below represent only a limited extract of TET's review of DSIS in 2025. For a complete picture of TET's review of DSIS and the PNR Unit, the report must be read in its entirety.

- 9 out of 28 reviews of DSIS and one review of the PNR Unit did not give rise to any comments. No reviews gave rise to comments concerning highly criticisable matters.

- TET found that DSIS generally had difficulties complying with section 9a(1) of the DSIS Act in relation to the processing of information in pre-production environments, as the reviews found a considerable amount of personal data which should have been erased after completion of testing (section 2.2.3).

  TET found it positive that DSIS would examine the possibilities of implementing automatic erasure of personal data in mailboxes and on drives. TET

recommended that these possibilities be explored across all pre-production environments. TET noted that, if the possibilities of automatic erasure prove to be limited, DSIS should implement other solutions and/or clean-up procedures capable of mitigating risks of unlawful processing of personal data in pre-production environments.

Finally, TET found it important that DSIS allocate sufficient resources to remedy the circumstances.

- TET found that DSIS generally had difficulties complying with section 17, cf. section 18, of the DSIS Executive Order on Security Measures in relation to the processing of information in email mailboxes and on file drives. In a number of instances in its review of transit systems in 2025, TET found information which was processed in email mailboxes and on file drives in which logging that meets the minimum requirements of section 17(1) of the DSIS Executive Order on Security Measures is not performed, and for longer than the deadline set by the service (section 2.2.4).

  TET found it positive that, in some cases, DSIS had initiated clean-up in the transit systems concerned and refreshed the rules for processing information in transit systems for the service's employees, and that in one case the service implemented a new system which limits the amount of personal data. TET found, however, that DSIS should examine the possibility of implementing automatic erasure of information in transit systems.

  Finally, TET found it important that DSIS allocate sufficient resources to remedy the circumstances.

- In its review of DSIS's operational tasks, TET found it problematic (section 2.2.1)

  - that DSIS had not revised the service's internal guidelines for the use of sources and contacts since 2015, considering that the service has amended internal processes and workflows so that they differ from the guidelines in a number of respects, and

  - that DSIS had not revised the service's guidelines for the approval and initiation of coercive measures in criminal proceedings since 2011, considering that the guidelines cover coercive measures in criminal proceedings where the competence or legal classification has changed since 2011 due to, for example, legislative amendments, developments in case law or technological developments, and that the service has amended internal processes and workflows since 2011 so that they differ from the guidelines in a number of respects.

  TET also assessed that DSIS's record management process, under which requests and court orders are in certain cases entered into records once a year, or only when the case is closed, was not in accordance with the record management requirement in section 3 of the DSIS Executive Order. Against this background, TET recommended that DSIS bring its record management process into compliance with section 3 of the DSIS Executive Order.

  TET noted that work is currently ongoing at DSIS to map and revise the service's guidelines. TET encouraged DSIS to prepare updated and accurate

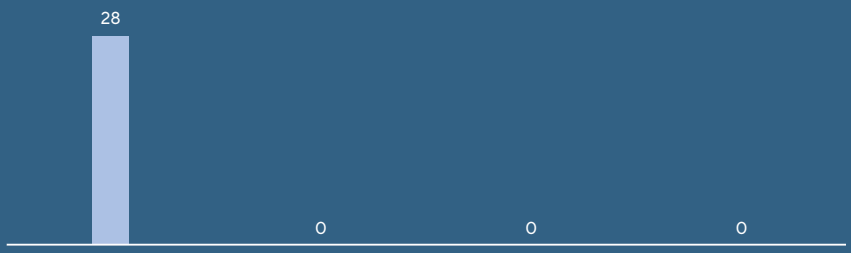
guidelines for the above areas as soon as possible. TET also requested to be informed of DSIS's timetable for doing so.

- On the basis of its review of the processing of information using artificial intelligence (section 2.2.5), TET initiated a dialogue with DSIS on whether a specific language model can be regarded as anonymous, or whether it must be regarded as personal data.

- In 2025, TET processed requests from 39 natural or legal persons asking TET to examine whether DSIS was processing information about them without being entitled to do so. In this connection, TET found that, in 37 cases, DSIS was not processing information about the persons concerned without being entitled to do so.

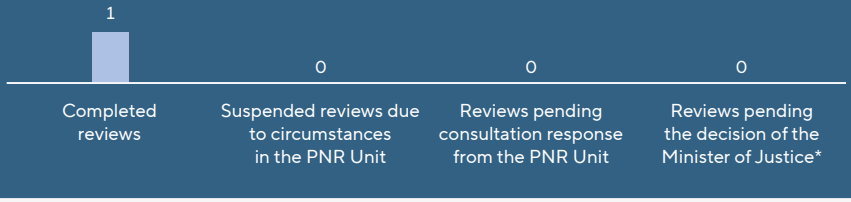
  In two cases, DSIS processed information about the persons concerned which no longer fulfilled the conditions for processing in section 7(1) or section 8(1) of the DSIS Act. Against this background, DSIS erased the information. In this connection, it should be noted that DSIS is not under an obligation on an ongoing basis and of its own motion to review the service's files and documents, etc., in order to assess whether the said conditions for processing continue to be met (section 2.4).

TET's review of DSIS in 2025

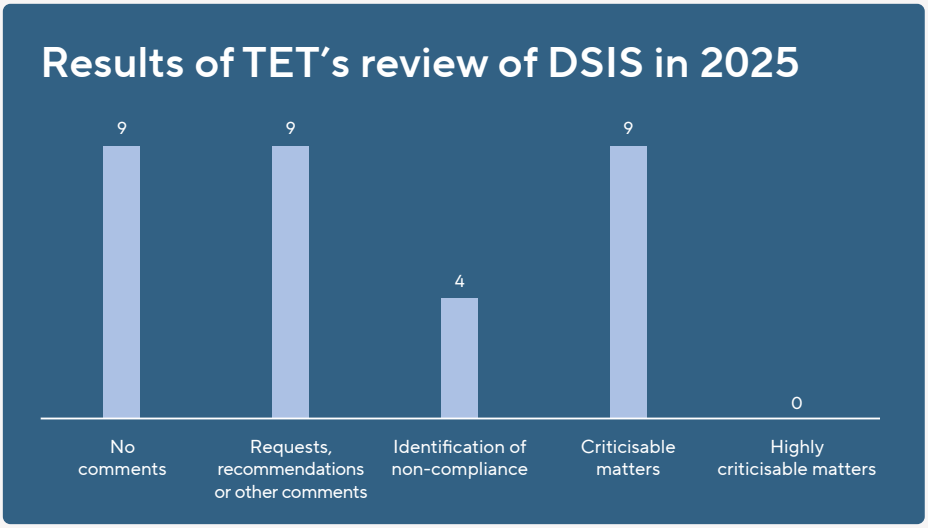


*see section 2.8

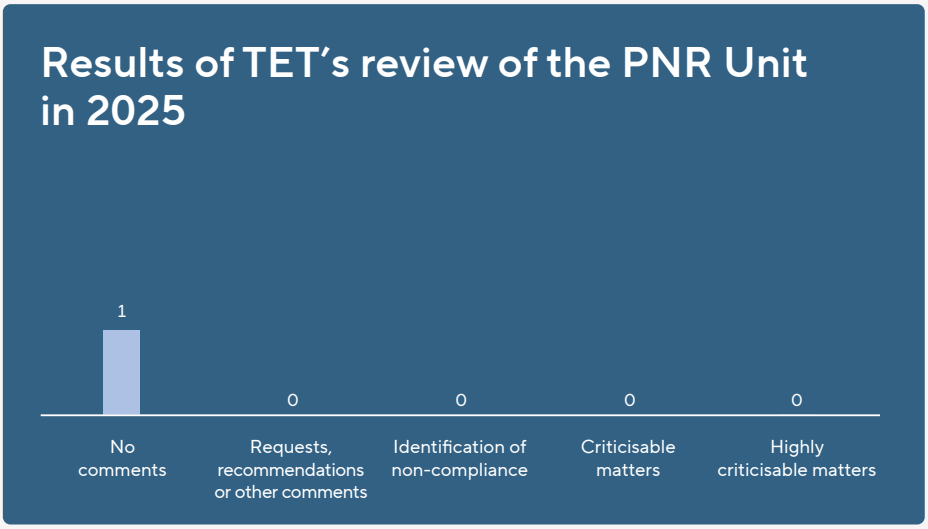
TET's review of the PNR Unit in 2025



*see section 2.8



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.



