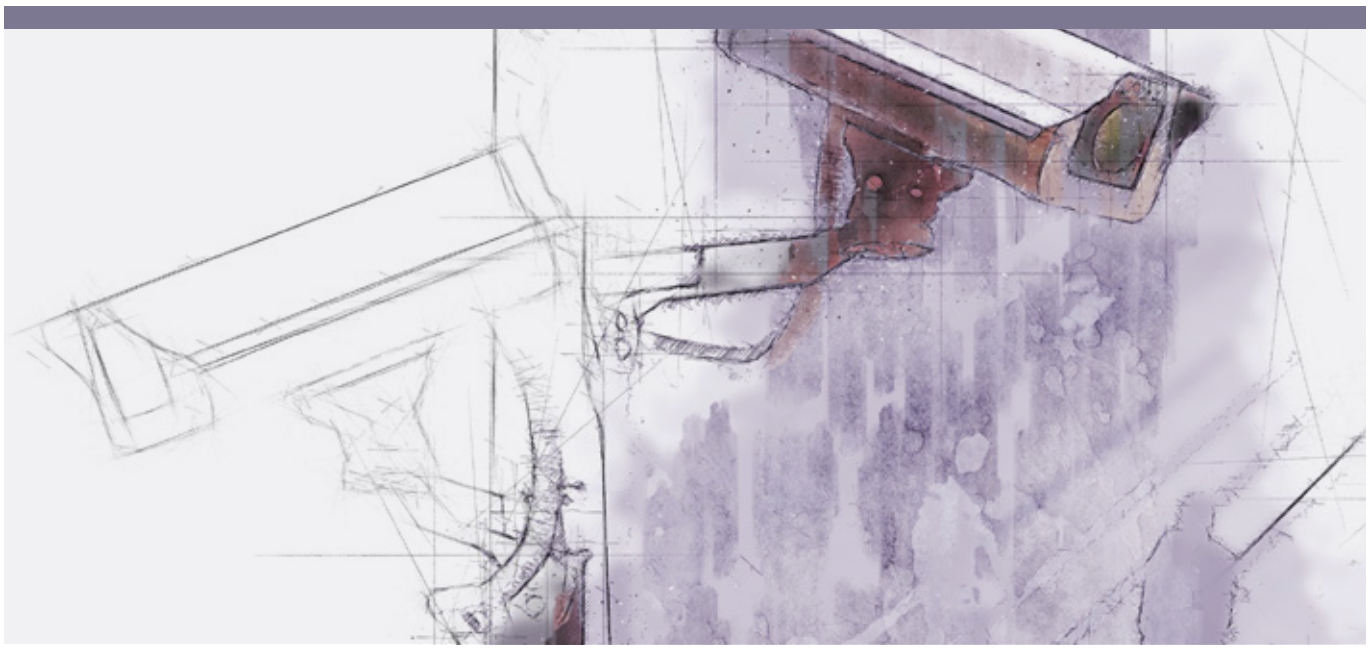
Danish Intelligence Oversight Board



Annual report 2022

Danish Security and Intelligence Service (DSIS)

Contents

To the Minister of Justice

The Danish Intelligence Oversight Board (TET) hereby submits its report on its activities concerning the Danish Security and Intelligence Service (DSIS) for 2022 in accordance with section 22 of the Danish Security and Intelligence Service (DSIS) Act (Consolidated Act No. 231 of 7 March 2017, as amended most recently by Act No. 1706 of 27 December 2018). The annual report must be submitted to the Parliamentary Intelligence Services Committee and subsequently published.

The report also contains a description of TET's activities concerning the PNR Unit of the Danish National Police (RPNR) in 2022.

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

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

- procurement of information, including collection and obtaining
- internal processing of information, including time limits for erasure of information
- disclosure of information, including to the Danish Defence Intelligence Service (DDIS) and to other Danish administrative authorities, private individuals or organisations, foreign authorities and international organisations, and
- the prohibition of processing information about natural persons resident in Denmark solely on grounds of their legal political activities

Furthermore, TET oversees compliance with the provisions of the PNR Act concerning

- procurement of information
- internal processing of information, including unmasking, and
- disclosure of information

when the RPNR procures, processes and discloses information on behalf of DSIS.

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

Copenhagen, June 2023

Michael Kistrup
Chair of the Danish Intelligence Oversight Board

Introductory comments

As the national security and intelligence service, DSIS is tasked with the responsibility of preventing, investigating and countering operations and activities that pose or may pose a threat to Denmark. DSIS thus performs a vital function in ensuring a free, democratic and safe society.

In order to perform this nationally important function, DSIS has very broad powers under the law to procure information on citizens and businesses. In order to ensure due process protection for the individual citizen and business, DSIS' powers are counterbalanced by rules governing the subsequent processing and erasure by DSIS of the information procured, including in relation to the DSIS' security of processing.

In 2022, TET has carried out in-depth and intensive compliance reviews with regard to DSIS, including of DSIS' processing of information and compliance with time limits for erasure. TET's compliance reviews of DSIS in 2022 are described in more detail in section 2.

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

In 2022, because of DSIS' processing times in relation to responding to seven consultation notices, TET experienced that the work involved in its risk assessment of DSIS, the planning of next year's reviews and the preparation of its annual report on DSIS has been impeded. In addition, DSIS' processing times have in specific cases limited TET's possibilities of performing supplementary reviews of DSIS' processing of information.

In 2022, TET has been in dialogue with DSIS about its case processing times, and on that basis, TET and DSIS have developed a new consultation handling process, which supports DSIS in responding to TET's consultation questions within the agreed deadline.

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

Finally, in 2022, DSIS has reported to TET on its extensive efforts to bring its IT infrastructure up to date, among other things with a view to ensuring increased compliance and support for DSIS' internal controls and TET's independent oversight. DSIS has informed TET that the project is expected to run for a number of years and that the purpose is, among other things, to ensure better IT support for the areas that experience has shown to be challenging.

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

Scale of TET's comments

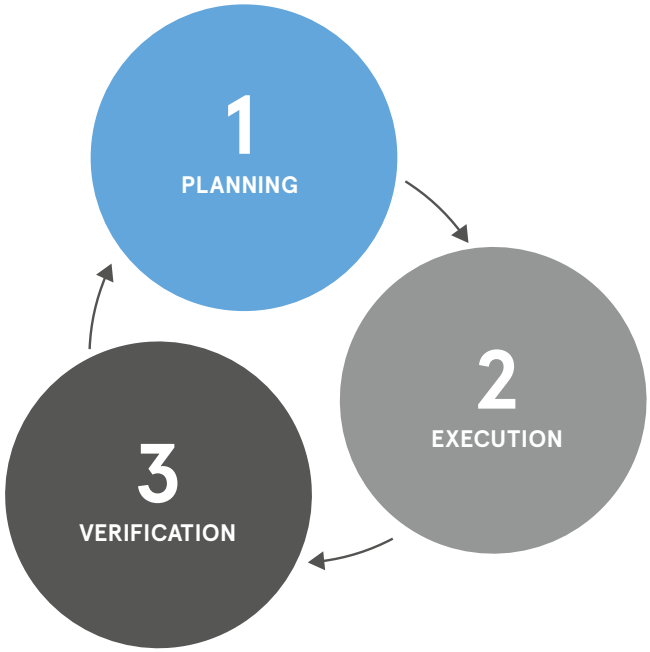
TET's comments are based on the following scale:

Comments	Background to comments
»[...] **does not give rise to any comments**«	Used when TET agrees with DSIS or RPNR 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 DSIS, RPNR 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 DSIS or RPNR having demonstrated a willingness to ensure the necessary remedial action.

1. Oversight method

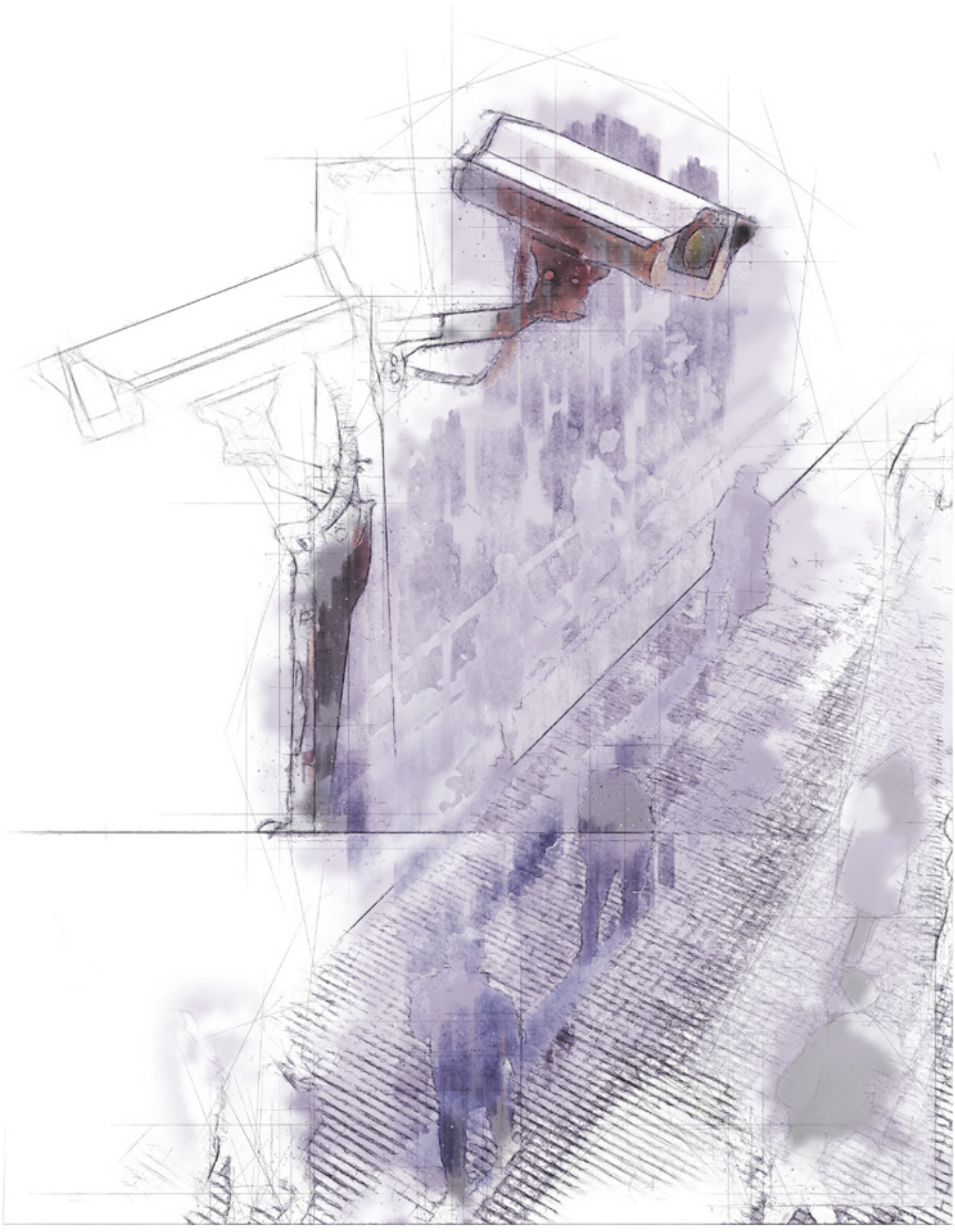
TET continuously works to improve the methods it uses in the planning and performance of its oversight of DSIS in order for the oversight to be as effective as possible within the framework set for the work of TET.

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



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

The purpose of the risk analyses is to ensure that the oversight activities are focused on the areas with the highest risk of errors and that other relevant factors are taken into account, e.g. areas where TET's oversight activities are given special weight by the legislators such as the rules on legal political activity.



Areas that are deemed to have a low risk of errors are generally reviewed once every five years in order to achieve completeness in the oversight of DSIS and ensure that the assessment of the risk of errors in the area still holds.

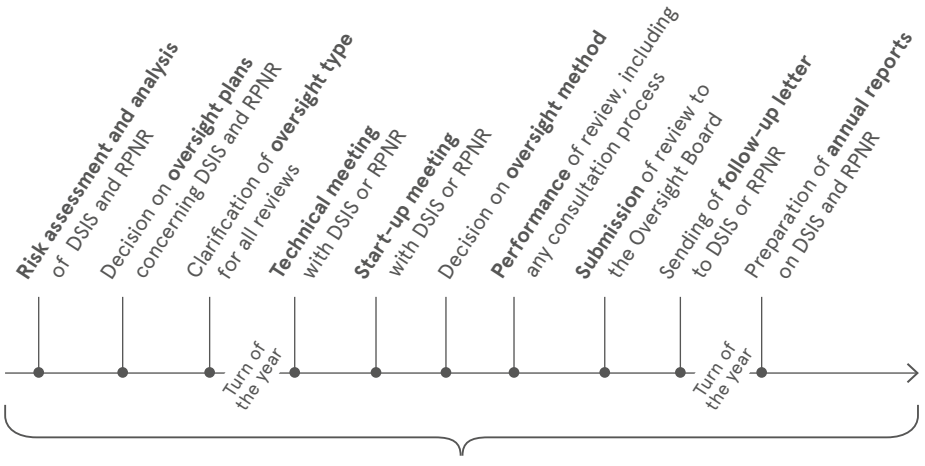
The reviews **2)** are conducted regularly throughout the year based on the DSIS oversight plan approved by TET. TET does not define the methods for the individual reviews in connection with the preparation of risk assessments and analyses, and the choice of method must thus be determined prior to initiating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

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

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

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

TET's activities include the following stages:



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

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

Prior to initiating its reviews for a particular year, TET will share its risk analysis and oversight plan with DSIS for the purpose of ensuring, among other things, openness

about TET's assessment of the situation in DSIS. The openness also allows DSIS to take into account TET's reviews in the organisation of its own internal controls, which contributes to TET's reviews and the internal controls collectively covering a larger part of DSIS' activities. Finally, the openness allows DSIS to dedicate sufficient resources to serve TET.

