



Danish Intelligence Oversight Board

Annual report 2023

Danish Security and Intelligence Service (DSIS)



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 2023 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 Police (PPNR) in 2023.

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

TET reviews 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 deletion 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 reviews compliance with the provisions of the PNR Act concerning

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

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

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

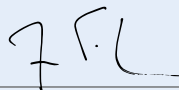
Copenhagen, May 2024



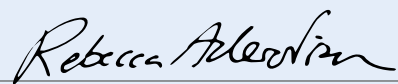
Pernille Christensen



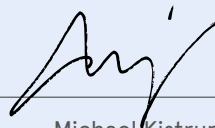
Henrik Udsen



Jesper Fisker



Rebecca Adler-Nissen



Michael Kistrup

CONTENTS

1. Introductory comments	3
2. Generally about TET's review activities	4
2.1 General prerequisites for TET's reviews and its expectations from DSIS, DDIS, CFCS and PPNR	5
2.2 Scale for TET's comments	8
2.3 Review method	9
3. TET's review in 2023	14
3.1 Summary of TET's review in 2023	14
3.2 Review of DSIS in 2023	17
3.2.1 Review of DSIS' opening of new files	18
3.2.2 Review of DSIS' compliance with the rules on deletion	18
3.2.3 Reviews of DSIS' use of other agencies' systems	19
3.2.4 Reviews of DSIS' compliance with the rules on legal political activity	20
3.2.5 Review of DSIS' special databases	21
3.2.6 Review of DSIS' transit systems	21
3.2.7 Review of DSIS' internal compliance review	24
3.2.8 Review of DSIS' security clearance cases	24
3.2.9 Review of DSIS' compliance with the rules on material subject to legal deposit etc.	25
3.2.10 Review of DSIS' security of processing	25
3.2.11 Follow-up on TET's reviews of DSIS in 2022	26
3.2.12 TET's technical reviews and mapping of DSIS' IT landscape	27
3.3 DSIS' briefing of TET	28
3.4 Subject access requests under sections 12 and 13 of the DSIS Act	30
3.4.1 Processing of requests by TET	30
3.4.2 Number of requests and processing time	30
3.5 DSIS' processing times in 2023	32
3.6 Reviews of PPNR in 2023	32
3.7 Cases submitted to the Minister of Justice for decision	32
3.7.1 Application of the DSIS Act and the DSIS Executive Order in relation to DSIS' processing of information in another agency's database	34

APPENDIX

1. About Danish Security and Intelligence Service (DSIS)	37
2. About Danish Intelligence Oversight Board (TET)	38
2.1 TET's duties in relation to DSIS	39
2.2 TET's access to information held by DSIS	40
2.3 Responses available to TET	40
3. Legal framework	42
3.1 Procurement of information	42
3.1.1 About collection and obtaining of information, see section 3 of the DSIS Act	42
3.1.2 About the obligation of other administrative authorities to disclose information to DSIS, see section 4 of the DSIS Act	43
3.2 Internal processing of information	43
3.2.1 About internal processing of information under sections 6a-8 of the DSIS Act	43
3.2.2 About deletion of information, see sections 9 and 9a of the DSIS Act and sections 1-3, 8 and 18 of the DSIS Executive Order	44
3.2.3 About security of processing, see sections 3-5 and section 17 of the DSIS Executive Order on Security Measures	46
3.2.4 About internal compliance review, see sections 10 and 11 of the DSIS Executive Order	47
3.3 Disclosure of information	47
3.3.1 About disclosure of information, see section 10 of the DSIS Act	47
3.4 Legal political activity	48
3.4.1 About legal political activity, see section 11 of the DSIS Act	48
3.5 Rules on subject access requests etc.	50
3.5.1 About subject access requests, see sections 12 and 13 of the DSIS Act	50
3.6 PPNR's processing of passenger name records (PNR information) for DSIS	51
3.6.1 Obtaining of intelligence by PPNR for DSIS, see sections 4 and 16 of the PNR Act	51
3.6.2 PPNR's processing and disclosure of PNR information on behalf of DSIS, see sections 8, 10 and 15 of the PNR Act	51
3.6.3 Security of processing, see section 24 of the PNR Act	51

1. INTRODUCTORY COMMENTS

The Danish 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 be able to perform this nationally important function, DSIS has broad powers under the law to procure information on private individuals and businesses. Confidentiality is therefore a fundamental prerequisite for DSIS's work as a national intelligence and security service.