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 DSIS in 2025

For the purpose of reviewing whether DSIS, in connection with its processing of information concerning natural and legal persons, complies with the rules set out in the DSIS Act, the DSIS Executive Order and the DSIS Executive Order on Security Measures, TET reviewed the service's

- operational tasks (section 2.2.1),
- special databases (section 2.2.2),
- pre-production environments (section 2.2.3),

- transit systems (section 2.2.4),
- processing of information using artificial intelligence (section 2.2.5),
- use of other authorities' systems (section 2.2.6),
- compliance with the rules on processing information concerning lawful political activities (section 2.2.7), and
- internal review (section 2.2.8).

Furthermore, in 2025, TET performed

- follow-up on TET's review of DSIS in 2024 (section 2.2.9), and
- technical investigations and mapping of the service's IT infrastructure (section 2.2.10).

2.2.1 Review of DSIS's operational tasks

In 2025, TET reviewed the operational tasks of DSIS by carrying out

- a review of the service's compliance with internal guidelines for the use of sources and contacts, and
- a review of the service's compliance with court orders and compliance with internal guidelines for the approval and initiation of coercive measures in criminal proceedings.

In addition, the members of TET received separate briefings concerning DSIS's operational tasks with a view to building knowledge, just as TET's chair participated in the performance of a data-level review.

What does legality review of operational tasks mean?

Under section 18(1) of the DSIS Act, TET reviews whether DSIS carries out its operational tasks in accordance with the applicable rules and guidelines.

DSIS's "operational tasks" generally means all operational activities which the service performs as part of the actual performance of its tasks, including preventing, investigating and countering terrorism and espionage, etc., see section 1 of the DSIS Act. Matters related to administrative issues fall outside the concept, including personnel cases concerning employees of DSIS and the service's budget and accounts.

This is an ex post legality review, which means that the review of DSIS's operational tasks concerns whether the service has acted within the rules that

apply to it. The review includes DSIS's compliance with, inter alia, applicable laws, including the DSIS Act, administrative regulations, general administrative law rules and principles, and Denmark's international obligations, including the European Convention on Human Rights (ECHR). In addition, TET may review whether DSIS has complied with internal guidelines within the scope of its operational tasks.

The fact that this is a legality review means that TET will not be tasked with reviewing whether DSIS performs its tasks in an expedient manner. TET will therefore not review DSIS's intelligence and police professional discretion, but may review the legal elements connected with the exercise of that discretion, which may include compliance with general administrative law rules and principles.

As the national intelligence and security service, DSIS has, in some respects, more far-reaching powers than the rest of the police, and the service is therefore in certain cases exempt from the rules of the Administration of Justice Act. This applies, for example, to the rules of the Administration of Justice Act on agent activities and the question of destruction of material procured by interference with the secrecy of communications. TET will not be able to review DSIS's compliance with such rules from which the service is exempt.

Within these areas, TET will, for example, be able to review whether DSIS has recruited and handled sources in accordance with internal guidelines in the area or other applicable rules, including the ECHR, just as TET may review the service's case processing in connection with any claims for compensation by sources, etc. Correspondingly, TET may review, among other things, DSIS's erasure of material originating from interference with the secrecy of communications under the rules thereon in the Administration of Justice Act.

Comments by TET

The review of DSIS's operational tasks showed the following:

- TET found it problematic that DSIS had not revised the service's internal guidelines for the use of sources and contacts since 2015, considering that the service has amended internal processes and workflows so that they differ from the guidelines in a number of respects.

  TET recognised that, in connection with its operational activities, DSIS may need to have a practice which to some extent differs from or supplements the service's written guidelines. TET assessed, however, that the deviations in the specific guidelines had a scope and character which meant that the guidelines had to be regarded as outdated. TET further assessed that, at that time, TET's external review would be able to provide added value only to a limited extent, considering the stage which DSIS's work on its own guidelines appeared to have reached.

  Against this background, TET decided not to perform a more detailed review of DSIS's compliance with the internal guidelines, considering that they to some extent did not correspond to the actual case processing. TET assessed that such a review must await revision and implementation of guidelines so that they correspond to the actual case processing.

TET noted that DSIS has initiated work to map and revise the service's guidelines, and TET encouraged the service to prepare updated and accurate guidelines for the use of sources and contacts as soon as possible and to forward them to TET.

In connection with the review, DSIS stated that, in the service's view, the guidelines are fundamentally accurate for its work with sources and contacts, and that the deviations are to a large extent of an administrative nature, relating for example to matters where the service's practice ensures a higher quality and level of security than assumed in the guidelines. DSIS explained to TET the specific respects in which the service deviates from the guidelines. In continuation of this, DSIS stated that, in the service's view, it is possible to review the service's compliance with the guidelines. On the basis of TET's review and with a view to reporting to TET in the second quarter of 2026, DSIS's independent internal audit unit subsequently initiated an ex post legality review of the service's compliance with the guidelines, with participation from TET.

- TET found it problematic that DSIS had not revised the service's guidelines for the approval and initiation of coercive measures in criminal proceedings since 2011, considering that the guidelines cover coercive measures in criminal proceedings where the competence or legal classification has changed since 2011 due to, for example, legislative amendments, developments in case law or technological developments, and that the service has amended internal processes and workflows since 2011 so that they differ from the guidelines in a number of respects. TET therefore assessed that the guidelines, which have not been revised since 2011, had to be regarded as outdated in important respects, which in principle may entail a risk of non-compliance with legislation.

  TET noted that DSIS has initiated work to map and revise the service's guidelines, and TET encouraged the service to prepare updated and accurate guidelines for the area as soon as possible and to forward them to TET.

- In a sample review of DSIS's action in accordance with court orders, TET found that, in 20 out of 20 cases, the service had performed coercive measures in accordance with the court orders issued, for which reason this review did not give rise to criticism or comments. TET found, however, that in six out of 20 coercive measures DSIS had not entered documents from the court into records within four weeks of receipt in accordance with section 3 of the DSIS Executive Order.

  TET assessed that DSIS's record management process, under which requests and court orders are in certain cases entered into records once a year, or only when the case is closed, is not in accordance with the record management requirement in section 3 of the DSIS Executive Order. Against this background, TET recommended that DSIS bring its record management process into compliance with section 3 of the DSIS Executive Order.

In parallel with the above reviews, TET began mapping DSIS's operational tasks and methods in 2025 with a view to building a knowledge capacity and thereby a stronger basis for performing an accurate risk assessment and review of the service's operational tasks.