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

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

2. TET's review

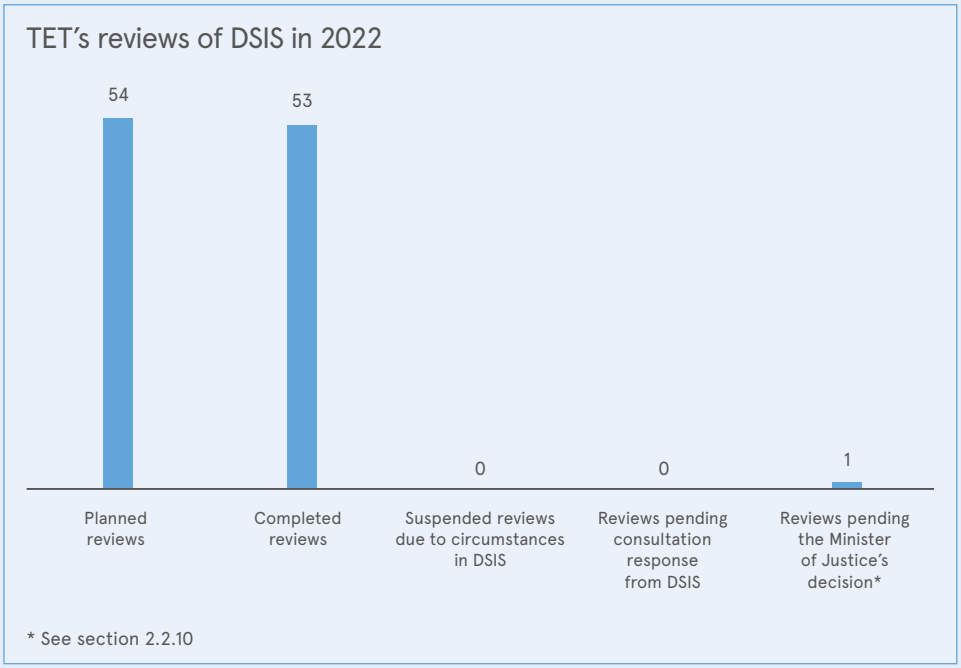
2.1 Summary of TET's reviews in 2022

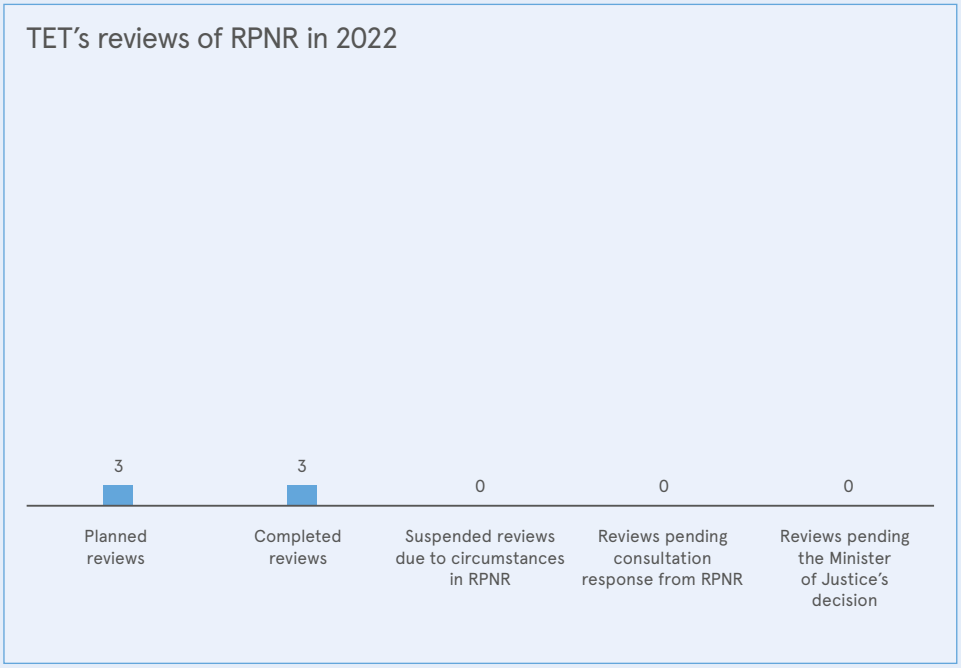
In 2022, TET has completed 53 out of 54 planned reviews of DSIS and 3 out of 3 planned reviews of the PNR Unit of the Danish National Police (RPNR).

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

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

- 19 out of 53 reviews of DSIS and 3 out of 3 reviews of RPNR did not give rise to any comments.
- TET found the following highly criticisable:
  - That DSIS had not established logging for two of its special databases, see section 17 of the DSIS Executive Order on Security Measures, considering that the databases were established before 1 January 2014 and in 2015, respectively. DSIS subsequently informed TET that it had now established a temporary logging solution for the databases (section 2.2.5).
  - That DSIS had not established logging in one of its special databases, see section 17 of the DSIS Executive Order on Security Measures, considering that the database was established in 2018 and that the system had been used for processing confidential information since the entry into force of the DSIS Act on 1 January 2014. DSIS subsequently informed TET that it had now established a temporary logging solution for the database (section 2.2.5).
- TET found the following criticisable:
  - That DSIS processed 104,818 files from cases investigated by DSIS in cooperation with the police districts on a shared drive in violation of sections 7(2) and 8(2) of the DSIS Act, see section 17, cf. section 18, of the DSIS Executive Order on Security Measures, and DSIS guidelines on the use of transit systems, particularly in view of the fact that it was standard DSIS practice to process information for more than the permitted 28 days on the transit system when a criminal case was to be transferred from DSIS to the police districts (section 2.2.6).





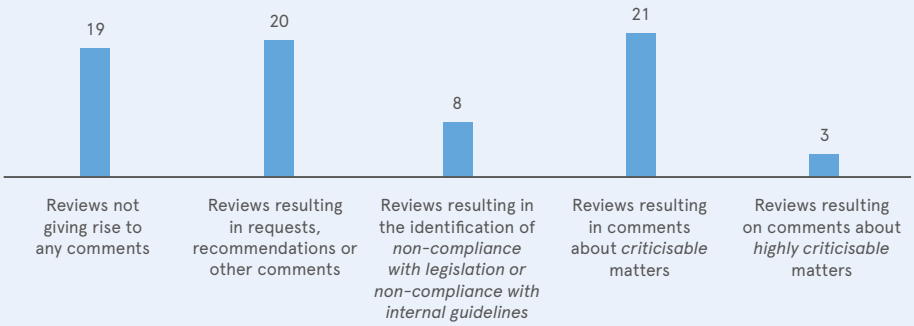
- That DSIS in 497 cases processed information about persons about whom DSIS had started to consolidate information more than ten years ago in violation of sections 1(2) and 2(2) of the DSIS Executive Order, as the consolidated information should have been erased when the related source data (files, documents and entries) was erased (section 2.2.2).

- That DSIS processed information about 19 persons and 84 organisations in violation of section 9a(1) of the DSIS Act, as DSIS, in connection with TET's review in 2021, erased the information in its production environment without erasing the copy of the information in two different pre-production environments (section 2.2.2).

- That DSIS processed 62,040 files in violation of section 9a(1) of the DSIS Act in a pre-production environment, as DSIS should have erased the information after the development of a piece of software (section 2.2.2).

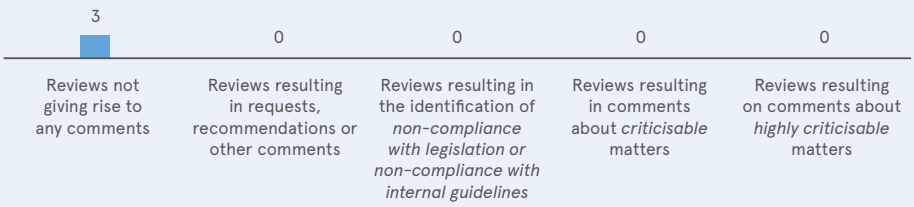
- That DSIS continued having difficulties observing the statutory requirements for erasure of consolidated information when the related source data is erased, considering that TET generally pointed out DSIS' challenges in this respect already in its annual reports for 2014 and 2015 as well as for 2020 and 2021, and that TET's reviews in the period from 2016 to 2021 specifically showed that DSIS continued to be having challenges in this respect (section 2.2.2).

Result of TET's review of DSIS in 2022



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

Results of TET's review of RPNR in 2022



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

- That DSIS did not inform TET about the existence of a special database until 2022, despite the fact that the database has been used since 2020, see section 2(2) of the DSIS Executive Order (section 2.2.5).

- That DSIS processed 245 files on a shared drive in violation of sections 7(2) and 8(2) of the DSIS Act, see section 17, cf. section 18, of the DSIS Executive Order on Security Measures, and DSIS guidelines on the use of transit systems, particularly in view of the fact that DSIS to a certain extent used the drive for case management purposes (section 2.2.6).

- That DSIS processed 4,423 emails in shared mailboxes in violation of sections 7(2) and 8(2) of the DSIS Act, see section 17, cf. section 18, of the DSIS Executive Order on Security Measures, and DSIS guidelines on the use of transit systems (section 2.2.6).

- TET's reviews showed the following:

  - That DSIS in specific cases has difficulties observing section 17, see section 18, of the DSIS Executive Order on Security Measures in relation to the processing of information in transit systems (section 2.2.10).

  - That DSIS' access restrictions in specific cases were insufficient, see sections 10 and 11 of the DSIS Executive Order on Security Measures, as a very large amount of personal information was processed on a drive that was not properly protected by access restriction (section 2.2.10).

- In 2022, TET received subject access requests from 45 natural or legal persons, asking TET to review if DSIS was processing information about them in violation of DSIS legislation. In that connection, TET found that in 12 cases DSIS had processed information about the persons in question in violation of the conditions of processing in section 7(1) or 8(1) of the DSIS Act. In this connection, it should be noted that DSIS is not required beyond that to review its cases and documents, etc. of its own motion in order to assess if the above conditions of processing are still met. DSIS has on that basis erased the information.

2.2 Review of DSIS in 2022

For the purpose of reviewing DSIS' compliance with the provisions of the DSIS Act, the DSIS Executive Order and the DSIS Executive Order on Security Measures when processing information about natural and legal persons, TET has carried out reviews in 2022 of DSIS'

- opening of new files (2.2.1),
- compliance with time limits for erasure (2.2.2),
- use of other agencies' systems (2.2.3),
- compliance with the rules on legal political activity (2.2.4),
- special databases (2.2.5),
- transit systems (2.2.6),
- processing of material classified as TOP SECRET (2.2.7),
- internal controls (2.2.8),
- compliance with the rules on material subject to legal deposit (2.2.9), and
- compliance with the rules on security of processing (2.2.10).

Furthermore, in 2022, TET has completed

- follow-up on its reviews of DSIS in 2021 (2.2.11), and
- technical reviews and mapping of DSIS' IT landscape (2.2.12).

2.2.1 Reviews of DSIS' opening of new files

In 2022, TET completed reviews of DSIS' opening of new files in 2021 within the areas of espionage, terrorism, non-proliferation and other operative files.

Furthermore, in 2022, TET performed reviews of DSIS' opening of new files within the areas of espionage, terrorism, non-proliferation and other operative files.

Comments by TET

In connection with the review in 2021, TET found that DSIS' processing of information about a specific person no longer met the conditions in section 7(1) of the DSIS Act and that, based on the review, DSIS erased the information, see section 9a(1) and (2) of the DSIS Act, cf. section 7.

In connection with the review in 2021, TET found it problematic that it only got access to one of the files sampled 82 working days after TET had requested access.

In connection with its review in 2022, TET became aware that it was not possible to access two of the files sampled. Against this background, TET requested DSIS for access

to the files in question, but DSIS informed TET that it could not have access to the files as they contained particularly sensitive information of a nature described in the specific explanatory notes to section 20 of the DSIS Act. The review was completed on the basis of the information available. It is noted that DSIS suggested to TET alternative ways of carrying out the reviews, but that TET did not find the alternatives adequate.

TET's reviews of DSIS' opening of new files in 2021 and in 2022 within the areas of espionage, terrorism, non-proliferation and other operative files did not otherwise give rise to any comments.

2.2.2 Review of DSIS' compliance with time limits for erasure

Each year, DSIS conducts an audit of those of its files which will reach the time limit for erasure of ten years in order to determine whether the file concerns inquiries or investigations under sections 5 and 6 of the DSIS Act, or whether the file is to be erased or extended, see section 1(2) and (4) of the DSIS Executive Order.

DSIS has established a number of pre-production environments in order to be able to test and develop software before it is commissioned in DSIS' production environment. Data from the production environment is sometimes used for software testing and development purposes. The time limits for erasure under DSIS legislation also apply to information in pre-production environments.

In 2022, TET reviewed DSIS' compliance with time limits for erasure by reviewing

- information held by DSIS about natural persons on whom DSIS had started to consolidate information more than ten years ago,
- information held by DSIS about organisations about which DSIS had started to consolidate information more than ten years ago, and
- DSIS' files more than ten years old in DSIS' previous file system,
- DSIS' decisions in 2022 not to erase files under section 9(2), see subsection (1), of the DSIS Act and section 1(4), cf. subsection (2), of the DSIS Executive Order, and
- DSIS' processing of information in three pre-production environments.

Comments by TET

TET's review of DSIS' compliance with time limits for erasure gave rise to the following comments:

- TET found it criticisable that in 497 cases DSIS processed information relating to persons about whom DSIS has started to consolidate data more than ten years ago, in violation of sections 1(2) and 2(2) of the DSIS Executive Order, as the consolidated data should have been erased when the related source data (files, documents and entries) was erased.
- TET found it criticisable that in 27 cases DSIS processed information relating to persons about whom DSIS has started to consolidate data more than ten years ago to which source data should have been attached, in violation of sections 1(2) and 2(2) of the DSIS Executive Order, as the attachment of relevant source data is decisive

for DSIS to be allowed to consolidate information about persons in the system in question.