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

As will appear from this report, TET has in 2023 carried out in-depth and intensive compliance reviews with regard to DSIS. TET's reviews focused on DSIS' processing of information and the prohibition of processing information solely on grounds of legal political activities.

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

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

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



Generally about TET's review activities

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

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

TET's activities are determined by law, including

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

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

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

TET's access to information

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

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

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

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

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

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

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

Response to TET's consultation questions

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

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

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

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

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

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

Follow-up on TET's reviews

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

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

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

2.2

Scale for TET's comments

TET's comments are based on the following scale:

COMMENTS	BACKGROUND TO COMMENTS
»[...] does not give rise to any comments «	Used when TET agrees with the authority on how they are generally or specifically administering the law.
»On the information available, TET is unable to assess [...]«	Used when TET's review is limited by either factual or legal circumstances.
»TET finds it striking [...]«	Used for situations in the authority or legislation which do not quite match the general or immediate impression of an outsider.
»TET finds it problematic [...]«	Used for situations where no actual non-compliance with legislation has been established, but where there is considered to be a high risk that the situation could lead to non-compliance with legislation or where TET has been prevented from performing its activities for a certain period of time.
»TET has identified [...]«	Used for situations where actual non-compliance with legislation of an isolated nature or non-compliance with internal guidelines has been identified.
»TET finds it criticisable [...]«	Used for situations where actual non-compliance with legislation of a not insignificant extent has been identified or where TET has been prevented from exercising its activities for a prolonged period.
»TET finds it highly criticisable [...]«	Used for situations where serious non-compliance with legislation has been identified or where TET has been prevented from performing its activities for a prolonged period without the authority having demonstrated a willingness to ensure the necessary remedial action.

2.3

Review method

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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



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

Prior to initiating its reviews for a particular year, TET will share its risk analyses and review plans with DSIS, DDIS, CFCS and PPNR for the purpose of ensuring, among other things, openness about TET's assessment of the situation at each of the agencies. The openness also allows DSIS, DDIS, CFCS and PPNR to take into account TET's reviews in the organisation of the agencies' own internal compliance reviews, which contributes to TET's reviews and their internal compliance reviews collectively covering a larger part of the agencies' activities. Finally, the openness allows DSIS, DDIS, CFCS and PPNR to dedicate sufficient resources to serve TET.

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

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



TET's review in 2023

3.1

Summary of TET's review in 2023

In 2023, the Danish Intelligence Oversight Board (TET) has completed 48 out of 49 planned reviews of the Danish Security and Intelligence Service (DSIS) and 3 out of 3 planned reviews of the Danish National Police PNR unit (PPNR).

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

It is noted that the below references only represent a minor cross-section of TET's reviews of DSIS in 2023. For a full picture of TET's reviews of DSIS and PPNR, the report should be read in its entirety.

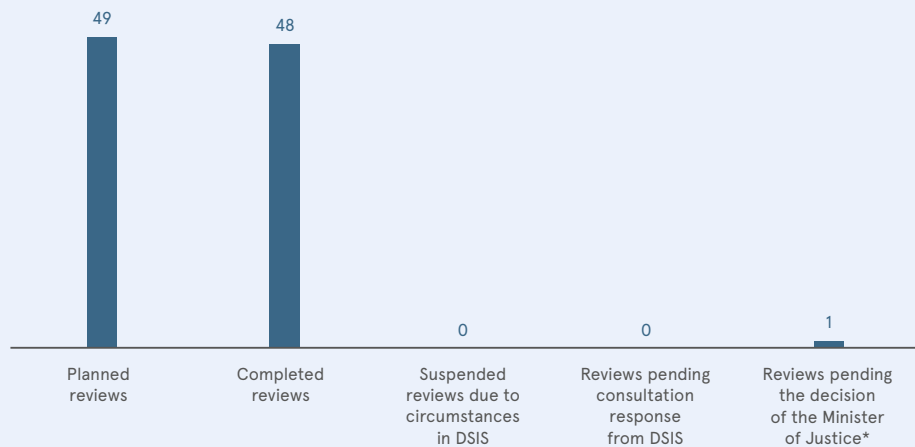
- ▶ 29 out of 48 reviews of DSIS and 3 out of 3 reviews of PPNR did not give rise to any comments. Of the remaining 19 reviews, none gave rise to observations about highly criticisable matters.