It follows from the amendment to the DSIS Act that TET must plan, adapt and perform its review of DSIS on the basis of ongoing annual risk and materiality

assessments of the service's workflows and IT systems, including performing risk and materiality assessments of the service's operational tasks. In 2025, TET has been in dialogue with DSIS about how risk-based legality review of the service's operational tasks can most appropriately be implemented so that it meets the requirements in the preparatory works of the Act. TET will continue to focus on developing its risk-based approach to the review of DSIS (see section 3.3).

2.2.2 Review of DSIS's special databases

In 2025, TET reviewed four operational databases of DSIS.

DSIS's databases

DSIS may maintain special databases in connection with the service's operational and administrative tasks, cf. section 2(1) of the DSIS Executive Order.

Databases are used to structure large amounts of data so that it is possible to carry out effective searches, perform backups, implement access control, establish logging, implement security measures and perform analyses quickly. Databases are a prerequisite for an organisation to be able to handle large amounts of data effectively and securely.

Comments by TET

TET's review of DSIS's processing of information in four operational databases in 2025 did not give rise to any comments.

2.2.3 Review of DSIS's pre-production environments

In 2025, TET reviewed the processing of information by DSIS in pre-production environments by reviewing

- four mail systems distributed across different environments, and
- one drive.

What is a pre-production environment?

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

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

Comments by TET

TET's review of DSIS's processing of information in pre-production environments showed the following:

- TET found that DSIS's processing of information in one pre-production environment did not give rise to any comments.
- TET found it criticisable that DSIS processed 25 out of 30 elements in 28 mailboxes in violation of section 9a(1) of the DSIS Act, as the elements should have been erased after completion of testing. TET further found that the error rate in the sample of approximately 83 percent showed that DSIS had a general challenge in processing the 2,430 elements in the 28 mailboxes covered by TET's review in compliance with section 9a(1) of the DSIS Act.
- TET found it criticisable that DSIS processed 11 out of 30 elements in 106 mailboxes in violation of section 9a(1) of the DSIS Act, as the elements should have been erased after completion of testing. TET further found that the error rate in the sample of approximately 37 percent showed that DSIS had a general challenge in processing the 5,336 elements in the 106 mailboxes covered by TET's review in compliance with section 9a(1) of the DSIS Act.
- TET found it criticisable that DSIS processed 28 out of 30 emails in a shared mailbox in violation of section 9a(1) of the DSIS Act, as they should have been erased after completion of testing. TET further found that the error rate in the sample of approximately 93 percent showed that DSIS had a general challenge in processing the 498 emails in the shared mailbox covered by TET's review in compliance with section 9a(1) of the DSIS Act.
- TET found it criticisable that DSIS processed five out of 30 files on a drive in a pre-production environment in violation of section 9a(1) of the DSIS Act, as the files should have been erased after completion of testing. TET further found that the error rate in the sample of approximately 17 percent showed that DSIS could have a general challenge in processing the 542 files on the drive covered by TET's review in compliance with section 9a(1) of the DSIS Act.

On the basis of the reviews, TET found that DSIS generally had difficulties complying with section 9a(1) of the DSIS Act in relation to the processing of information in pre-production environments, as the reviews found a considerable amount of personal data which should have been erased after completion of testing.

TET found it positive that DSIS would examine the possibilities of implementing automatic erasure of personal data in mailboxes and on drives. TET recommended that these possibilities be explored across all pre-production environments. TET noted that, if the possibilities of automatic erasure prove to

be limited, DSIS should implement other solutions and/or clean-up procedures capable of mitigating risks of unlawful processing of personal data in pre-production environments.

Finally, TET found it important that DSIS allocate sufficient resources to remedy the circumstances. This should be seen in light of the fact that TET selected the area for review in 2025 on the basis of an initial assessment that breaches of section 9a of the DSIS Act may have a significant impact on the legal certainty of a natural or legal person and/or a significant impact on public confidence in DSIS.

In 2026, TET will allocate limited resources to reviewing the area. TET finds it appropriate to await further review, as DSIS must have the opportunity to remedy the circumstances and as TET's review in the intervening period will not be able to contribute further insight. In addition, in 2026 TET will review whether DSIS implements the measures which the service has stated in its consultation responses for reviews of the area in 2025.

2.2.4 Review of DSIS's transit systems

In 2025, TET reviewed the processing of information by DSIS in transit systems by reviewing

- shared mailboxes on three of the service's networks,
- drives on two of the service's networks, and
- one other transit system.

What is a transit system?

It follows from section 3(1) of the DSIS Executive Order that DSIS must store personal data in record management systems or databases within four weeks of receipt or procurement. For practical reasons, DSIS needs to be able to process personal data on other systems, including drives, mail systems, external storage media, file servers and similar systems, before the information is stored in the service's record management systems or databases. Such systems are collectively referred to as transit systems.

DSIS processes a wide range of different operational information in transit systems.

Section 17(1), cf. section 18, of the DSIS Executive Order on Security Measures contains a requirement that information of a confidential nature must be processed in systems in which logging is performed.

Under subsection (2), second sentence, documents in final form may be stored in systems in which logging is not performed if erasure takes place within a shorter deadline set in more detail by DSIS.

DSIS has set a shorter deadline under section 17(1), subsection (2), second sentence, of the DSIS Executive Order on Security Measures by preparing guidance on the service's use of transit systems. If DSIS processes information for longer than the deadline set by the service, this will therefore constitute a breach of section 17(2) of the DSIS Executive Order on Security Measures. DSIS may, in special cases and within the framework of section 17(2) of the DSIS Executive Order on Security Measures, set varying deadlines of shorter duration.

In DSIS's assessment, "confidential nature" must be understood in accordance with the special categories of personal data under data protection law, including information on political opinions and health information. Furthermore, information that a person or an organisation is of interest to DSIS will often be of a confidential nature.

Accordingly, DSIS is permitted to process information which is not of a confidential nature in a system in which logging has not been established (a transit system) for longer than the deadline set by the service for this purpose.

Comments by TET

TET's review of DSIS's processing of information in transit systems showed the following:

- TET found that the review of one transit system did not give rise to any comments in respect of information in the folders covered by TET's review. TET found, however, that on the basis then available it was not possible to assess whether DSIS observed the provisions of DSIS legislation for processing information in five folders to which TET did not have access. TET found it inappropriate that DSIS did not arrange access to the folders in connection with TET's first consultation, as TET's review was thereby limited and therefore did not meet TET's methodological standards for review. DSIS subsequently stated that all folders are located in the same directory and that the same erasure rule has therefore been set up for the five folders as for the folders covered by TET's review.

- TET found it criticisable that DSIS processed 26 out of 30 files on a drive in violation of section 17(2), cf. section 18, of the DSIS Executive Order on Security Measures, as the service had exceeded the deadline set by the service for storing information in transit systems. TET further found that the error rate in the sample of approximately 87 percent showed that DSIS had a general challenge in processing the 4,731 files covered by TET's review in compliance with section 17, cf. section 18, of the DSIS Executive Order on Security Measures. TET found it positive that DSIS reconsidered the workflow in relation to the drive and addressed the 4,731 files by categorising the folder on the drive as a database with a set deletion deadline.

- TET found it criticisable that DSIS processed 28 out of 30 files on a drive in violation of section 17(2), cf. section 18, of the DSIS Executive Order on Security Measures, as the service had exceeded the deadline set by the service for storing information in transit systems. TET further found that the error rate in the sample of approximately 93 percent showed that DSIS had a general challenge in processing the 132,472 files covered by TET's

review in compliance with section 17, cf. section 18, of the DSIS Executive Order on Security Measures. TET found it positive that DSIS has reconsidered and amended the workflow for information on the drive and that the service has cleaned up and erased the majority of the files.