- TET found it criticisable that in 26 cases DSIS processed consolidated data relating to organisations about which DSIS has started consolidating data more than ten years ago, in violation of sections 1(2) and 2(2) of the DSIS Executive Order, as the consolidated data should have been erased when the related source data (files, documents and entries) was erased.

- TET found it criticisable that in 18 cases DSIS processed information relating to organisations about which DSIS has started to consolidate data more than ten years ago to which source data should have been attached, in violation of sections 1(2) and 2(2) of the DSIS Executive Order, as the attachment of relevant source data is decisive for DSIS to be allowed to consolidate information about organisations in the system in question.

- TET found it criticisable that DSIS processed information relating to 19 persons and 84 organisations in violation of section 9a(1) of the DSIS Act, as DSIS, in connection with TET's review in 2021, erased the information in its production environment without erasing the copy of the information in two different pre-production environments.

- TET found it criticisable that DSIS processed 62,040 files in violation of section 9a(1) of the DSIS Act in a pre-production environment, as DSIS should have erased the information after the development of a piece of software.

- TET has noted that DSIS has initiated work to identify the possibilities of full or partial technical support of its audit process.

TET's reviews of files more than ten years old in DSIS' previous file system and reviews of DSIS' decisions in 2022 not to erase files under section 9(2), see subsection (1), of the DSIS Act and section 1(4), cf. subsection (2), of the DSIS Executive Order did not give rise to any comments.

Through its ongoing reviews of DSIS' compliance with the time limits for erasure in 2022, TET learned

- that DSIS is generally having difficulties erasing consolidated information when the related source data is erased,

- that DSIS' audit is carried out in several systems in the production environment, where not all systems are automatically updated across DSIS' systems,

- that DSIS' audit in the production environment does not automatically involve an update of DSIS' pre-production environments, and

- that DSIS' audit process is characterised by manual processes.

TET finds it criticisable that DSIS continues to have difficulties observing the statutory requirements for erasure of consolidated information when the related source data is erased, considering that TET generally pointed out DSIS' challenges in this respect already in its annual reports for 2014 and 2015 as well as for 2020 and 2021, and that TET's reviews in the period from 2016 to 2021 specifically showed that DSIS continued to be having challenges in this respect. Furthermore, TET found that DSIS is having difficulties in facilitate consistent erasure across IT environments.

TET found it essential for DSIS' compliance with the statutory requirements for erasure or extension of time limits for erasure that DSIS implements a higher degree of IT support for the auditing of files and database entries across DSIS' IT systems and environments, including ensures automatic erasure of consolidated data when the related source data is erased.

TET has noted that DSIS is focusing on timely audit of files and on notifying TET, and that the reviews in 2022 showed that DSIS has erased or extended files before the overall time limit for erasure expired, and that DSIS has notified TET accordingly.

2.2.3 Reviews of DSIS' use of other agencies' systems

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

However, DSIS is responsible for ensuring that its employees do not access systems belonging to other agencies in violation of the rules, which DSIS must counter by complying with the legislation governing the processing of personal data in these systems, see section 6a of the DSIS Act and the DSIS Executive Order on Security Measure.

Comments by TET

TET found it criticisable that DSIS' processing time for responding to TET's consultation questions was 200 working days. Due to DSIS' long processing time and the nature of its consultation responses, TET was not able to complete meaningful compliance reviews of DSIS' use of other agencies' systems in 2022. In this connection, it should be noted that TET's consultation was of a larger scope and that TET on that basis entered into a dialogue on with DSIS about DSIS' ability to answer TET's questions.

Against this background, TET recommended that DSIS clarify its use of systems to which it has direct access, but where data responsibility lies with another agency.

2.2.4 Review of DSIS' compliance with the rules on legal political activity

Section 11 of the DSIS Act provides in subsection (1) that the participation by a natural person resident in Denmark in legal political activity does not in itself warrant processing of information about that person by DSIS.

The prohibition of processing information about legal political activity is not absolute. This will be seen from the expression "not in itself". Thus, DSIS is allowed to process information about a person's legal political activity if there are other factors, which mean that a person has attracted DSIS' interest.

If the person in question has already become the focus of DSIS in connection with the performance of its activities, DSIS is also allowed to process information about the person's legal political activity if such information is relevant to the inquiries. By way of example, this could be a person who engages in political activity as a pretext for planning, preparing or engaging in espionage, terrorism or violent extremist activity.

In each individual case, DSIS must thus assess whether processing of information about legal political activity is warranted by other grounds than the very performance of such activity, and such an assessment is inherently discretionary.

DSIS may also process information about a person's legal political activity with a view to determining if the activity is legal. If DSIS' investigations show that the political activity is legal, the information must be erased. This applies no matter that the overall time limits for erasure for such information under section 9 of the DSIS Act or section 1(2) of the DSIS Executive Order have not been reached yet.

In 2022, TET completed a review of DSIS' processing of information about legal political activity on the basis of a search in DSIS' systems for all local politicians in Denmark in order to identify information on the political activities of local politicians where DSIS' need to process information is not immediately apparent from the context. TET then made supplementary searches in DSIS' systems to assess DSIS' need to process the information.

Comments by TET

TET's review of DSIS' compliance with the legislation on legal political activity in 2022 did not give rise to any comments.

2.2.5 Review of DSIS' special databases

DSIS may operate special databases in connection with its operative and administrative activities, see section 2(1) of the DSIS Executive Order.

Databases are used to structure large volumes of data to allow for efficient searches, backups, implementation of access control, logging and security measures as well as the analysis of large volumes of data in a short period of time. Databases are thus a prerequisite for an organisation to handle large volumes of data efficiently and securely. A single database may contain very large volumes of data.

In 2022, TET reviewed DSIS' special databases.

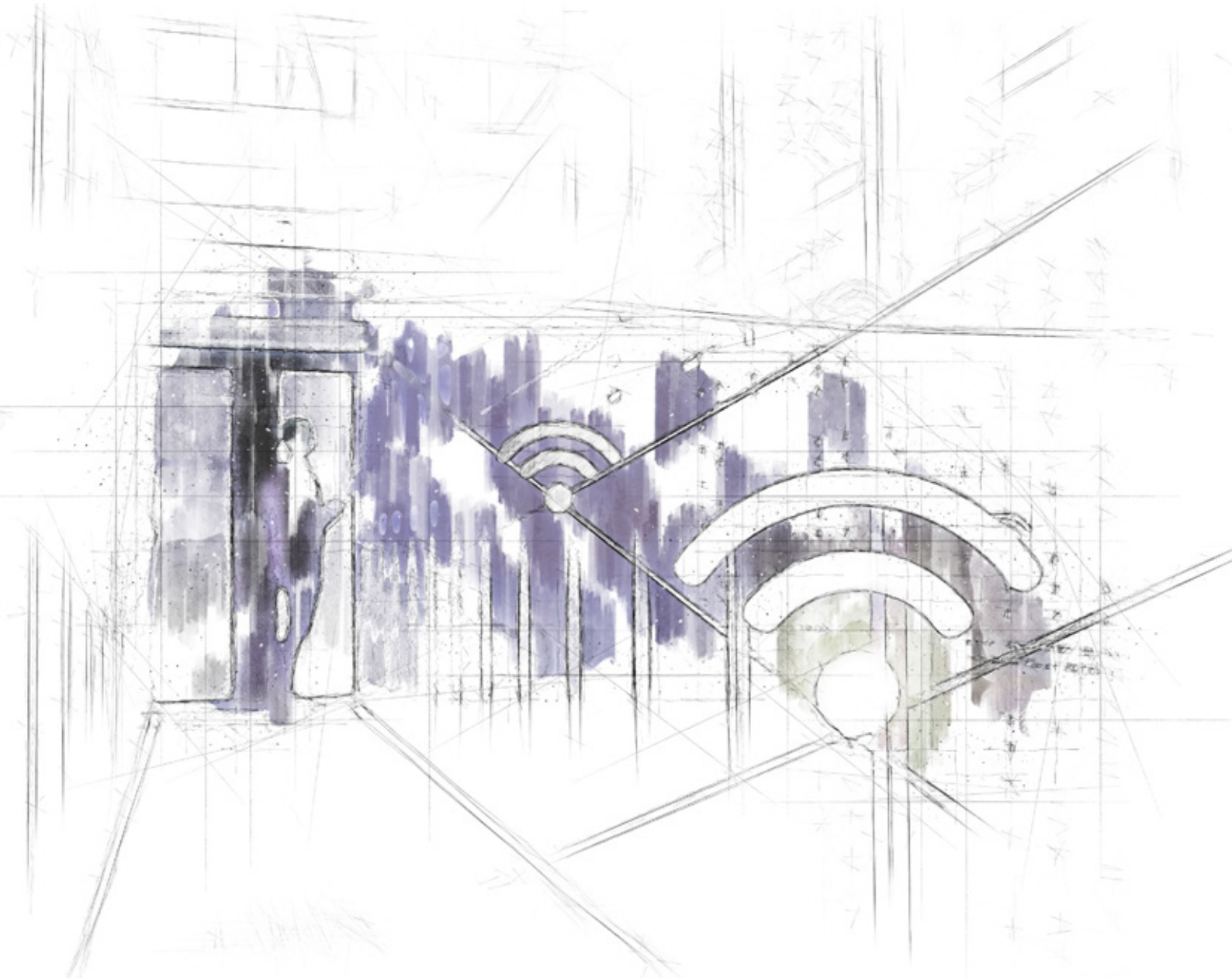
Comments by TET

TET's review of DSIS' special databases gave rise to the following comments:

- TET found it highly criticisable that DSIS, due to a lack of IT support, had not established logging for two of its special databases, see section 17 of the DSIS Executive Order on Security Measures, considering that the databases were established before 1 January 2014 and in 2015, respectively. DSIS subsequently informed TET that it had now established a temporary logging solution.

- TET found it highly criticisable that DSIS had not established logging for one of its special databases, see section 17 of the DSIS Executive Order on Security Measures, considering that the database was established in 2018 and that the system had been used for processing confidential information since the entry into force of the DSIS Act on 1 January 2014. DSIS subsequently informed TET that it had now established a temporary logging solution for the database.

- TET found it highly criticisable that DSIS did not answer TET's questions concerning the requirements for security of processing according to ISO control "12.4.1 Event logging" concerning one of DSIS' special databases, as in TET's opinion all of its consultation questions concern DSIS' security of processing and also concern requirements for logging which DSIS itself has laid down. Reference is also made to section 2.2.10 for TET's reviews of DSIS' security of processing in 2022.



- TET found it criticisable that DSIS did not inform TET about the existence of a special database until 2022, despite the fact that the database has been used since 2020, see section 2(2) of the DSIS Executive Order.

- TET found that in one of its special databases DSIS processed three records in violation of section 2(2) of the DSIS Executive Order.

- TET found it problematic that one of DSIS' special databases did not contain reliable metadata regarding the time of entry of information in the database. In continuation thereof, TET found that according to section 2(2) of the DSIS Executive Order, the time of entry into the database must be understood as the time when DSIS first enters a record into the database, regardless of whether the record has been completed or is being processed. As a consequence, it follows that it is a prerequisite for DSIS' compliance with section 2(2) of the DSIS Executive Order that a time stamp is affixed to all records in a database for the entry of the record in the database. It must not be possible to change the time stamp as long as the record is stored in the database, as the stamp is crucial for DSIS' compliance with the provisions of the DSIS Executive Order on time limits for erasure and for TET's review of this area. Therefore, in TET's assessment, no meaningful review could be carried out of DSIS' compliance with the time limit for erasure of information in the database in question as, because of the quality of the metadata, the time limit for erasure was in practice unverifiable. TET will resume reviewing the database when DSIS has established a solution that ensures reliable metadata, including in particular a fixed time of entry of information into the database. In connection with the review, DSIS has stated that it does not immediately agree with TET's interpretation of section 2(2) of the DSIS Executive Order.

In connection with a number of databases, DSIS stated that in its immediate opinion TET has no authority to oversee compliance with the time limit for erasure in the databases, as the time limits are set on the basis of the provisions of the Danish Administration of Justice Act.

TET has informed DSIS that, in TET's opinion, the time limits for erasure have been set in accordance with the rules in section 2(2) and (3) of the DSIS Executive Order, see section 9(1), cf. section 9(2), of the DSIS Act, and that TET therefore has authority to review compliance with the time limits for erasure in the databases in question.

In view of the fact that it is crucial for TET's reviews of DSIS' databases that the question of TET's authority to review DSIS' compliance with the time limit for erasure of information in the databases is clarified, TET requested DSIS to state as soon as possible whether DSIS agrees with TET's conception of the law.

TET found it criticisable that DSIS, in connection with its reviews of the databases in question, had a processing time of 110, 134 and 161 working days, respectively, when responding to TET's consultation questions.

TET's review of DSIS' use of other special databases did not give rise to any comments.

Finally, TET's review of DSIS' databases for the purpose of clarifying whether all DSIS databases are known to TET did not give rise to any comments.

2.2.6 Reviews of DSIS' transit systems

According to section 3(1) of the DSIS Executive Order, DSIS must store personal information in electronic file management systems or databases within four weeks after it was received or procured. For practical reasons, DSIS needs to be able to process personal information on other systems, including drives, email systems, external storage devices, file servers and the like, before it is stored in DSIS' electronic file management systems or databases. Such systems are collectively referred to as transit systems.

DSIS processes a wide range of different types of information for operational purposes on transit systems.

DSIS has prepared guidelines on the use of its transit systems with a view to ensuring that DSIS' processing of information complies with DSIS legislation, including the requirements on logging under section 17 of the DSIS Executive Order on Security Measures.

According to sections 17-18 of the DSIS Executive Order on Security Measures, DSIS must keep records of its processing of personal information of a confidential nature. However, the logging requirement does not apply to information contained in documents and the like which are erased within a relatively short time limit set by DSIS or in documents which are not in final form. According to DSIS' guidelines, "confidentiality" in this context is to be understood in accordance with the special categories of personal data under data protection law, including information on political opinions and health data. Furthermore, information that a person or an organisation is of interest to DSIS will often be of a confidential nature.