- ▶ TET found it criticisable
 - ▷ that DSIS processed 67,459 files in violation of section 9a(1) of the DSIS Act in a pre-production environment as, according to DSIS, the files should have been deleted after completion of testing and implementation of an IT system (section 3.2.2),
 - ▷ that DSIS processed 3,178 files in one database in violation of section 9a(1) of the DSIS Act, as TET found it highly likely that the files contained personal information and as the files had not been deleted or extended before expiry of the time limit for deletion set by DSIS (section 3.2.5),
 - ▷ that DSIS had not complied with its duty to inform TET, see section 3(2) of the DSIS Executive Order, in relation to various information processed in a transit system, considering that the information was transferred to DSIS in mid-2021, after which DSIS should have informed TET within four weeks, and that the transit system contained a not insignificant amount of sensitive information at the time of the transfer (section 3.2.5),
 - ▷ that DSIS had not complied with its duty to inform TET, see section 15 of the DSIS Executive Order, in relation to one database, given that, according to DSIS, the database had been in operation for several years. It should be noted that TET and DSIS are in dialogue about the interpretation of the scope of the duty to inform and the practical implementation thereof (section 3.2.5),
 - ▷ that DSIS processed 30 out of 30 randomly sampled emails in one shared mailbox on one of its networks in violation of section 17, see section 18, of the DSIS Executive Order on Security Measures, as DSIS had exceeded the time limit set by DSIS for holding information in transit systems (section 3.2.6),
 - ▷ that DSIS processed 24 out of 30 randomly sampled emails in one shared mailbox on one of its networks in violation of section 17, see section 18, of the DSIS Executive Order on Security Measures, as DSIS had exceeded the time limit set by DSIS for holding information in transit systems (section 3.2.6),
 - ▷ that DSIS processed 15 out of 30 randomly sampled emails in one shared mailbox on one of its networks in violation of section 17, see section 18, of the DSIS Executive

Order on Security Measures, as DSIS had exceeded the time limit set by DSIS for holding information in transit systems (section 3.2.6),

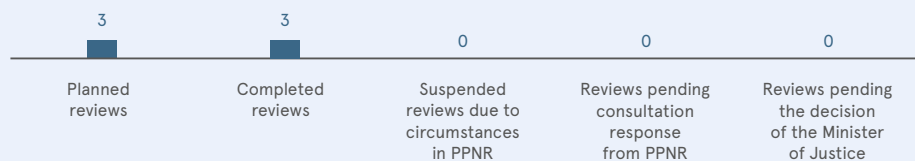
- ▷ that DSIS had not established a logging solution for the SQL servers holding material deleted following compliance reviews from two of the systems in accordance with section 17 of the DSIS Executive Order on Security Measures, see section 18 (section 3.2.9), and
- ▶ In 2023, TET received subject access requests from 24 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 three cases, DSIS had processed information about the persons in question, which at the time of the review no longer met the conditions of processing in section 7(1) or 8(1) of the DSIS Act. On that basis, DSIS has deleted the information. 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 (section 3.4.2).