- TET found it criticisable that DSIS processed 28 out of 30 emails in a shared mailbox in violation of section 17(2), cf. section 18, of the DSIS Executive Order on Security Measures, as the service had exceeded the deadline set by the service for storing information in transit systems. TET further found that the error rate in the sample of approximately 93 percent showed that DSIS had a general challenge in processing the 268 emails in the shared mailbox covered by TET's review in compliance with section 17, cf. section 18, of the DSIS Executive Order on Security Measures. TET found it positive that DSIS has reconsidered the workflow for information in the mailbox and addressed the 268 emails by initiating clean-up and refreshing the rules for processing information in transit systems.

- TET found it criticisable that DSIS processed 30 out of 30 emails in a shared mailbox in violation of section 17(2), cf. section 18, of the DSIS Executive Order on Security Measures, as the service had exceeded the deadline set by the service for storing information in transit systems. TET further found that the error rate in the sample of 100 percent showed that DSIS had a general challenge in processing the 853 emails in the shared mailbox covered by TET's review in compliance with section 17, cf. section 18, of the DSIS Executive Order on Security Measures. TET found it positive that DSIS had put a new system into operation to process the information previously processed in the shared mailbox, thereby limiting the processing of information in the shared mailbox.

- TET found it criticisable that DSIS processed 30 out of 30 emails in a shared mailbox in violation of section 17(2), cf. section 18, of the DSIS Executive Order on Security Measures, as the service had exceeded the deadline set by the service for storing information in transit systems. TET further found that the error rate in the sample of 100 percent showed that DSIS had a general challenge in processing the 1,338 emails in the mailbox covered by TET's review in compliance with section 17, cf. section 18, of the DSIS Executive Order on Security Measures.

  Finally, TET found that DSIS had not entered 30 out of 30 emails in the shared mailbox into records in accordance with section 3 of the DSIS Executive Order, and that the service had not notified TET thereof, cf. section 3(2) of the DSIS Executive Order.

- One of TET's reviews was concluded without a data-level review, as the system had been decommissioned.

- TET also reviewed DSIS's compliance with sections 4-5, section 7, sections 10-11 and sections 15-18 of the DSIS Executive Order on Security Measures. DSIS's technical and organisational measures did not give rise to comments in any case.

On the basis of the reviews of transit systems, TET found that DSIS generally had difficulties complying with section 17, cf. section 18, of the DSIS Executive Order on Security Measures in relation to the processing of information in transit

systems, as TET's reviews found information which was processed in systems in which logging that meets the minimum requirements of section 17(1) of the DSIS Executive Order on Security Measures is not performed, and for longer than the deadline set by the service, and as the error rate across TET's five reviews in 2025 was between approximately 87 and 100 percent in all cases.

TET found it positive that DSIS in some cases initiated clean-up in the transit systems concerned and refreshed the rules for processing information in transit systems for the service's employees, and that the service in one case implemented a new system which limits the amount of personal data.

TET found, however, that DSIS should examine the possibility of implementing automatic erasure of information in transit systems.

Finally, TET found it important that DSIS allocate sufficient resources to remedy the circumstances. This should be seen in light of the fact that TET selected the area for review in 2025 on the basis of an initial assessment that breaches of section 17, cf. section 18, of the DSIS Executive Order on Security Measures may have a significant impact on the legal certainty of a natural or legal person and/or a significant impact on public confidence in DSIS.

In 2026, TET will allocate limited resources to reviewing the area. TET finds it appropriate to await further review, as DSIS must have the opportunity to remedy the circumstances and as TET's review in the intervening period will not be able to contribute further insight. In addition, in 2026 TET will review whether DSIS implements the measures which the service has stated in its consultation responses for reviews of the area in 2025.

2.2.5 Review of DSIS's processing of information using artificial intelligence

In 2025, TET reviewed the processing of information by DSIS using artificial intelligence in four systems.

Use of artificial intelligence

Like other Danish authorities, DSIS increasingly uses various types of artificial intelligence (AI), including generative AI tools. This does not in itself give rise to comments from TET.

AI can improve efficiency and enable the processing of much larger volumes of data than traditional methods, but this often entails compromises. In many cases, AI does not surpass human accuracy, but offers gains in scale and throughput, which can still result in an improved overall output. However, if not handled correctly, the use of AI may introduce new risks, including reduced accountability, unintended bias or lack of explainability, which must be managed.

TET limits its review of AI to systemsthat operate with varying degrees of autonomy and are capable of inferring, learning or reasoning on the basis of data. This includes, among other things, machine learning (ML), where

systems are trained on large datasets to identify patterns and generate outputs such as probability scores or classifications, as well as self-learning algorithms which can adapt to new data and improve their performance over time without explicit reprogramming.

DSIS's use of AI takes place in closed systems in which the models and their underlying technology are not publicly available. Access to the AI functions is therefore administered exclusively by DSIS. This makes it possible for the AI functions to handle sensitive and classified information.

Comments by TET

TET's review of DSIS's processing of information using AI showed the following:

- DSIS had put one language model into operation which, in certain cases, whether intended or unintended, can produce responses that may contain personal data.

  In its review, TET used a number of simple prompts which, within a short time, in all cases produced a result containing personal data.

  TET's review thus showed that it was possible by simple means and with few resources to extract personal data from the implemented language model. Against this background, TET assessed that the AI function could not be regarded as anonymous, as it was possible - whether intended or unintended - to obtain personal data from queries. The language model therefore had to be regarded as containing personal data.

  Against this background, TET found that DSIS should consider how the service ensures that the rules of DSIS legislation on the processing of information, erasure and security of processing, including logging, are observed in relation to information in the language model.

  On the basis of the review, TET expressed understanding that DSIS has initiated a strategic initiative to strengthen and develop the use of AI/ML in the service, including that DSIS is at an early stage in the strategy. In addition, there is currently some development in the general data protection law understanding of the legal status of language models, and the legal position has therefore not yet been finally clarified.

  Against this background, TET chose not to criticise DSIS, but instead wished to draw the service's attention to TET's legal assessment of the implemented language model and to give the service the opportunity to consider it. TET and DSIS subsequently initiated a more detailed dialogue on the future use of the language model in question and the use of language models generally.

- DSIS had put one AI-based system into operation and classified it as a database under the DSIS Executive Order. TET and DSIS are in dialogue about the possibilities for observing the logging requirement in section 17, cf. section 18, of the DSIS Executive Order on Security Measures in relation to the specific database.

TET's other two reviews of DSIS's processing of information using AI did not give rise to any comments. The reviews were concluded without data-level reviews, as the systems were either under development or did not contain personal data.

2.2.6 Review of DSIS's use of other authorities' systems

In 2025, TET reviewed the use by DSIS of other authorities' systems by reviewing the service's use of ten systems belonging to other authorities to which selected employees of the service have direct access.

Other authorities' systems

DSIS has access to use a number of other authorities' systems. The processing rules of the DSIS Act do not apply to information processed in systems belonging to other authorities.

However, DSIS is responsible for ensuring that the service's employees do not misuse access to systems belonging to other authorities, which the service must prevent by complying with the legislation on the processing of personal data in these systems, cf. section 6a of the DSIS Act and the DSIS Executive Order on Security Measures.

Comments by TET

In its review of DSIS's use of one other authority's system, TET found that the service did not fully meet the requirement that the service must take the necessary technical and organisational measures to prevent information concerning natural and legal persons from coming to the knowledge of unauthorised persons, being misused or otherwise being processed in violation of the DSIS Act, cf. section 3 of the DSIS Executive Order on Security Measures.