Thus, DSIS is allowed to process non-confidential information and information of a confidential nature for up to 28 days on a system where no logging is established (transit system). Furthermore, DSIS may process information of a confidential nature in a system where no log is kept if the information is included in a document which is not available in its final form.

In 2022, TET reviewed DSIS' processing of information in transit systems by reviewing

- five of DSIS' shared drives,
- all shared mailboxes on three of DSIS' networks,
- work stations in three of DSIS' departments, including checking DSIS' processing of information in Greenland, and
- six of DSIS' other transit systems.

Comments by TET

TET's review of DSIS' processing of information in transit system gave rise to the following comments:

- TET found it criticisable that DSIS processed 104,818 files from cases investigated by DSIS in cooperation with the police districts on a shared drive in violation of sections 7(2) and 8(2) of the DSIS Act, see section 17, cf. section 18, of the DSIS Executive Order on Security Measures, and DSIS guidelines on the use of transit systems, particularly in view of the fact that it was standard DSIS practice to process information for more than the permitted 28 days on the transit system when a criminal case was to be transferred from DSIS to the police districts.

- TET found it criticisable that DSIS processed 245 files on a shared drive in violation of sections 7(2) and 8(2) of the DSIS Act, see section 17, cf. section 18, of the DSIS Executive Order on Security Measures, and DSIS guidelines on the use of transit systems, particularly in view of the fact that DSIS to a certain extent used the drive for case management purposes.

- TET found it criticisable that DSIS had not established sufficient access restrictions on three shared drives, see sections 10-11 of the DSIS Executive Order on Security Measures. Against this background, TET recommended that DSIS conduct a review of all shared drives and ensure that sufficient measures are in place to ensure that only authorised users have access to information on the drives.

- TET found it criticisable that DSIS processed a total of 4,423 emails in shared mailboxes in violation of sections 7(2) and 8(2) of the DSIS Act, see section 17, cf. section 18, of the DSIS Executive Order on Security Measures, and DSIS guidelines on the use of transit systems.

- TET found it criticisable that DSIS was not in compliance with the provisions of sections 3, 4-13 and 17, cf. section 18, of the DSIS Executive Order on Security Measures in relation to USB disks provided to DSIS' employees, as DSIS had not prepared a documented process to ensure that the disks are handled correctly after they have been provided to the employee, including how the USB disks are to be stored, how long they may be stored and how they are to be disposed of, and that the information is not processed for more than 28 days after the information on the disks has been obtained. In connection with the review, DSIS pointed out that the handling of USB disks – in DSIS' opinion – is already described in its general guidelines on the use of transit systems. TET noted that in connection with the review, DSIS became aware that the process for handing over USB disks should be reconsidered, and that DSIS will initiate work in this regard.

- TET found that DSIS processed 31 files on other shared drives in violation of sections 7(2) and 8(2) of the DSIS Act, see section 17, cf. section 18, of the DSIS Executive Order on Security Measures.

- Furthermore, TET found that DSIS processed files in two folders on a shared drive in violation of sections 7(2) and 8(2) of the DSIS Act, see section 17, cf. section 18, of the DSIS Executive Order on Security Measures. TET had questions about 224 files in the folders. DSIS informed TET that it could not generally exclude the possibility that these files contained personal information of a confidential nature, but that, according to DSIS, a proportion of the images did not contain personal information of a confidential nature and that the information had therefore been processed in accordance with the rules. Thus, TET was unable to determine the exact number of files in the folders processed by DSIS in violation of sections 7(2) and 8(2) of the DSIS Act, see section 17, cf. section 18, of the DSIS Executive Order on Security Measures.

- TET found that DSIS processed information on two servers in violation of the logging requirement in section 17, see section 18, of the DSIS Executive Order on Security Measures, cf. sections 7(2) and 8(2) of the DSIS Act. TET noted that, in light of the review, DSIS is considering whether there is a basis for changes to the system, including whether the system should continue to be defined as a transit system.

- TET found that DSIS processed five files and six emails on work stations in violation of the logging requirement in section 17, see section 18, of the DSIS Executive Order on Security Measures, cf. sections 7(2) and 8(2) of the DSIS Act.

TET's review of DSIS' other transit systems did not give rise to any comments.

2.2.7 Review of DSIS' processing of material classified as TOP SECRET

As part of its intelligence activities, DSIS processes information, which is classified as TOP SECRET.

In 2022, TET reviewed DSIS material classified as TOP SECRET with the aim of verifying whether DSIS processes the information in compliance with the DSIS Act and DSIS' internal guidelines issued pursuant thereto.

Comments by TET

TET's review of DSIS' processing of material classified as TOP SECRET did not give rise to any comments.

2.2.8 Review of DSIS' internal review

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

In 2022, TET reviewed DSIS' internal reviews. The review comprised all internal reviews carried out by DSIS and DSIS' planning of the same for 2023.

In November 2022, DSIS informed TET about its

- risk analysis concerning compliance with statutory requirements,
- notice about internal reviews in 2023, and
- review plan for 2023.

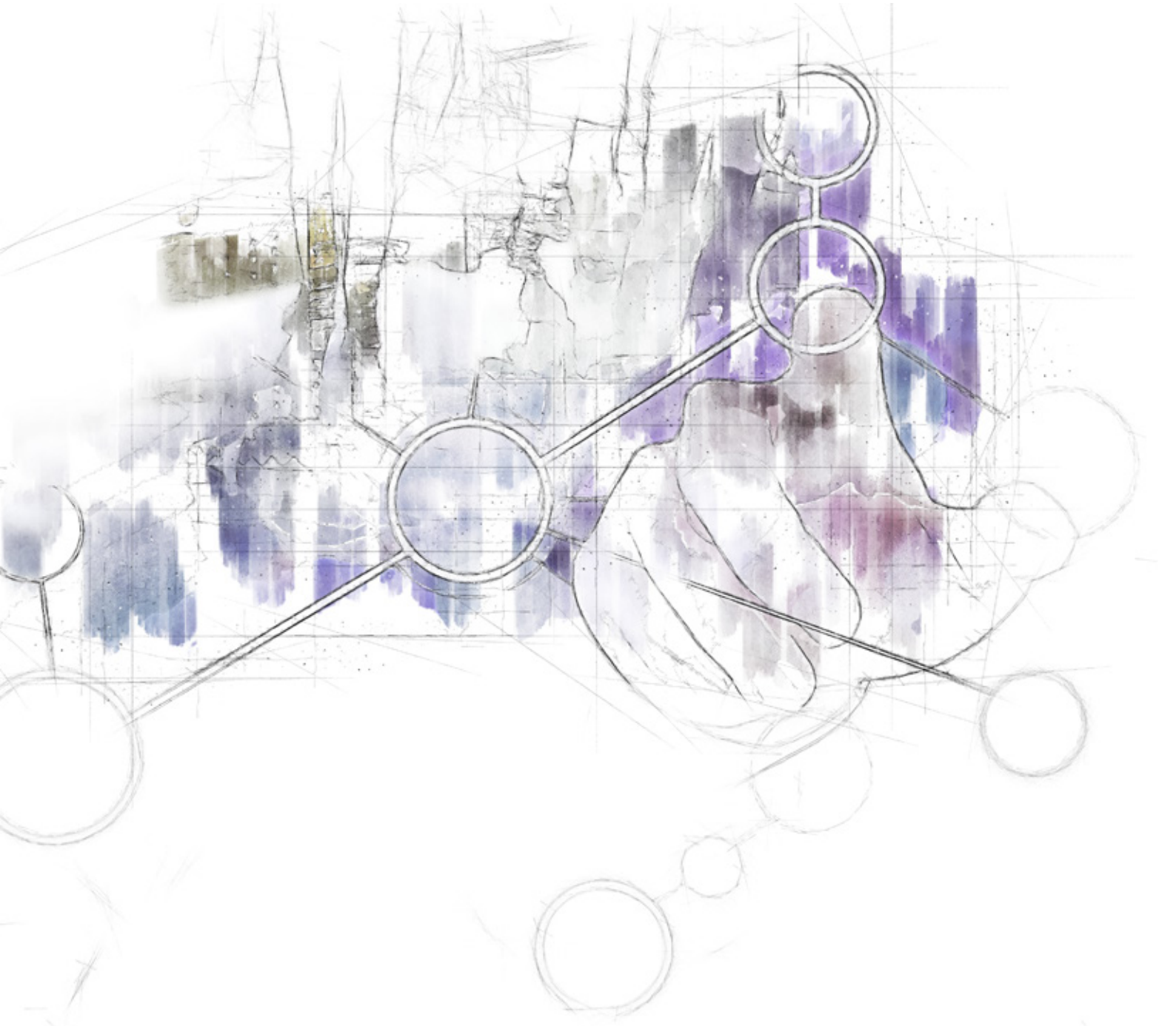
In addition, DSIS has regularly updated TET on its internal reviews, see section 2.3.

Comments by TET

TET's review of DSIS' internal reviews did not give rise to any comments. TET found that DSIS' organisation and performance of its internal reviews were satisfactory, including that DSIS has ensured that the reviews are well-documented and that the random sampling fairly present the audit results. Furthermore, DSIS regularly followed up on the results of its internal reviews. It should also be noted that there is a high degree of consistency between TET's and DSIS' risk analyses concerning the risk of DSIS non-compliance with legislation and that the risk analyses have been prepared independently of each other.

2.2.9 Review of DSIS' compliance with the rules on material subject to legal deposit etc.

DSIS is obliged under section 18(1) of the DSIS Executive Order to transfer information to be preserved for future generations to the National Archives.



Subsection (2) of the provision provides that, to the extent that such information cannot be transferred to the National Archives for practical or security reasons, the information must, from such time when destruction or erasure should have taken place, be processed separately from DSIS' other information, so that only staff specifically authorised by the Director General of DSIS have access to the information.

According to subsection (3) of the provision, DSIS may only process this information if it is deemed to be of significance to the performance of DSIS' activities concerning prevention and investigation of offences under Parts 12 and 13 of the Penal Code or in connection with the processing of records, subject access requests, oversight cases, etc. In addition, DSIS processes a large amount of material, which falls within the scope of the Ministry of Justice's shredding ban.

In 2022, TET reviewed DSIS' processing of material subject to legal deposit and material falling within the scope of the Ministry of Justice's shredding ban from 1998, which was originally intended to secure the basis for the work of two commissions of inquiry and which was extended in connection with the reestablishment of the Tibet Commission.

Comments by TET

TET found it problematic that in 8 out of 30 cases DSIS was unable to document that it had carried out searches in accordance with section 18(3) of the DSIS Executive Order as DSIS failed to explain the background for the individual searches but only provided a general explanation as to why it had carried out searches.

Furthermore, TET found it problematic that DSIS had not established a logging solution which could be used to document whether DSIS has used the systems in accordance with DSIS legislation, as the systems are thus not verifiable in relation to compliance with section 18(3) of the DSIS Executive Order.

Against this background, TET recommended that DSIS establish a logging solution which can be used to document whether it has used the systems in accordance with DSIS legislation.

2.2.10 Review of DSIS' compliance with the rules on security of processing

In 2022, TET has carried out a general review of DSIS' compliance with the rules on security of processing in the DSIS Executive Order on Security Measures.

In the assessment of whether DSIS fulfilled the requirements for security measures in connection with its processing of personal information, TET has since 2015 had regard to the ISO/IEC 27001 standard when interpreting the provisions of the DSIS Executive Order on Security Measures. In TET's assessment, this is the most appropriate way to perform the review, as DSIS is already obliged to implement the ISO/IEC 27001 standard and as there is a high degree of overlap between the requirements of the ISO/IEC 27001 standard and the requirements for security of processing under data protection law.

On 28 April 2022, TET sent a consultation notice to DSIS regarding its security of processing.

In a letter dated 1 August 2022, DSIS stated that – after discussions with DDIS – DSIS has by letter dated 27 June 2022 asked the Department of the Ministry of Justice to decide on

TET's mandate to review DSIS' work with information security, including implementation of the ISO/IEC 27001 standard.

DSIS also informed TET that, in its opinion, DSIS' response to consultation questions which wholly or partly concern reviews of DSIS' information security should await the decision of the Department of the Ministry of Justice and that TET will be informed when the Department of the Ministry of Justice has arrived at a decision in the matter.

In connection with 12 reviews, TET had questions to DSIS regarding specific security measures.

Comments by TET

TET found that it was unable to carry out its general review of DSIS' compliance with the rules on security of processing in 2022 as well as parts of four other reviews as DSIS did not answer TET's questions in this respect as, in DSIS' opinion, the reviews concerned information security and not security of processing. In this connection, DSIS stated that its response to consultation questions which wholly or partly concern reviews of DSIS' information security is pending the decision of the Department of the Ministry of Justice. TET noted in this connection that, in its opinion, the questions asked in connection with the reviews all concerned security of processing. The questions were based solely on DSIS' implemented ISO/IEC 27001 controls as DSIS had failed to inform TET how it had otherwise set up central procedures at management level to ensure compliance across the entire DSIS organisation with the provisions of the DSIS Executive Order on Security Measures on security of processing.

In connection with a number of reviews, TET requested DSIS to give an account of its risk assessment in relation to compliance with the rules on security of processing. In this connection, DSIS argued that the rules in the DSIS Executive Order on Security Measures imply that DSIS must consider security measures, but that the rules in the DSIS legislation are not identical to the rules on security of processing in the General Data Protection Regulation, including the requirement that actual risk assessments must be carried out. TET stated that it does not agree with DSIS. DSIS subsequently clarified that, in its opinion, the overall obligation under the DSIS Executive Order on Security Measures to carry out risk-based considerations should not be implemented in a specific form or at a specific level.

In TET's assessment, the DSIS Executive Order on Security Measures – like section 41(3) of the then current Data Protection Act – specifically imposes on DSIS an obligation to take any such appropriate technical and organisational measures which protect against the risks described in the provision.