TET's review of DSIS in 2023

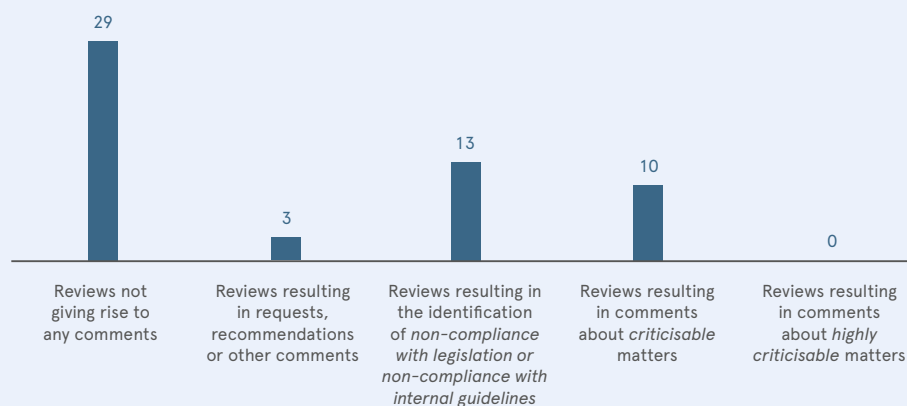


* See section 3.7

TET's review of PPNR in 2023

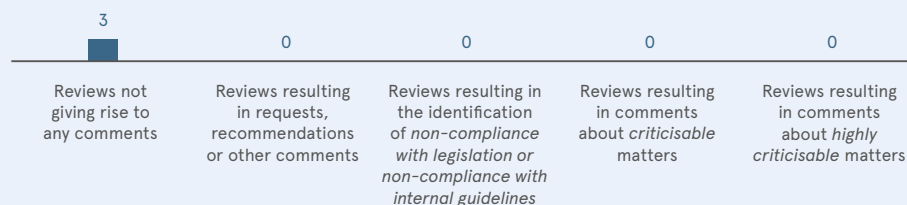


Results of TET's review of DSIS in 2023



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

Results of TET's review of PPNR in 2023



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

3.2

Review of DSIS in 2023

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 carried out reviews in 2023 of DSIS':

- ▶ opening of new files (section 3.2.1),
- ▶ compliance with rules on deletion (section 3.2.2),
- ▶ use of other agencies' systems (section 3.2.3),

- ▶ compliance with the rules on legal political activity (section 3.2.4),
- ▶ special databases (section 3.2.5),
- ▶ transit systems (section 3.2.6),
- ▶ internal compliance review (section 3.2.7),
- ▶ security clearance cases (section 3.2.8),
- ▶ compliance with the rules on material subject to legal deposit (section 3.2.9), and
- ▶ security of processing (3.2.10).

Furthermore, in 2023, TET completed

- ▶ follow-up on its reviews of DSIS in 2022 (section 3.2.11), and
- ▶ technical reviews and mapping of DSIS' IT landscape (section 3.2.12).

3.2.1

Review of DSIS' opening of new files

In 2023, TET completed reviews of DSIS' opening of new files within the areas of counter-espionage, counter-terrorism, non-proliferation and other operative files.

Comments by TET

TET's reviews of DSIS' opening of new files did not give rise to any comments.

3.2.2

Review of DSIS' compliance with the rules on deletion

Each year, DSIS conducts an audit of those of its files which will reach the time limit for deletion 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 deleted 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 deletion under DSIS legislation also apply to information in pre-production environments.

In 2023, TET completed reviews of DSIS' compliance with the rules on deletion by reviewing

- ▶ information held by DSIS about natural and legal persons on whom DSIS had started to consolidate information more than ten years ago,
- ▶ DSIS' decisions in 2023 not to delete 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 five pre-production environments.

Comments by TET

In 2023, TET's review of DSIS' compliance with the rules on deletion gave rise to the following comments:

- ▶ TET found it criticisable that DSIS processed 67,459 files in violation of section 9a(1) of the DSIS Act in a pre-production environment as, according to DSIS, the files should have been deleted after completion of testing and implementation of an IT system. TET agreed with DSIS that the specific information processed solely for the purpose of testing was not of a confidential nature, which is why it was not a condition for the processing to be logged, see section 18 of the DSIS Executive Order on Security Measures, cf. section 17. However, TET found that this presupposes that DSIS has established safeguards to ensure that test data in the environment in question is not used for operational purposes at a later date. DSIS can establish such safeguards by drawing up a policy for this purpose and by implementing it through, for example, action cards, training of employees, awareness, controls, etc. Furthermore, TET found that DSIS should prepare a risk assessment of whether information from the pre-production environment is accidentally or illegally destroyed, lost or altered as well as against unauthorised disclosure, abuse or other unlawful processing of such information in violation of the DSIS Act.
- ▶ TET found that in one case 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 deleted when the related source data (files, documents and entries) was deleted.
- ▶ TET found that in 164 cases DSIS processed information in violation of section 3 of the DSIS Executive Order on an analytics platform, as the information was not attached to logged source data. TET recommended that DSIS as soon as possible attach logged source data to the 164 pieces of information or set up the analytics platform as a journal or a special database, see sections 1 and 2 of the DSIS Executive Order.