In its assessment, TET attached weight to the fact that neither DSIS nor the authority concerned reviews the service's employees' user actions.

2.2.7 Review of DSIS's compliance with the rules on processing information concerning lawful political activities

In 2025, TET reviewed the organisational maturity of DSIS in relation to the service's processing of information concerning lawful political activities by reviewing the service's relevant internal guidelines, instructions and action cards. TET assessed that it was inappropriate to perform a data-level review of DSIS's processing of information concerning lawful political activities in 2025, considering the identified disagreement on the interpretation of section 11 of the DSIS Act (see section 2.8).

Processing of information concerning lawful political activities

Section 11(1) of the DSIS Act contains a provision that the participation by a natural person domiciled in Denmark in lawful political activities cannot in itself justify DSIS's processing of information about the person in question.

The prohibition against processing information concerning the exercise of lawful political activities is not absolute. This is indicated by the wording "in itself". DSIS may therefore process information concerning a person's lawful political activities when other circumstances mean that a person is of interest to the service.

If the person concerned is already in focus in connection with DSIS's performance of its tasks, the service may also process information concerning the person's lawful political activities if such information is relevant to the investigation. For example, a person may use the exercise of political activities as a pretext for planning, preparing or carrying out espionage, terrorism or violent extremist activity.

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

DSIS may also process information concerning a person's political activities with a view to clarifying whether the political activities are lawful. If DSIS's investigations show that the political activities are lawful, the information must be erased. This applies even if the general deletion deadlines for such information in section 9 of the DSIS Act or section 1(2) of the DSIS Executive Order have not yet been reached.

A principled provision with a long history

On 30 September 1968, the government of the time published a declaration prohibiting the registration of Danish citizens solely on the basis of lawful political activities.

The government declaration is based, among other things, on the consideration that it is a necessary prerequisite for free political formation of opinion in a democratic society that the formation of opinion is not limited by fear that citizens are being secretly registered by the intelligence services.

The prohibition in the registration declaration was continued in the Ministry of Justice's instruction to the Head of DSIS in 2009 and in the guidelines for DSIS's processing of personal data.

In light of this, the Wendler Pedersen Committee proposed that a provision be inserted in the DSIS Act which essentially continues the government declaration from 1968.

The Ministry of Justice endorsed the Committee's proposal and emphasised in the general notes to section 11 of the DSIS Act that the prohibition is intended, among other things, to prevent

- the intelligence service from being used by the government of the day to target political opponents,
- the service from developing into a state within the state, and
- citizens' exercise of their civil liberties from being limited by fear of secret registration.

Comments by TET

TET's review of DSIS's processing of information concerning lawful political activities showed that the service had generally established a sound process for training and guidance of the service's employees, including how employees are to use metadata in the service's record management system so that it becomes possible for the service's internal audit unit and TET to review the service's processing of information concerning lawful political activities.

In relation to selected systems, however, TET found that there were limited possibilities for linking relevant metadata, which may entail a risk that information cannot be retrieved in connection with DSIS's internal audit or TET's review of the service's processing of information concerning lawful political activities.

2.2.8 Review of DSIS's internal review

In 2025, TET reviewed the internal review of DSIS by examining the results of the service's internal review in 2024 and the service's planning of such review for 2025.

In addition, TET and DSIS's internal audit unit held quarterly meetings with a view to coordinating the internal and external review and to continuously exchanging experience from the review performed.

How does DSIS conduct internal review?

DSIS continuously conducts internal review of the service's compliance with specific parts of the DSIS Act, etc. For the purpose of organising the internal review, DSIS annually prepares a risk analysis of the service's compliance with statutory requirements and a plan for the internal review in the following year. DSIS continuously informs TET about the organisation and results of the internal review, including by forwarding the service's risk analysis and review plan.

Comments by TET

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

TET found that DSIS had organised and conducted its internal reviews satisfactorily, including ensuring that the reviews were well documented and that the sample reviews produced audit-accurate results. Furthermore, DSIS continuously followed up on the results of the service's internal review. Finally, the review showed a high degree of correspondence between TET's and DSIS's independent risk analyses concerning the risk of non-compliance with legislation in the service.

2.2.9 Follow-up on TET's review of DSIS in 2024

TET annually reviews whether DSIS has implemented the actions which the service, on the basis of TET's review in the previous year, stated that it would implement.

In 2025, TET followed up on TET's review of DSIS in 2024.

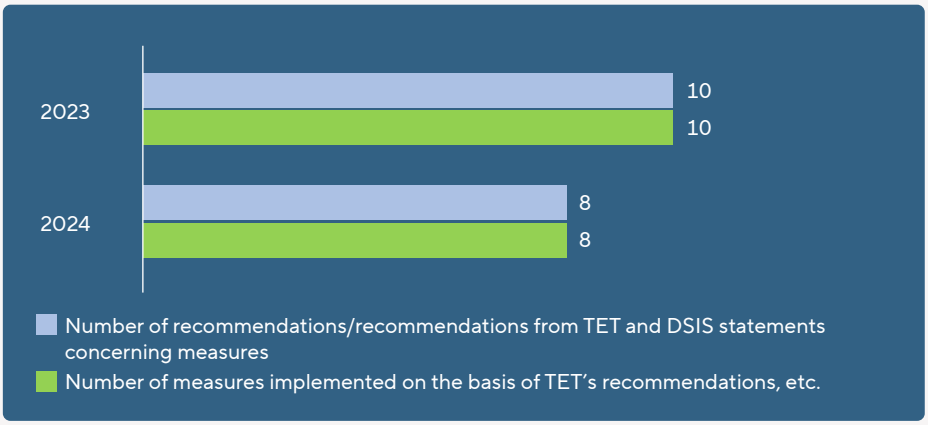
TET reviewed the information which DSIS, in connection with TET's reviews in 2024, had agreed to erase, and reviewed the recommendations which TET, in connection with completed reviews, found it necessary to implement.

The purpose of the review was also to ascertain whether DSIS had implemented the measures which, in connection with the reviews in 2024, the service had stated to TET that it would implement.

Comments by TET

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

TET noted that, in eight cases, DSIS had forwarded notifications or implemented the recommendations and measures which TET had either recommended or which the service had stated that it would implement.



2.2.10 TET's technical investigations and mapping of DSIS's IT infrastructure

In 2025, TET conducted verification reviews and mapping of the IT infrastructure of DSIS by carrying out

- verification review of database servers for the purpose of clarifying whether TET is aware of all databases in DSIS,
- verification review of file servers for the purpose of clarifying whether TET is aware of all file shares in DSIS, and
- mapping of DSIS's server infrastructure.

In 2025, TET had also planned a mapping of workflows in selected departments of DSIS with a view to identifying systems, storage points and similar elements which had not been identified by TET's mapping of the service's IT infrastructure.

Mapping as a prerequisite for risk management

DSIS'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 infrastructure and perform TET's tasks, in 2025 TET reviewed and verified extensive parts of DSIS's IT infrastructure and worked continuously to ensure up-to-date knowledge of the service's systems.

It is a prerequisite for meaningful review of DSIS that TET has knowledge of the service's entire IT infrastructure, so that the review can be directed at the parts of the infrastructure which pose the greatest risk of processing in violation of legislation.