TET noted in this connection that according to the specific explanatory notes to section 41(3) of the Data Protection Act, it is assumed that the measures, taking into account the current state of the art and the costs associated with their implementation, will provide an adequate level of security in relation to the risks posed by the processing and the nature of the data to be protected.

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

TET stated that it is a prerequisite for its review of DSIS' compliance with the DSIS Executive Order on Security Measures that DSIS documents its assessment of which measures it finds necessary to implement in order to provide an adequate level of security in relation to the risks involved in the processing and the nature of the data to be protected.

Based on its reviews, TET found that DSIS has not provided documentation for its assessment of the measures which DSIS considers necessary to implement in order to provide an adequate level of security across DSIS' organisation in relation to the risks posed by the processing and the nature of the information to be protected.

Finally, TET's reviews showed

- that DSIS in specific cases has difficulties observing section 17, see section 18, of the DSIS Executive Order on Security Measures in relation to the processing of information in transit systems, and
- that DSIS' access restrictions in specific cases were insufficient, see sections 10 and 11 of the DSIS Executive Order on Security Measures, as a very large amount of personal information was processed on a drive that was not properly protected by access restriction.

2.2.11 Follow-up on TET's reviews of DSIS in 2021

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

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

In its annual report on the review of DSIS in 2021 (section 1.2), TET described a number of reviews which revealed that DSIS was holding information that should have been erased because the information was no longer necessary for DSIS in the performance of its activities.

TET reviewed the information in question again with a view to determining whether – and, if so, to which extent – the information had subsequently been erased.

Based on the review in 2021, TET also recommended DSIS to make changes or submit specific briefings within ten areas.

TET has reviewed the recommendations which TET found necessary for DSIS to implement in connection with completed reviews. Furthermore, TET has reviewed the measures which DSIS found necessary to implement in connection with completed reviews. Finally, TET has reviewed the cases where it is still awaiting responses to requests for briefings in relation to completed reviews.

Comments by TET

TET found it criticisable that in 16 cases DSIS had not erased information in accordance with section 9a(1) and (2) of the DSIS Act, see section 11(2), as DSIS should either have erased the information on the basis of TET's letter of 18 January 2022 or informed TET that it did not agree with TET's assessment.

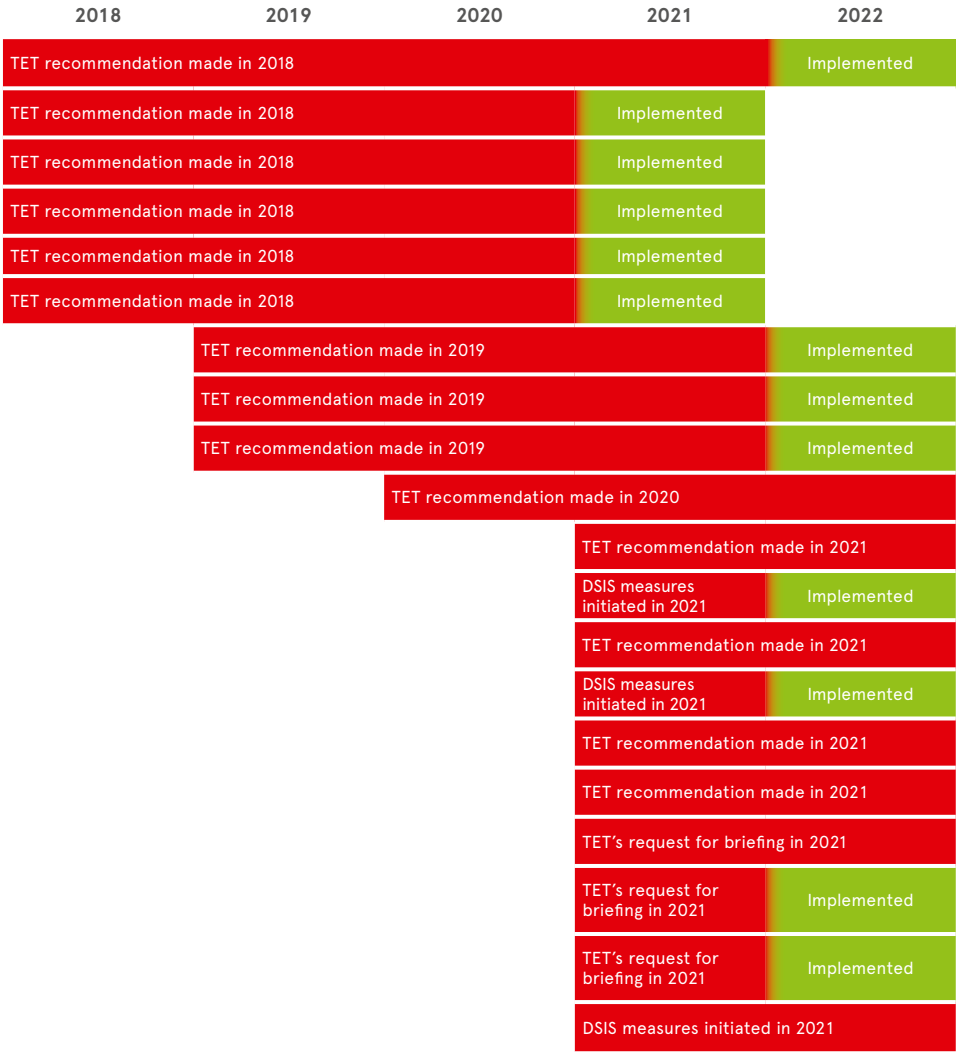
DSIS subsequently expressed its regret that it had not informed TET that it was still of the opinion that the processing of the information was not in violation of section 11 of

the DSIS Act as the processing of the information was necessary for the performance of DSIS' other activities, see section 7(1)(iii) of the DSIS Act.

DSIS also informed TET that in connection with this review, DSIS had reassessed the information in question and that it has now erased the 16 documents, see section 9a(1) and (2) of the DSIS Act, cf. section 7. DSIS stressed in this connection that it was not the legal political activities of the persons in question which in itself justified the collection and further processing of the information.

Furthermore, TET found it problematic that DSIS had not implemented three of TET's recommendations and three of the measures which DSIS had informed TET that it would implement. TET has noted that DSIS has initiated work on the three recommendations and three measures which DSIS has informed TET that it will implement.

Finally, TET has noted that in 13 cases DSIS had implemented TET's recommendations and measures which DSIS had informed TET that it would implement, or had provided briefings.



Note: The graphical representation shows in which year TET has made a recommendation, DSIS has informed TET that it will implement a measure or provide a briefing. Furthermore, the graphical representation shows in which year DSIS has implemented the relevant recommendation or measure or provided a briefing.

2.2.12 TET's technical reviews and mapping of DSIS' IT landscape

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

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

In 2022, TET has performed validation reviews and inspections by performing

- validation reviews of databases for the purpose of clarifying whether all DSIS databases are known to TET,
- validation reviews of file servers for the purpose of clarifying whether all DSIS file shares are known to TET, and
- inspected a number of databases and systems, which, in TET's immediate assessment, should not form part of TET's general reviews, in order to clarify whether the immediate assessment thereof was correct.

Comments by TET

TET's validation reviews of databases and file servers did not give rise to any comments.

Following its inspection of the databases, TET found that four of the databases are in future to form part of TET's general reviews.

2.3 DSIS' briefing of TET

According to the explanatory notes to the DSIS Act and Parts 1 and 6 of the DSIS Executive Order, DSIS must keep TET informed of its exercise of powers under a number of provisions of the Act. More specifically, the Executive Order prescribes that DSIS must thus inform TET of the following matters:

- DSIS' decisions under section 9(2) of the DSIS Act not to erase information which has reached the time limit for erasure of 15 years under section 9(1)
- DSIS' decisions under section 1(4) of the DSIS Executive Order not to erase files which have reached the time limit for erasure of ten years under section 1(2)
- DSIS' decisions under section 2(2) of the DSIS Executive Order to increase time limits for erasure of information beyond five years in exceptional cases for persons, entries or information held in DSIS' special databases, see section 2(1) of the provision
- DSIS' decisions under the second sentence of section 2(2) of the DSIS Executive Order to set time limits for erasure which do not begin to run on the date of entry, where so justified by the circumstances, see subsection (1) of the provision

- Instances in which, as an exception, DSIS is unable to comply with the time limit under section 3(1) of the DSIS Executive Order for electronic registration

- DSIS' exercise of its powers under section 4 of the DSIS Act to request information from other administrative authorities which may be assumed to be important to the performance of DSIS' activities concerning prevention and investigation of offences under Parts 12 and 13 of the Penal Code

- Files concerning security clearance where DSIS discloses information from its file management system or databases to public authorities other than the Ministry of Justice, the Prosecution Service and other parts of the police

- All important issues concerning DSIS' processing of information

- DSIS' internal reviews with regard to the processing of information about natural and legal persons under sections 10 and 11 of the DSIS Executive Order

- New administrative guidelines of importance to TET's reviews

- Other guidelines, if so requested by TET

DSIS has regularly informed TET of:

- DSIS' decisions under section 9(2) of the DSIS Act not to erase information which has reached the time limit for erasure of 15 years under section 9(1)

- DSIS' decisions under section 1(4) of the DSIS Executive Order not to erase files which have reached the time limit for erasure of ten years under section 1(2)

- DSIS' decisions under section 2(2) of the DSIS Executive Order to increase time limits for erasure of information beyond five years in exceptional cases for persons, entries or information held in DSIS' special databases, see section 2(1) of the provision

- Important issues concerning DSIS' processing of information on natural and legal persons

On 6 August 2021, 26 January 2022 and 22 March 2022, TET received briefings on the following matters:

- DSIS' exercise of powers under section 4 of the DSIS Act

- Files concerning security clearance where DSIS has disclosed information from its file management system or databases to public authorities other than the Ministry of Justice, the Prosecution Service and other parts of the police

- DSIS' internal review regarding section 4 of the DSIS Act

- DSIS' internal review regarding section 10 of the DSIS Act

- DSIS' internal review of information outside approved documentation systems (transit systems)

- DSIS' internal review of logging in specified systems

- DSIS' internal review of erasure of PNR information

- DSIS' internal review of material classified as TOP SECRET
- DSIS' audits
- DSIS' internal review of registration of files in electronic systems

TET followed up on the answers and reports submitted by DSIS.

2.4 Subject access requests under sections 12 and 13 of the DSIS Act

2.4.1 Processing of requests by TET

When a natural or legal person requests TET to review if DSIS is processing information about them in violation of DSIS legislation, TET will examine the matter at DSIS' premises where TET has access to any information and all material of importance to TET's activities.

It may be a quite resource-intensive and complicated exercise to identify all information about a data subject, which is being processed by DSIS, but TET will endeavour to identify all information, which DSIS is processing about a data subject who has submitted an indirect subject access request.

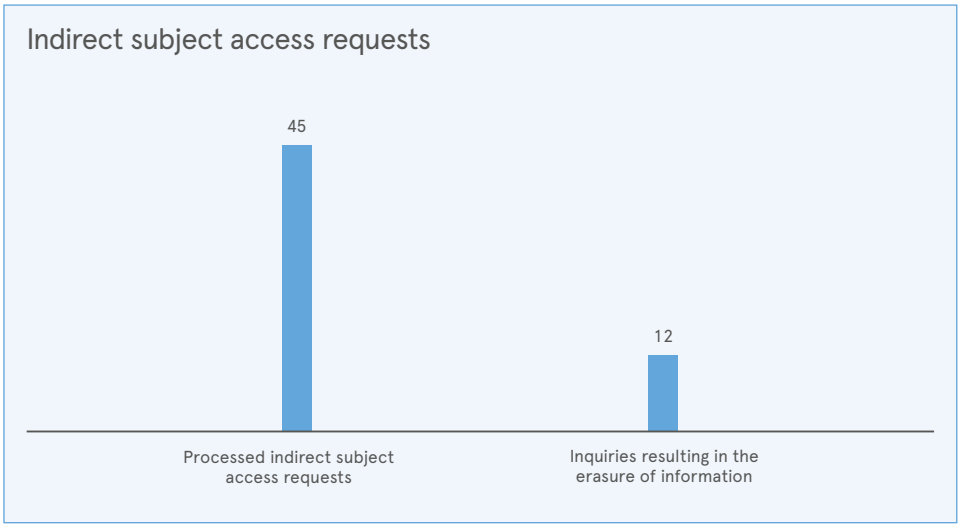
When the process has been completed, TET will assess whether, in TET's view, DSIS is processing information about the data subject in violation of DSIS legislation. If TET concludes that this is the case, TET will order DSIS to erase the information. When TET has verified that DSIS is no longer processing information about the data subject in violation of DSIS legislation, TET will send a reply to the data subject's request.

If special circumstances weigh in favour of doing so, TET may order DSIS to inform a natural or legal person of the information which DSIS is processing about them or inform them whether DSIS is processing information about them. Where TET receives a subject access request, TET will find out which information, if any, DSIS is processing about the data subject and will obtain DSIS' comments before TET makes a decision under the relevant provision. For indirect subject access requests, TET will review of its own motion whether special circumstances weigh in favour of ordering DSIS to grant full or partial access to the information in question.

2.4.2 Number of requests and processing time

In 2022, TET received subject access requests from 45 natural or legal persons, asking TET to review if DSIS was processing information about them in violation of DSIS legislation. In that connection, TET found that in 12 cases DSIS had processed information about the persons in question in violation of the conditions of processing in section 7(1) or 8(1) of the DSIS Act. In this connection, it should be noted that DSIS is not required beyond that to review its cases and documents, etc. of its own motion in order to assess if the above conditions of processing are still met. DSIS has on that basis erased most of the information.

However, in one case, DSIS informed TET that for technical reasons it is currently not possible to erase information at data-level in one of the systems in which the information is held. As DSIS found that the document in question contains other information deemed by DSIS to be necessary for the performance of its activities, the document cannot be erased in its entirety, and thus DSIS cannot arrange for the erasure of the information in question. DSIS will immediately erase the information if it becomes possible at some point to erase information at data-level in the system in question and, similarly, DSIS has informed TET that it will once a year consider whether the information in question can be erased.



In 2022, the average processing time for the processed requests was 172 days, 92 days of which were DSIS' processing time. Compared with 2021, the average processing time decreased by 11 days.

TET endeavours to answer subject access requests as quickly as possible, but as already mentioned this may be a quite resource-intensive and complicated process. The results of this process are presented to TET at monthly meetings where TET will make a decision in the matter.

It should be noted that in order for TET to perform its duties in connection with the indirect subject access request system, information about natural and legal persons must be stored in DSIS' IT systems in accordance with sections 1-3 of the DSIS Executive Order, and the IT systems must facilitate efficient consultations and erasure of information at data-level.

Based on the special risk assessment and analysis for 2020 regarding reviews in relation to DSIS under the indirect subject access request system, TET decided to include another two systems in its future reviews. However, DSIS informed TET that it is not technically possible in these systems to conduct effective reviews of DSIS' processing of information (see TET's annual report for 2021, section 1.4.2).

In connection with its reviews in 2022, TET became aware that in a system that is currently subject to TET's reviews, it is not technically possible to erase information at data-level. Therefore, TET is unable to verify that information which no longer meets the conditions of processing in sections 7 and 8 of the DSIS Act is erased in the system in question.

Based on the special risk assessment and analysis for 2022 regarding reviews in relation to DSIS under the indirect subject access request system, TET decided to include another

three systems in its future reviews. TET and DSIS are in dialogue about the possibilities of conducting effective searches in the systems in question.

2.5 DSIS' processing times in 2022

In 2022, TET submitted 33 legal consultations to DSIS in connection with its review activities. DSIS has responded 11 of TET's consultation questions within the specified deadline and two after the specified deadline. DSIS' average processing time for responding to consultation questions that were responded to after the deadline was 67 working days. The average processing time is due to a long response time in seven out of the 22 consultations where the deadline had been exceeded.

In 2022, as a result of DSIS' processing times, TET experienced that the work involved in its risk assessment of DSIS, the planning of next year's reviews and the preparation of its annual report on DSIS has been impeded. In addition, DSIS' processing times have in specific cases limited TET's possibilities of performing supplementary reviews of DSIS' processing of information.

In 2022, TET has been in dialogue with DSIS about its case processing times, and on that basis, TET and DSIS have developed a new consultation handling process which TET expects will support DSIS in responding to TET's consultation questions within the agreed deadline.

2.6 Review of RPNR in 2022

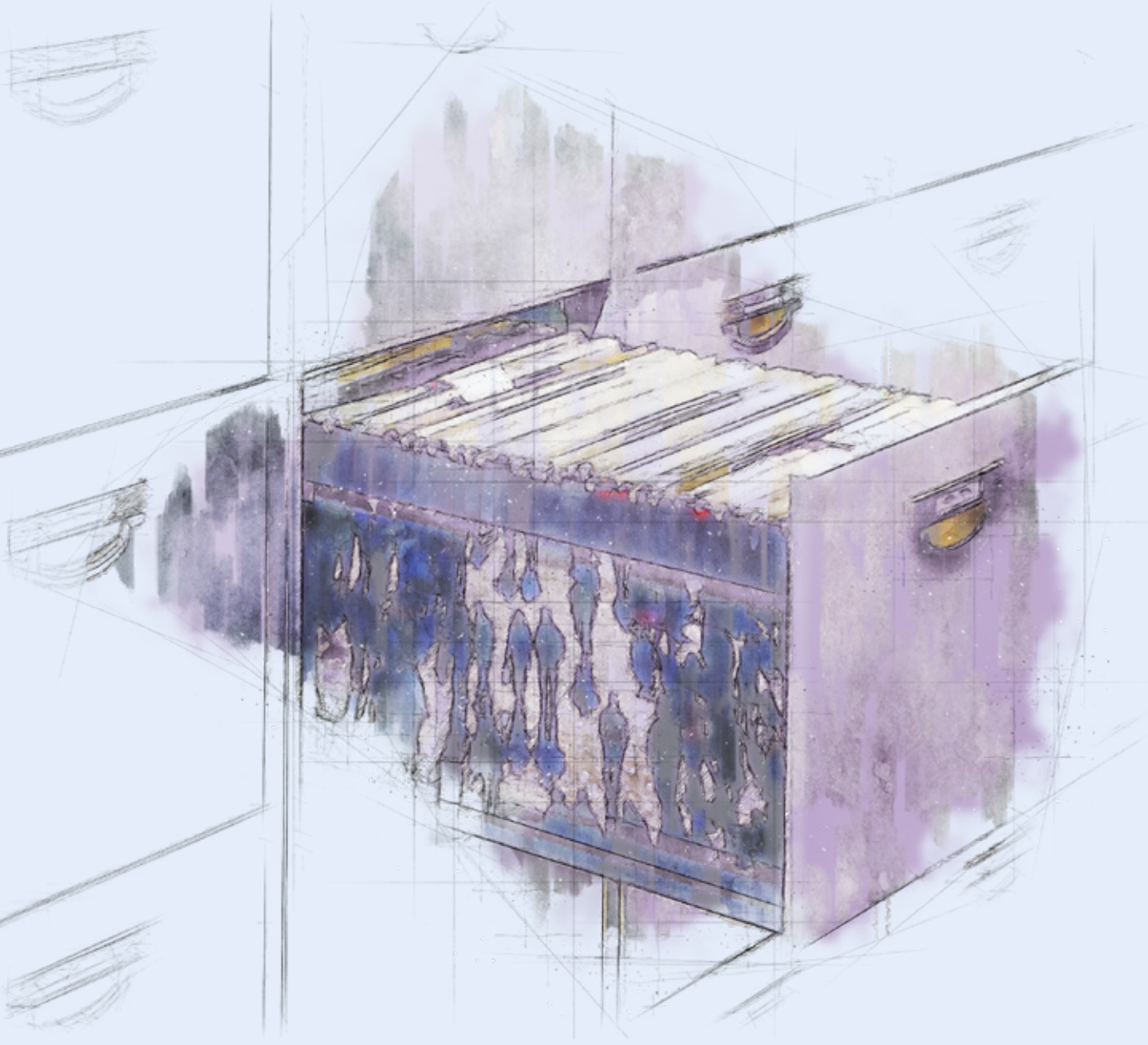
TET is tasked with overseeing the processing of airline passenger name records by the PNR Unit under the Danish National Police (RPNR) on behalf of DSIS and DDIS.

RPNR's processing of airline passenger name records on behalf of DSIS and DDIS is carried out by the employees of DSIS and DDIS who are seconded to RPNR.

In 2022, TET has performed checks of RPNR's processing of information under the PNR Act on behalf of DSIS and DDIS.

Comments by TET

TET's reviews of RPNR's processing of information under the PNR Act on behalf of DSIS and DDIS did not give rise to any comments.



Appendix

1. About Danish Security and Intelligence Service (DSIS)

The Danish Security and Intelligence Service (DSIS) is tasked with the main responsibility of acting as:

- national intelligence and security service,
- national security authority, and
- IT security authority under the Ministry of Justice.

DSIS is tasked with the overall responsibility of preventing, investigating and countering operations and activities that pose or may pose a threat to freedom, democracy and safety in Danish society. Through its activities, DSIS must thus provide the basis for ensuring that threats of the said nature are identified and addressed as quickly and effectively as possible and, being part of the police, DSIS' essential objective is to work not only for overall safety, security, peace and order in society but also for the safety and security of each individual.

DSIS' responsibility is to prevent, investigate and counter offences against state autonomy and security as well as offences against the constitution and the supreme authorities of the state, etc., see Parts 12 and 13 of the Penal Code.

In addition, DSIS' responsibilities include preparing threat assessments, providing assistance to the other branches of the police, acting as national security authority and advising and assisting public authorities and private individuals on security-related issues as well as protecting private individuals, organisations and public authorities (personal protection etc.). If so requested by for example the relevant authority or agency, DSIS acting as national security authority performs vetting of individuals when it is contemplated to authorise such persons to access classified documents. However, for authorities in the areas under the Ministry of Defence, this task is undertaken by DDIS.

The legal framework for DSIS' activities is essentially laid down in the DSIS Act and the relevant executive orders, the PNR Act as well as the Administration of Justice Act.

The DSIS Act governs, among other things, DSIS' responsibilities and the procurement, internal processing and disclosure of personal information. In addition, the DSIS Act sets up an independent oversight board, the Danish Intelligence Oversight Board (TET), which is charged with overseeing that DSIS processes personal information in compliance with DSIS legislation.

DSIS is also subject to external supervision by the Ministry of Justice, the Danish courts, the Independent Police Complaints Authority, the Parliamentary Ombudsman and the Parliamentary Intelligence Services Committee.

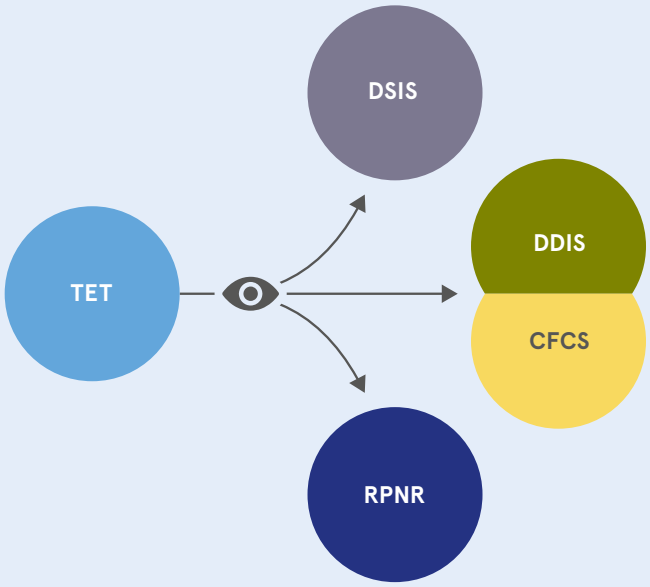
Appendix

2. Danish Intelligence Oversight Board (TET)

TET's activities

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

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



TET is completely autonomous and is thus not subject to the directions of the Ministry of Justice or any other administrative authority with respect to the performance of its activities.

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

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

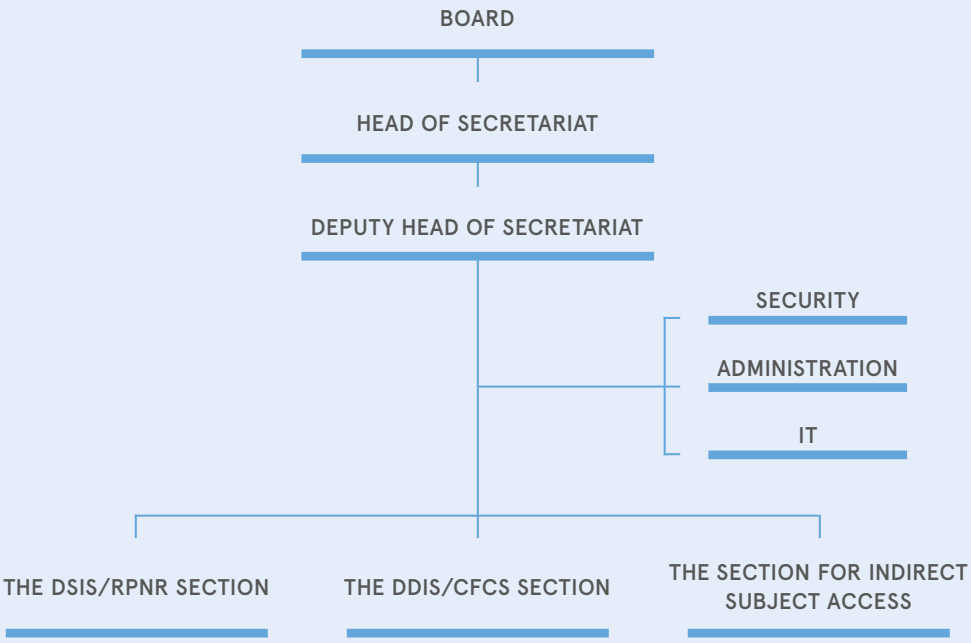
- High Court Judge Michael Kistrup, High Court of Eastern Denmark (Chair)
- Legal Chief Pernille Christensen, Local Government Denmark
- Professor Henrik Udsen, University of Copenhagen
- Professor Rebecca Adler-Nissen, University of Copenhagen
- Director Jesper Fisker, Danish Cancer Society

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

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

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

Organisation 2022



2.1 TET's duties in relation to DSIS

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

- procurement of information, including collection and obtaining of information,
- internal processing of information, including time limits for erasure of information,

- disclosure of information, including to DDIS and to other Danish administrative authorities, private individuals or organisations, foreign authorities and international organisations, and
- the prohibition of processing information about natural persons resident in Denmark solely on grounds of their legal political activities.

Furthermore, TET reviews compliance with the provisions of the PNR Act concerning

- procurement of information,
- internal processing of information, including unmasking, and
- disclosure of information

when RPNR procures, processes and discloses information on behalf of DSIS.

TET must oversee by way of compliance reviews that DSIS processes information about natural and legal persons in compliance with DSIS legislation, and TET thus has no mandate to review whether DSIS carries out its activities in an appropriate manner, including how DSIS' operational and investigative resources are prioritised, as these aspects are to be determined by DSIS itself based on a police professional assessment.

TET itself decides the intensity of oversight, including whether to perform full reviews or random samplings, which aspects of the activities are to be given special priority and the extent to which TET wishes to raise a matter of its own motion. No specific guidelines have been provided for TET's performance of its oversight functions, except that – according to the legislative history of the Act – TET must for example carry out 4-6 inspections of DSIS each year in the course of its own motion compliance checks.

At the request of a natural or legal person, TET will also investigate whether DSIS is processing information about the data subject in violation of DSIS legislation. TET will verify that this is not the case and then notify the data subject (the indirect subject access request system). According to the legislative history of the Act, it must only be possible to infer from TET's reply that no information is being processed about the data subject in violation of DSIS legislation. Accordingly, it must not be stated in or possible to infer from the reply whether any information is being or has been processed at all, whether any information has been processed in violation of DSIS legislation or whether information is being processed in compliance with DSIS legislation.