Comments by TET

The technical examinations and mappings performed by TET showed the following:

- In the verification review of database servers, TET found that DSIS's response to TET's consultation in connection with the mapping of the service's server infrastructure could not be described as adequate.
- TET found it unsatisfactory that, in connection with TET's mapping of workflows in selected departments of DSIS, the service initially chose not to comply with TET's request to set a time for mapping a workflow in the service.

  TET assesses that DSIS's failure to respond regarding the fixing of a date for the mapping delayed the process unnecessarily. TET expects DSIS to answer and, to the greatest extent possible, comply with TET's questions and requests in accordance with section 20 of the DSIS Act.

  Against this background, it was not possible for TET to perform the mapping before the end of 2025.

TET's verification review of file servers did not give rise to any comments.

2.3 DSIS's briefing of TET

In 2025, DSIS continuously informed TET about the service's decisions

- to refrain from erasing information which had reached the deletion deadlines of 15 years and 10 years, respectively,
- exceptionally to set deletion deadlines longer than five years for persons, entries or information in the service's special databases, and
- concerning significant questions relating to DSIS's processing of information concerning natural and legal persons.

Furthermore, DSIS continuously informed TET about the results of the service's internal review.

Statutory duty of notification

It follows from the preparatory works of the DSIS Act and chapters 1 and 6 of the DSIS Executive Order that DSIS must continuously inform TET about the application of a number of provisions of the Act. Under the Executive Order, DSIS must thus inform TET of the following:

- DSIS's decisions under section 9(2) of the DSIS Act to refrain from erasing information which has reached the 15-year deletion deadline in subsection (1) of that provision
- DSIS's decisions under section 1(4) of the DSIS Executive Order to refrain from erasing files which have reached the 10-year deletion deadline in subsection (2) of that provision
- DSIS's decisions under section 2(2) of the DSIS Executive Order exceptionally to set deletion deadlines longer than five years for persons, entries or information in the service's special databases, cf. subsection (1) of that provision
- DSIS's decisions under section 2(2), second sentence, of the DSIS Executive Order to set deletion deadlines which are not calculated from the time of entry because special needs so require, cf. subsection (1) of that provision
- Cases in which DSIS is exceptionally unable to comply with the deadline for entering information into records under section 3(1) of the DSIS Executive Order
- DSIS's use of section 4 of the DSIS Act on procurement of information from other public administrative authorities which may be assumed to be of significance for the performance of the service's tasks concerning prevention and investigation of offences under chapters 12 and 13 of the Criminal Code

- Cases concerning security clearance where DSIS discloses information from the service's records or databases to authorities other than the Ministry of Justice, the prosecution service or other parts of the police
- All significant questions relating to DSIS's processing of information
- DSIS's internal review of the processing of information concerning natural and legal persons under sections 10 and 11 of the DSIS Executive Order
- New administrative guidelines of relevance to TET's review
- Other guidelines, if TET so requests

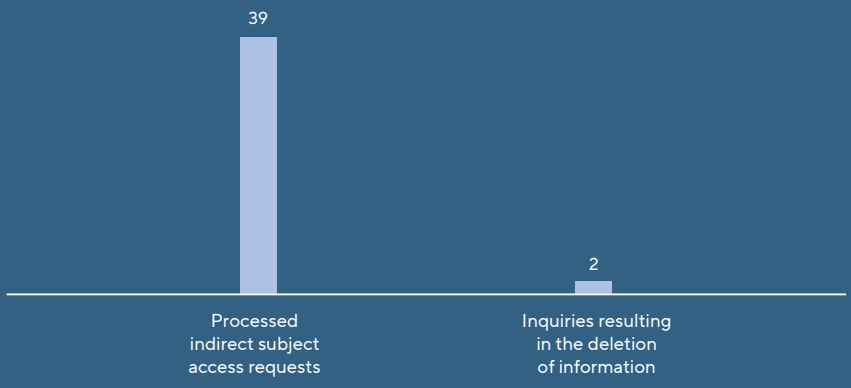
2.4 Requests for access under sections 12 and 13 of the DSIS Act

In 2025, TET processed requests from 39 natural or legal persons asking TET to examine whether DSIS was processing information about them without being entitled to do so. In this connection, TET found that, in 37 cases, DSIS was not processing information about the persons concerned without being entitled to do so.

In two cases, DSIS processed information about the persons concerned which no longer fulfilled the conditions for processing in section 7(1) or section 8(1) of the DSIS Act. Against this background, DSIS erased the information. In this connection, it should be noted that DSIS is not under an obligation on an ongoing basis and of its own motion to review the service's files and documents, etc., in order to assess whether the said conditions for processing continue to be met.

The average case processing time for the completed requests was 75 working days in 2025, of which 13 days constituted case processing time at DSIS.

Requests for indirect subject access



TET seeks to answer requests for access as quickly as possible, but the examinations may be both resource-intensive and complicated. The results of the examinations are submitted to TET at monthly meetings, at which TET decides how the requests are to be answered.

It should be noted that it is a prerequisite for TET's performance of its task in connection with the indirect subject access scheme that personal data is stored in DSIS's IT systems in accordance with sections 1-3 of the DSIS Executive Order, that it is possible to carry out effective searches in the systems concerned, and that it is possible to erase information at data level.

Processing of requests for access

When a natural or legal person asks TET to examine whether DSIS is processing information about the person concerned without being entitled to do so, TET conducts an examination at the service, where TET has access to any information and all material of significance to TET's activities.

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

Once the examinations have been completed, TET assesses whether, in TET's view, DSIS is processing information about the person concerned without being entitled to do so. If TET finds this to be the case, TET orders DSIS to erase the information. Once TET has ensured that information about the person concerned is no longer being processed without entitlement, TET responds to the request.

Where special circumstances justify doing so, TET may order DSIS to give a natural or legal person access to information which the service processes about them, or access to whether the service is processing information about them.

In cases where TET receives a request for access to information, TET examines which information DSIS may process about the person concerned, just as the service's comments are obtained 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 justify ordering DSIS to grant full or partial access to the information referred to.

Which systems are covered by TET's examinations?

TET annually prepares a separate risk assessment and analysis for TET's tasks in relation to DSIS 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.

TET's examinations cover a number of central systems in DSIS. TET has previously assessed - considering the current legal framework for TET's processing of indirect subject access requests - that the examinations should cover a further four systems which, for various reasons, are not covered at present, which affects the completeness of TET's examinations. TET and DSIS are in dialogue about a joint clarification of the scope of the indirect subject access scheme, including which systems are currently covered by the scheme.

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

2
systems in which it is not technically possible to carry out an effective search

1
system out of operation

1
system regarding which DSIS and TET are in dialogue

2.5 Reports to the external whistleblower scheme for DSIS

In 2025, TET received seven reports to the whistleblower scheme. All seven reports were rejected, as the reporting person was either not covered by the protected category of persons under section 3, no. 7, letters a-h, of the Whistleblower Act, or the content of the report was not covered by the scope of application of the Whistleblower Act. The reports did not otherwise give rise to further processing/examination or notification of DSIS or the Ministry of Justice.

Reports to the whistleblower scheme

The external whistleblower scheme for DSIS

TET is responsible for the external whistleblower scheme concerning DSIS, which is a supplement to the service's internal whistleblower scheme and other existing possibilities, such as contacting HR or employee representatives.

A report is as a general rule anonymous unless the whistleblower discloses their identity or provides contact details.

TET has designated a limited number of employees who are responsible for administering the whistleblower scheme and who process the reports in such a way that they are kept separate from TET's other tasks and functions.