2.2 TET's access to information held by DSIS

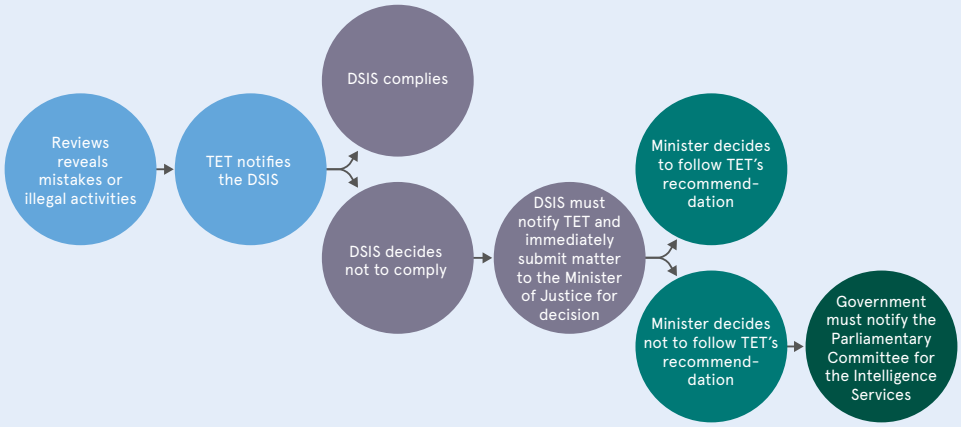
TET may require DSIS to provide any information and material of importance to TET's activities, and TET is entitled at any time to access any premises where the information being processed may be accessed or where technical facilities are being used. TET may furthermore require DSIS to provide written statements on factual and legal matters of importance to TET's oversight activities and request the presence of a DSIS representative to give an account of current processing activities.

DSIS has made office premises available to TET for TET to make its own searches in DSIS' IT systems.

2.3 Responses available to TET

TET generally has no authority to order DSIS to implement specific measures in relation to data processing. However, TET may issue statements to DSIS providing its opinion on matters such as whether DSIS complies with the DSIS Act, the DSIS Executive Order and the DSIS Executive Order on Security Measures. If DSIS decides not to comply with a recommendation issued by TET in exceptional cases, DSIS must notify TET and immediately submit the matter to the Minister of Justice for a decision. If the Minister of Justice decides not to follow the recommendation of TET in exceptional cases, the Government must notify the Parliamentary Intelligence Services Committee.

Responses available for TET



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

As part of the indirect subject access request system which, as already mentioned, requires TET, if so requested by a natural or legal person, to investigate whether DSIS is processing information about that person in violation of DSIS legislation, TET may order DSIS to erase any information which, in the opinion of TET, is being processed by DSIS in violation of DSIS legislation.

Each year, TET submits a report on its activities to the Minister of Justice. The report, which is available to the public, provides general information about the nature of the oversight activities performed with regard to DSIS. According to the legislative history of the Act, the aim of the annual report is to provide general information about the nature of the oversight activities performed with regard to DSIS, including a general description of the aspects, which TET has decided to examine more closely. Similarly, TET may include statistical data on the number of instances where information has been found to be processed by DSIS in violation of DSIS legislation, including the number of instances where TET has ordered DSIS to erase information under the indirect subject access request system.

TET submitted its most recent annual report on its activities to the Minister of Justice in May 2022. The annual report was submitted to the Parliamentary Intelligence Services Committee and then published in June 2022.

Appendix

3. Legal framework

1) The Danish Security and Intelligence Service (DSIS) Act (Consolidated Act No. 231 of 7 March 2017, as amended (most recently by Act No. 1706 of 27 December 2018)) (the DSIS Act).

2) Executive Order on the processing by the Danish Security and Intelligence Service (DSIS) of information about natural and legal persons, etc. (Executive Order No. 763 of 20 June 2014), as amended (most recently by Executive Order No. 438 of 7 April 2022) (the DSIS Executive Order).

3) Executive Order on security measures to protect personal information on natural and legal persons being processed by the Danish Security and Intelligence Service (DSIS) (Executive Order No. 516 of 23 May 2018 (the DSIS Executive Order on Security Measures).

4) Decree No. 1622 of 17 November 2020 on the entry into force for Greenland of the Danish Security and Intelligence Service (DSIS) Act.

5) Decree No. 1623 of 17 November 2020 on the entry into force for the Faroe Islands of the Danish Security and Intelligence Service (DSIS) Act.

6) Act on the collection, use and storage of airline passenger name records (the PNR Act) (Act No. 1706 of 27 December 2018).

7) Executive Order on the PNR Unit's processing of PNR information (Executive Order No. 1035 of 29 June 2020).

3.1 Procurement of information

3.1.1 About collection and obtaining of information, see section 3 of the DSIS Act

Under section 3 of the Act, DSIS is authorised to collect and obtain information, which may be of importance to the performance of its activities. According to the explanatory notes to the DSIS Bill concerning section 3, DSIS' work is largely preventive in nature and, as a result, DSIS should be allowed to collect information even if the assessment of whether the data subjects actually intend to commit an offence is subject to uncertainty. The only requirement is that it cannot be ruled out in advance that the information may be of relevance for DSIS. Under this provision, DSIS may thus collect information about "secondary persons" in the same way as before, including persons belonging to the same social circle as the suspect who are not under suspicion of being involved in the potential offence being investigated.

3.1.2 About the obligation of other administrative authorities to disclose information to DSIS, see section 4 of the DSIS Act

Under section 4 of the Act, DSIS may request information from Danish administrative authorities other than the Danish Defence Intelligence Service (DDIS) when the information may be assumed by DSIS to be important to the performance of DSIS' activities concerning prevention and investigation of offences under Parts 12 and 13 of the Penal Code. There must be a somewhat substantive presumption that the information requested by DSIS will be of importance for DSIS in its performance of the activities in question, but if DSIS believes that this is the case, other administrative authorities will be required to disclose the information to DSIS. The disclosing administrative authority itself will thus not have to make an assessment of whether the condition of disclosure is satisfied, but will simply have to rely on DSIS' assessment.

Under the provision, DSIS is allowed to obtain information about all persons who have contacted a given public authority within a given time, or about other groups of persons who are not identified in advance (extended obtaining of information).

According to the explanatory notes to the DSIS Bill concerning this provision, TET may test DSIS' assessment of whether the information may be assumed to be of importance to the performance of its activities concerning prevention and investigation of offences under Parts 12 and 13 of the Penal Code, and it is assumed that DSIS will inform TET on a regular basis of its exercise of the powers under this provision.

3.2 Internal processing of information

3.2.1 About internal processing of information under sections 6a-8 of the DSIS Act

Under section 6a(1)-(7) of the DSIS Act, a number of the provisions of the Data Protection Act apply to DSIS' processing of information collected and obtained about natural and legal persons.

According to the explanatory notes to the DSIS Act, the same general data protection principles etc. will generally apply to the determination of which fundamental conditions must be satisfied by DSIS when processing personal information as those applying to other Danish authorities when processing personal information.

Under sections 7(1) and 8(1) of the Act, DSIS is allowed to process any information about natural and legal persons if

1) consent has been obtained from the data subject,

2) processing may be assumed to be of importance to the performance of DSIS' activities concerning prevention and investigation of offences against state autonomy and security as well as offences against the constitution and the supreme authorities of the state, etc., see Parts 12 and 13 of the Penal Code, or

3) processing is necessary for the performance of DSIS' activities.

Under sections 7(1)(ii) and 8(1)(ii) of the Act, DSIS is thus authorised to process any information about natural and legal persons if processing may be assumed to be of importance to the performance of DSIS' activities concerning prevention and investigation of offences under Parts 12 and 13 of the Penal Code. The condition that the information may be assumed to be of importance to the performance of DSIS' activities concerning prevention and investigation of offences under Parts 12 and 13 of the Penal Code reflects the requirement of a somewhat substantive presumption that the information DSIS wishes to process will be of importance to DSIS' performance of those activities.

Under sections 7(1)(iii) and 8(1)(iii) of the Act, DSIS is authorised to process any information about natural and legal persons if processing is necessary for the performance of DSIS' other activities, i.e. activities other than those involved in the prevention and investigation of offences under Parts 12 and 13 of the Penal Code. The condition that the information must be necessary for the performance of DSIS' other activities reflects the requirement that, based on an assessment in each individual case, DSIS may be assumed to have a genuine need to process the information in question in order to perform its activities.

3.2.2 About erasure of information, see sections 9 and 9a of the DSIS Act and sections 1-3, 8 and 18 of the DSIS Executive Order

Under section 9 of the DSIS Act, unless otherwise prescribed by law or statutory regulation, DSIS must erase information about natural and legal persons, which has been procured in the course of inquiries or investigations directed at such persons when in connection with the inquiries or investigations no new information has been procured within the last 15 years. However, erasure of such information will not be required if the information is necessary to safeguard important interests with regard to the performance of DSIS' activities. According to the explanatory notes to the DSIS Bill concerning this provision, which only covers information procured in the course of inquiries or investigations directed at natural and legal persons, the provision lays down an overall time limit for erasure of information held by DSIS.

In other parts of DSIS legislation, including in particular Danish archiving law, there are rules, which mean that DSIS is not allowed to erase information. Thus, the Director General of the National Archives has issued a set of rules, which mean that DSIS must retain information of historical interest. Such rules must be observed by DSIS, which means that DSIS is precluded from erasing the information as section 9 of the DSIS Act prescribes that DSIS' obligation to erase information does not apply if otherwise prescribed by law or statutory regulation.

The legislative history of the DSIS Act presumes that more detailed time limits for erasure will be laid down for the information processed by DSIS. Under the authority granted to the Minister of Justice under the Act to introduce more detailed rules on DSIS' processing of information about natural and legal persons, the DSIS Executive Order has laid down more detailed rules, including on erasure of personal information.

Thus, section 1 of the DSIS Executive Order provides that DSIS must erase files no later than ten years after they were opened in the electronic file management system if they do not contain information about natural and legal persons that has been obtained in the course of inquiries or investigations directed at such persons. However, erasure will not be required if the files are necessary to safeguard important interests with regard to the performance of DSIS' activities and if TET is duly notified.

Under section 2 of the DSIS Executive Order, DSIS must lay down a time limit for erasure for the individual person or piece of information in the database of up to five years from the date of entry in the database for information which has not been obtained in the course of inquiries or investigations. DSIS may, after notifying TET, in exceptional cases set longer time limits for erasure of persons, records or information in these databases etc. Furthermore, DSIS may, where so justified by the circumstances and after notifying TET, set time limits for erasure under the first or second sentence which do not begin to run on the date of entry. According to subsection (3) of the provision, the time limits for erasure of information about natural and legal persons obtained in the course of inquiries or investigations may not exceed the time limit in section 9(1) of the DSIS Act, but see subsection (2).

Section 3 of the Executive Order provides that information, which has not been stored in the file management system or in a database within four weeks after it was received or procured, see sections 1 and 2, must be erased unless the nature of the information does not allow for electronic storage. DSIS must notify TET if DSIS is unable to observe the time limit in exceptional cases. In addition, DSIS may, after informing TET and where so justified by the circumstances, set time limits for erasure, which do not begin to run on the date of entry.

It follows from the new provision in section 9a(1) that when DSIS becomes aware in connection with its activities that cases or documents, etc. no longer meet the conditions of processing in sections 7(1) and 8(1), they must be erased, regardless of whether the time limit for erasure of information in section 9 or any time limits set in pursuant of section 7(2) or 8(2) have expired, but that DSIS is not required beyond that to review its cases and documents, etc. of its own motion in order to assess if the above conditions of processing are still met.

In the notes to the individual provisions of the Bill, it is specified with regard to section 9a(1) that the term "activities" is to be understood in the broad sense as encompassing all the tasks that DSIS is engaged in. Thus, by way of example, in addition to operational activities, the term also includes DSIS' tasks in connection with indirect subject access requests, see section 13 of the Act, and random checks performed by TET.

It follows from the provision in section 9a(2) that notwithstanding the provisions of sections 7-9, DSIS is not required to erase information which does not meet the conditions of processing in sections 7(1) and 8(1) if the information forms part of documents etc. which otherwise meet the above-mentioned conditions of processing, but see subsection (3) and section 13(2).

In the notes to the individual provisions of the Bill, it is specified with regard to section 9a(2) that the provision concerns erasure at data-level whereas the provision in subsection (1) concerns erasure at case- and document-level. DSIS is thus not required to erase information at data-level even if DSIS becomes aware in connection with its activities that a specific piece of information no longer meets the conditions of processing in sections 7(1) and 8(1) if the information forms part of documents etc. which still meet those conditions of processing and for which the time limit for erasure has not yet expired. Furthermore, it is emphasised that TET may still check in connection with its random checks whether a file or document, etc. as a whole meets the above-mentioned conditions of processing but that as a general rule DSIS will not be required to erase individual pieces of information which form part of documents etc. which are to be retained, in connection with such random checks. However, DSIS will still be required to erase information if it is established that it has been procured in violation of sections 3 and 4 of the Act.

Under section 9a(3), the Minister of Justice may lay down provisions to increase DSIS' erasure obligations beyond the obligations set out in the Act in specified cases.

It can thus be seen from section 8(1) of the DSIS Executive Order that in cases where DSIS collects information under section 4(1), cf. section 3, of the DSIS Act, about all persons who within a given period of time have contacted a public authority or about other groups of persons who similarly have not been identified in advance, DSIS must as soon as permitted by circumstances in each case, make an assessment of whether the persons whom the information concerns are of relevance to DSIS' performance of its activities. To the extent that this is deemed not to be the case, the non-relevant information must be erased immediately. Collection of information of the type mentioned in section 4 is subject to prior approval by the Director General of DSIS or the legal head of DSIS. The same applies to collection of information about psychiatric diagnoses or other particularly sensitive health information.

As specified in section 18 of the DSIS Executive Order, physical or electronic information which must be preserved for posterity in accordance with provisions on storage and destruction issued by the National Archives may not be destroyed or erased, but must instead be handed over to the National Archives. If such information cannot be handed over to the National Archives for practical or security reasons, the information must – from the point in time when it should have been destroyed or erased – be processed separately from the other information held by DSIS to ensure that access to the information is restricted to employees with special authorisation from the Director General of DSIS.

3.2.3 About security of processing, see sections 3-5 and section 17 of the DSIS Executive Order on Security Measures

Under sections 7(2) and 8(2) of the DSIS Act, the Minister of Justice may lay down more detailed rules on DSIS' processing of information. Executive Order No. 516 of 23 May 2018 (Executive Order on security measures to protect personal information on natural and legal persons being processed by the Danish Security and Intelligence Service (DSIS) (the DSIS Executive Order on Security Measures) has been issued in pursuance thereof.

According to the legislative history of Act No. 503 of 23 May 2018, which implemented various consequential amendments to the DSIS Act as a result of the passing of the Data Protection Act and the General Data Protection Regulation (GDPR), it is a requirement that the level of security of processing laid down in executive orders issued under sections 7(2) and 8(2) of the DSIS Act is not lower than the level prescribed in section 41(1)-(4) and section 42 of the former Data Protection Act and executive orders issued pursuant thereto. The DSIS Executive Order on Security Measures is interpreted in accordance therewith.

Under section 3 of the DSIS Executive Order on Security Measures, DSIS must implement appropriate technical and organisational security measures to protect the information about natural or legal persons against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other unlawful processing in violation of the DSIS Act. The same applies to data processors processing information about natural and legal persons for DSIS.

According to section 4 of the DSIS Executive Order on Security Measures, DSIS must lay down specific internal provisions on security measures in the intelligence service

to clarify the provisions of the Executive Order, including in particular to lay down internal provisions on organisational matters and physical security, including security organisation, management of access control and authorisation schemes as well as control of authorisations.

Furthermore, under section 5 of the DSIS Executive Order on Security Measures, DSIS must ensure that the staff members who process information about natural and legal persons receive the necessary instructions.

Under section 17(1) of the DSIS Executive Order on Security Measures, all uses of personal information about natural and legal persons must be subject to machine registration (logging). The log must at least provide information about the time, user, type of use and identification of data subject or the search criterion used. The log must be kept for six months, and then be erased. DSIS may keep the log for up to five years, where necessary, to satisfy a special need. The provision in subsection (1) does not apply to information about natural and legal persons, which is contained in word processing documents and the like which are not available in their final form. The same applies to documents, which are available in their final form if the information in question is erased within a relatively short time limit set by DSIS.

3.2.4 About internal reviews, see sections 10 and 11 of the DSIS Executive Order

Section 10 of the DSIS Executive Order provides that DSIS must carry out regular random reviews concerning erasure, logging, initiation of inquiries, obtaining of information, interventions in the course of investigations and disclosure of information. The Director General of DSIS will lay down more detailed guidelines concerning such random reviews, see section 11 of the Executive Order.

3.3 Disclosure of information

3.3.1 About disclosure of information, see section 10 of the DSIS Act

Section 10 of the DSIS Act on disclosure of information provides in subsection (1) that DSIS is allowed to disclose information to DDIS if the disclosure may be of importance to the performance of the activities of the two intelligence services. The broad discretion thus allowed with regard to disclosure of information to DDIS is due to the close connection between the spheres of activity of the two intelligence services.

Under subsection (2), DSIS is allowed to disclose personal information to Danish administrative authorities (other than DDIS), private individuals and organisations, foreign authorities and international organisations subject to the conditions for internal processing in sections 6a and 7 of the DSIS Act. However, disclosure of information concerning purely private matters is also subject to the conditions in section 8(2) of the Data Protection Act. This means that the information may be disclosed only if (i) explicit consent has been obtained from the data subject; (ii) disclosure is made to safeguard private or public interests which clearly outweigh the interests of confiden-

tiality, including the interests of the data subject; (iii) disclosure is necessary for the performance of a public authority's activities or required for a decision to be made by the public authority; or (iv) if disclosure is necessary for the performance of the activities of a person or business on behalf of the public authorities. For DSIS' disclosure of information about legal persons to Danish administrative authorities (other than DDIS), private individuals and organisations, foreign authorities and international organisations, section 10(3) of the Act provides that the conditions for internal processing in section 8 of the Act must be satisfied.

Having regard to the serious implications which, depending on the circumstances, disclosure may involve for the data subjects, the conditions of disclosure in section 10(2) and (3) are supplemented by a condition in subsection (4) to the effect that DSIS will be allowed to disclose information about natural and legal persons only if the disclosure is deemed to be sound based on a specific assessment in each individual case.

According to the explanatory notes to section 10(4) of the DSIS Bill, this decision must be based on a test where all factors in each individual case are balanced against each other. In particular, this balancing of factors must include the specific contents of the information, the purpose of disclosure and an assessment of any adverse effects that disclosure may be deemed to involve for the data subject. The outcome of the soundness test may differ, depending on whether the disclosure is to another Danish administrative authority, a private individual or organisation, a foreign authority or an international organisation. For disclosure to foreign authorities, it may be taken into account in the test whether the disclosure of personal information is to be made with a view to preventing and investigating serious international crime which Denmark, too, has a material interest in combating. The conditions prevailing in the country of the recipient may also be taken into account in the test. The provision on disclosure is assumed to be supplemented by rules of a procedural nature issued administratively, which – like the provisions of DSIS' former internal guidelines on cooperation with foreign intelligence services and the like – will provide that disclosure of information to foreign authorities and international organisations etc. will usually be subject to approval at management level.

3.4 Legal political activity

3.4.1 About legal political activity, see section 11 of the DSIS Act

Section 11 of the DSIS Act on legal political activity provides in subsection (1) that the participation by a natural person resident in Denmark in legal political activity does not in itself warrant processing of information about that person by DSIS. Subsection (2) provides, however, that the provision in subsection (1) does not preclude DSIS from processing information about a person's political activity with a view to determining if the activity is legal. According to subsection (3), subsection (1) also does not preclude DSIS from including information about the leadership of political associations and organisations when processing information about such associations and organisations.

According to the explanatory notes to the DSIS Bill concerning section 11, the expression in subsection (1) "a natural person resident in Denmark" covers (i) Danish nationals; (ii)

Nordic nationals and other foreign nationals with residence in Denmark if the person in question is registered with the National Register; as well as (iii) asylum seekers having their (known) residence in Denmark for more than six months. Concerning political activity, the notes state that this must generally be taken as meaning any activity which concerns government and influence of existing societies and social conditions and that political activity not only covers statements but also includes political manifestations in other forms such as participation in political demonstrations.

The prohibition of processing information about legal political activity is not absolute. This will be seen from the expression "not in itself". Thus, DSIS is allowed to process information about a person's legal political activity if there are other factors, which mean that a person has attracted DSIS' interest. If the person in question has already become the focus of DSIS in connection with the performance of its activities, DSIS is also allowed to process information about the person's legal political activity if such information is relevant to the inquiries. By way of example, this could be a person who engages in political activity as a pretext for planning, preparing or engaging in espionage, terrorism or violent extremist activity. In each individual case, DSIS must thus assess whether processing of information about legal political activity is warranted by other grounds than the very performance of such activity, and such an assessment is inherently discretionary.

Under subsection (2), DSIS is allowed in the course of its investigations to process personal information about a person's political activity with a view to determining if the activity is legal or illegal. If the investigations show that the activity is legal, the personal information must be erased. TET may verify that the provision of subsection (2) is not abused to circumvent the prohibition in subsection (1) and thus that DSIS' investigations of whether a given political activity is legal is made in a sound and reasonable manner with due respect of the purpose underlying the prohibition.

Subsection (3) of the provision provides that in cases involving political associations and organisations DSIS is allowed to include information about the leadership of the association or organisation. The prohibition in subsection (1) against processing of information about legal political activity does not include processing of information about legal persons. However, the general rules of the Act on processing of information about legal persons apply to such processing of information.

Information about the leadership only covers identification information about the leaders in question, which in relation to a political association could be members of the general council or executive committee, ministers, members of Parliament and of the European Parliament and members of regional and local councils. Those who do not belong to this category would be ordinary members of a political party, persons supporting others' candidature for political office, delegates as well as participants in seminars, deputations and election meetings.

TET may oversee that a person's legal political activity in the form of participation in the leadership of a political organisation or association is only processed to the extent that it may be regarded as necessary for a meaningful processing of information about the organisation or association. According to the explanatory notes to the DSIS Bill concerning the provision in subsection (3), procedures must be implemented to prevent abuse of free text searches, e.g. in the form of self-oversight, logging or other security measures which will mitigate the risk of abuse and allow TET to identify the person who has made a particular search and the purpose for which the search was made.

3.5 Rules on subject access requests etc.

3.5.1 About subject access requests, see sections 12 and 13 of the DSIS Act

Under section 12 of the DSIS Act, natural and legal persons are not entitled to access information processed by DSIS about them or entitled to know whether DSIS is processing information about them. If special circumstances weigh in favour of doing so, however, DSIS may decide to grant full or partial access to such information.

Under section 13(1) of the DSIS Act, natural and legal persons are allowed to request TET to check if DSIS is processing information about them in violation of DSIS legislation. TET will verify that this is not the case and then notify the data subject. If special circumstances weigh in favour of doing so, TET may order DSIS to grant full or partial access to the information in the same way as under section 12.

Section 13 of the DSIS Act thus establishes an indirect subject access request system, meaning that as part of its oversight of DSIS' processing of information about natural and legal persons, TET must also check, if so requested by such a data subject, if DSIS is processing information about the data subject in violation of DSIS legislation. As part of this indirect subject access request system, TET is entitled among other things to order DSIS to erase information which, in the opinion of TET, DSIS is processing in violation of DSIS legislation. TET will verify that DSIS is not processing information about the data subject in violation of DSIS legislation and then notify the data subject. According to the explanatory notes to the Bill concerning this provision, however, it must only be possible to infer from TET's reply that no information is being processed about the data subject in violation of DSIS legislation. Accordingly, it must not be stated in or possible to infer from the reply whether any information is being or has been processed at all, whether any information has been processed in violation of DSIS legislation or whether information is being processed in compliance with DSIS legislation.

It can be seen from subsection (2) of the provision that if it is established in connection with a check under subsection (1) that DSIS processes information which no longer meets the conditions in sections 7(1) and 8(1), such information must be erased, regardless of section 9a(2).

Under subsection (3) of the provision, TET may, if special circumstances weigh in favour of doing so, order DSIS to grant full or partial access to the information mentioned in section 12(1).

It follows from section 2(3) of the PNR Act that when RPNR processes information on behalf of DSIS, the DSIS Act and rules issued under the DSIS Act will apply to the extent that the processing is not governed by provisions of the PNR Act. Thus, in connection with a check performed under section 13(1) of the DSIS Act, TET will thus check if RPNR is processing information about the person in question on behalf of DSIS without being entitled to do so.

A person who has received a reply from TET under section 13 of the DSIS Act is not entitled to receive a reply to a new request until six months after the most recent reply.

3.6 RPNR's processing of passenger name records (PNR information) for DSIS

3.6.1 Obtaining of intelligence by RPNR for DSIS, see sections 4 and 16 of the PNR Act

Under section 4(3)(i) of the PNR Act, airlines must disclose PNR Information, if so requested by RPNR in each case, where DSIS believes that the information may be of significance to the performance of its activities concerning prevention and investigation of offences under Parts 12 and 13 of the Penal Code.

Further, under section 16(3)(ii) of the PNR Act, RPNR may request the PNR units of other EU member states to disclose PNR information or the result of the processing of such information where DSIS believes that the information may be of significance to the performance of its activities concerning prevention and investigation of offences under Parts 12 and 13 of the Penal Code.

3.6.2 RPNR's processing and disclosure of PNR information on behalf of DSIS, see sections 8, 10 and 15 of the PNR Act

Under section 8(1) of the PNR Act, RPNR must store the result of a processing operation carried out for DSIS under paras (i) - (iv) of section 10 for as long as it is necessary to inform DSIS of a hit.

Para. (i) of section 10 of the PNR Act provides that RPNR must process PNR information to vet passengers before their scheduled arrival to or departure from Denmark to identify persons which DSIS is required to look into, as such persons may be involved in terrorist activities or serious crime punishable by at least three years' imprisonment.

Further, under para. (ii) of section 10 of the PNR Act, RPNR is allowed to process PNR information where DSIS believes that the information may be of significance to the performance of its activities concerning prevention and investigation of offences under Parts 12 and 13 of the Penal Code.

Moreover, under section 15(1) of the PNR Act, RPNR must disclose PNR information or the result of the processing of such information to DSIS as soon as possible in order to allow DSIS to examine the information more closely.

3.6.3 About security of processing, see section 24 of the PNR Act

Paras (i) - (vi) of section 24(1) of the PNR Act provide that RPNR must keep records of the following processing activities as a minimum:

1) Collection

2) Search

3) Changes

4) Disclosure

5) Masking and unmasking

6) Erasure

Subsection (2) of section 24 provides that the records to be maintained under paras (i) - (v) of subsection (1) must render it possible to determine the purpose and date and time of the processing activities. In addition, it must be possible in relation to, among other things, information about searches or unmasking to identify the user having performed the processing activity as well as the recipient of the information.

Furthermore, under section 24(5), RPNR must, if so requested, make the records available to the national supervisory authority, i.e. the Danish Data Protection Agency and TET.

Given the overlap which to a certain extent exists between the powers of the Danish Data Protection Agency and those of TET with regard to security of processing oversight, TET will – in connection with its security of processing oversight activities – contact the Danish Data Protection Agency for the purpose of clarifying to which extent the Agency intends to oversee or has overseen security of processing compliance in RPNR.

Annual report 2022
Danish Security and Intelligence Service
Published by the Danish Intelligence Oversight Board, June 2023

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

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

Members of the Danish Intelligence Oversight Board

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

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