In connection with reports to TET's whistleblower scheme for DSIS, TET performs an initial assessment and examination with a view to determining whether a report has been submitted by a person entitled to submit a report to the scheme, and whether the report is covered by the scope of application of the Whistleblower Act. The subsequent handling of each enquiry depends on the content and nature of the report.

Who may submit information as a whistleblower?

The following persons may submit reports to TET's external whistleblower scheme for DSIS:

- Employees of DSIS
- Paid or unpaid trainees at DSIS
- Persons who report or publicly disclose information to which they have gained access in a work-related context which has since ceased, i.e. former employees of DSIS
- Persons whose work-related relationship has not yet begun and who report information concerning breaches to which they have gained access during the recruitment process or other pre-contractual negotiations with DSIS
- Other persons protected under section 3, no. 7, letters a-h, of the Whistleblower Act

Persons not covered by the above category of persons cannot report to TET's whistleblower scheme for DSIS.

2.6 DSIS's case processing times in 2025

DSIS's case processing times in 2025	
Number of legal consultations of DSIS	21 consultations
Number of legal consultations answered within the deadline	18 consultations
Average number of days for overdue consultations	10 days*

* Of the three consultations answered after the deadline set by TET, DSIS answered two of the consultations within one day after expiry of the deadline, while the service answered the third consultation 27 days after expiry of the deadline.

2.7 Completed reviews of the PNR Unit in 2025

TET reviews the processing by the PNR Unit of information concerning airline passengers on behalf of DSIS and the Danish Defence Intelligence Service (DDIS).

In 2025, TET reviewed the PNR Unit's processing of information concerning airline passengers on behalf of DDIS by reviewing the PNR Unit's processing of bulk requests from the service.

TET's comments

TET's review of the PNR Unit's processing of information concerning airline passengers on behalf of DDIS in 2025 did not give rise to any comments.

2.8 Cases submitted to the Minister of Justice for decision

Since 2014, DSIS and TET have submitted seven questions of interpretation to the Minister of Justice, of which three questions remain unresolved.

On 5 February 2025, the Minister of Justice requested DSIS to resume discussions with TET concerning four questions of interpretation which had been submitted to the Minister of Justice but had not yet been decided, so that the new TET could have the opportunity to consider the questions.

In dialogue with DSIS, TET has continuously throughout 2025 considered whether the questions of interpretation should be resubmitted to the Minister of Justice.

Submission of questions to the Minister of Justice

As part of its review of DSIS, TET may issue statements to the service in which TET may, among other things, state its view as to whether the service complies with the rules of the DSIS Act.

At the conclusion of each review, TET issues a statement to DSIS describing the results of TET's review. The statement may also contain a description of one or more measures which TET assesses that DSIS should take. If DSIS exceptionally decides not to comply with a recommendation in a statement from TET, the service must notify TET thereof and - without undue delay - submit the matter to the Minister of Justice for decision. If the Minister of Justice were to decide not to comply with the recommendation from TET, the Government must inform the Parliamentary Intelligence Services Committee (UET) thereof. TET's possible responses in relation to DSIS are described in more detail in section 19 of the DSIS Act.

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

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

Question	Date of submission	Status
Whether the prohibition in section 11(1) of the DSIS Act and the obligation to remove information pursuant to subsection (2) apply to the service's processing of information concerning individuals' political activities in connection with participation in lawful demonstrations.	25 November 2024 (originally) and 26 November 2025 (resubmitted)	On 5 February 2025, the Minister of Justice requested DSIS to resume discussions with TET so that the new TET could have the opportunity to consider the question. TET discussed the question and agreed with the previous TET's interpretation and, on 27 June 2025, requested DSIS to submit the question to the Minister of Justice again. DSIS resubmitted the question to the Minister of Justice on 26 November 2025.
Whether section 18(2) of the DSIS Executive Order contains an independent obligation for DSIS to document whether information covered by the provision has been accessed, who accessed it and for what purpose. Further addressed in the present report (section 3.2.8).	10 July 2024 (originally) and 26 November 2025 (resubmitted)	On 5 February 2025, the Minister of Justice requested DSIS to resume discussions with TET so that the new TET could have the opportunity to consider the question. TET discussed the question and agreed with the previous TET's interpretation and, on 29 October 2025, requested DSIS to submit the question to the Minister of Justice again. DSIS resubmitted the question to the Minister of Justice on 26 November 2025.

Question	Date of submission	Status
Whether TET has authority to review DSIS's deletion of material obtained under the rules of the Danish Administration of Justice Act. The submission was made on the basis of a number of TET's reviews in 2022, which gave rise to doubts as to how the rules on the destruction of material obtained under section 791 of the Danish Administration of Justice Act interact with the rules on deletion in section 9 of the DSIS Act and section 2(2) and (3) of the DSIS Executive Order.	4 July 2023	Clarified by Act No. 666 of 11 June 2024 amending, among other things, the Act on DSIS. The amendment states, among other things, that TET must perform ex post legality review of DSIS's operational tasks, including review of whether DSIS has acted in accordance with a court order.
Whether TET can review whether DSIS complies with the national security standard for information security ISO 27001 in connection with reviewing DSIS's compliance with the DSIS Executive Order on Security Measures. Discussed in more detail in TET's annual report for 2022 (section 2.2.10).	27 June 2022	On 5 February 2025, the Minister of Justice requested DSIS to resume discussions with TET so that the new TET could have the opportunity to consider the question. On 30 January 2026, TET informed DSIS that TET wished the case to be submitted to the Minister of Justice again if the service continued to disagree with TET's interpretation. TET and DSIS remain in dialogue on this matter.
Whether the DSIS Act and the DSIS Executive Order apply to the processing of information in a database made available to DSIS by another agency. Discussed in more detail in TET's annual report for 2023 (section 3.7.1).	14 December 2021	Decided by the Minister of Justice on 2 June 2022. The Minister of Justice found that the DSIS Act and the DSIS Executive Order do not apply to the processing of information in a database made available to DSIS by another authority solely for the purpose of the service's processing of information in the database.
Whether time limits for deletion for databases, see section 2(2) of the DSIS Executive Order, should be calculated from the time of entry. Discussed in more detail in TET's annual report for 2021 (section 3).	TET has not been informed when DSIS submitted the case to the Minister of Justice.	Decided by the Minister of Justice on 1 November 2021. The decision led to clarification of the DSIS Executive Order, including an amended provision in section 2(2).
Whether the DSIS Act with accompanying comments and subsequent Executive Order should be understood to mean that personal information which DSIS no longer considers necessary for the performance of its activities must be deleted, see sections 7(1) and 8(1) of the DSIS Act, cf. section 5(5) of the Data Protection Act, even if the information is included in a document whose other information is still necessary for DSIS. Discussed in more detail in TET's annual report for 2016 (section 5).	12 May 2015	Decided by the Minister of Justice on 23 September 2016. The decision led to an amendment of the DSIS Act, including a new provision in section 9a.

2.9 Requests from the Parliamentary Intelligence Services Committee

The Parliamentary Intelligence Services Committee (UET) may, in special cases, request TET to examine specific cases, courses of events, issues, etc., which fall within TET's area of competence.

The scheme is intended for extraordinary situations. It may be in connection with cases of principled or otherwise more far-reaching significance for the general confidence of the population in the intelligence services, for example cases which have been the subject of particular public debate. It may also be as follow-up on significant issues in relation to the activities of the intelligence services which TET may have pointed out in TET's annual reports on its activities concerning, respectively, DSIS and DDIS.

It is a condition for UET to request that TET initiate an examination that the object of the examination falls within TET's area of competence.

This entails, among other things, that TET will not be able to examine whether, for example, the intelligence services have acted expediently in connection with their intelligence professional discretion. The examination must therefore be linked to a subsequent legality review. TET will also not be able to examine whether, for example, the content of an order from the courts is, in TET's view, correct, as TET must organise its review so that it does not in reality become a review or supervisory body for matters assigned to the courts. In the same way, TET will not be able to examine matters related to administrative issues, for example the intelligence services' accounts and budgets.

For the same reason, TET will not, as part of an examination, be able to assess whether individual employees of the intelligence services may have committed errors or neglect that may give rise to seeking to establish liability against the persons concerned, or to criticism otherwise being expressed of the persons concerned. TET's task is therefore solely to assess the activities of the intelligence services and not the individual employees.

To the extent that the object of the examination falls within TET's area of competence, UET will as a general rule be able to request that TET examine cases, courses of events, issues, etc., related to matters which took place before the entry into force of the Act. It should be noted, however, that it falls outside TET's competence to examine cases, etc., which do not have a certain connection to a current political or public debate, or which are not otherwise linked to a matter of current significance for the oversight of the intelligence services. It will therefore not be possible to initiate examinations of past matters which must be regarded as historical without any current relevance for the oversight of the intelligence services.

TET itself disposes of its resources and the detailed organisation of investigations on the basis of requests from UET, including the scope of the examinations.

TET received its first request from UET on 13 November 2025.

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)
See standard for TET's risk and materiality assessment (section 2)
See standard for TET's choice of method, performance of checks and verification (section 3)
Mapping of IT infrastructure of the DSIS, DDIS, and PNR Unit
QUALITY ASSURANCE
External consultation on factual matters
QUALITY ASSURANCE
Approval at managerial level
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
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 1 mapping, 2 risk assessment and planninng and 3 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.

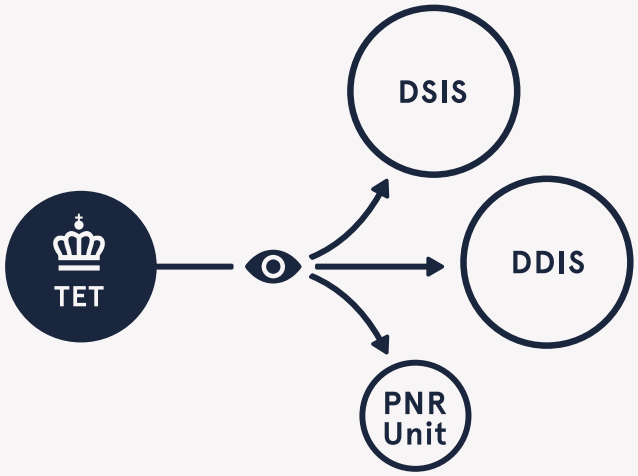
For further information on TET's review methodology, reference is made to TET's published standards, which are available on TET's website.

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.

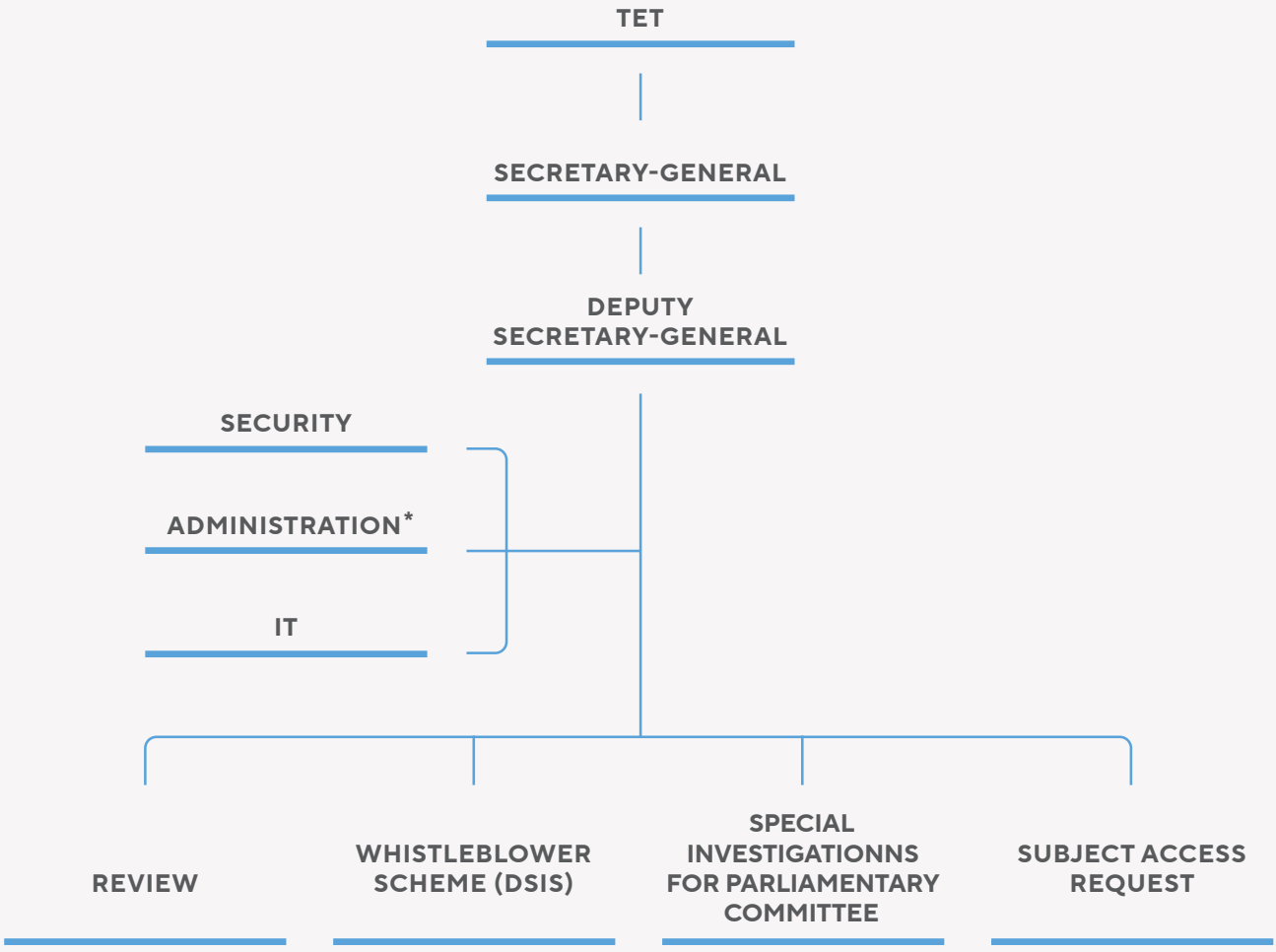
Rasmus Blaabjerg (Member)

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.

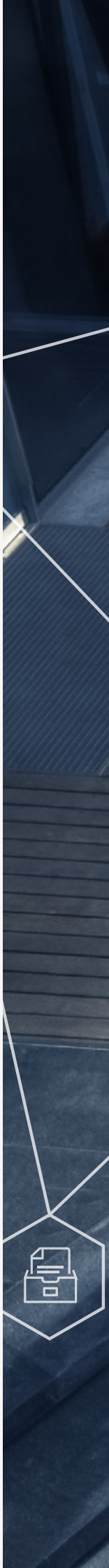
TET is served by a separate unit at the Danish Data Protection Agency (TET Unit), which in professional matters reports directly to the members of TET. At the end of 2025, TET Unit consisted of a legal head of office responsible for day-to-day management, a political science deputy head, two legal officers,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