TET's other reviews of DSIS' compliance with the rules on deletion did not give rise to any comments.

3.2.3

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 Measures.

In 2023, TET reviewed DSIS' use of other agencies' systems by reviewing

- ▶ DSIS' use of ten selected systems belonging to the Danish National Police to which selected DSIS employees have direct access, and
- ▶ DSIS' use of a selected system belonging to another agency to which selected DSIS employees have direct access.

Comments by TET

In 2023, TET's review of one selected system belonging to another agency to which DSIS employees have direct access gave rise to the following comments:

- ▶ TET found that DSIS does not fully comply with the requirement that DSIS must take the necessary technical and organisational measures to ensure that information about natural and legal persons is not disclosed to unauthorised persons, abused or otherwise processed in violation of the DSIS Act, see section 3 of the DSIS Executive Order on Security Measures, in relation to DSIS employees' access to the system, as the necessary reviews of DSIS' user actions has not been implemented.
- ▶ However, TET found it positive that DSIS and the agency are updating the agreement on DSIS' access to the system, that DSIS will inform TET when the agreement is updated and that DSIS expects to be able to initiate compliance reviews from Q1 2024. The reviews will be determined based on an assessment of risk and materiality. DSIS has subsequently sent the updated agreement to TET in 2023.

TET's reviews in 2023 of ten selected systems belonging to the Danish National Police to which DSIS employees have direct access did not give rise to any comments.

3.2.4

Reviews 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 deleted. This applies no matter that the overall time limits for deletion 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 2023, TET initiated a review of DSIS' compliance with the rules on legal political activity on the basis of a search in DSIS' shared mailboxes in order to identify information about individuals' political activities when participating in demonstrations where DSIS' need to process information was not immediately apparent from the context. TET made supplementary searches in DSIS' systems to assess the legality of the individuals' political activities.

Comments by TET

TET and DSIS are still in dialogue about the results of the review. The result of the review will be discussed in TET's annual report for 2024

3.2.5

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.

In 2023, TET reviewed DSIS' operative databases.

Comments by TET

TET's review in 2023 of DSIS' operative databases gave rise to the following comments:

- ▶ TET found it highly probable that 3,178 files in a database contained personal information. On this basis, TET found it criticisable that DSIS processed 3,178 files in one database in violation of section 9a(1) of the DSIS Act, as the files had not been deleted or extended before expiry of the time limit for deletion set by DSIS.
- ▶ TET found it criticisable that DSIS had not complied with its duty to inform TET, see section 15 of the DSIS Executive Order, in relation to one database, considering that, according to DSIS, the database has been in operation for several years. It should be noted that TET and DSIS are in dialogue about the interpretation of the scope of the duty to inform and the practical implementation thereof.
- ▶ TET found that the logging of three databases as stated by DSIS does not fulfil the minimum requirements in section 17(1) of the DSIS Executive Order on Security Measures, but that DSIS has established logging which, in relation to the nature of the information and the risks associated with the processing, makes it possible for DSIS to reconstruct the processing to a relevant and proportionate extent. TET found that, in its responses to TET's consultation questions, DSIS has prepared separate documentation of its assessments of which measures it considers necessary to implement in order to provide an adequate level of security for the processing in the three databases in relation to the risks involved in the processing and the nature of the information to be protected, taking into account the state of the art and the costs associated with their implementation. TET also found that, on this basis, DSIS should establish and carry out an ongoing evaluation and testing of the security level of processing in the three databases.

TET's other reviews of DSIS' operational databases in 2023 did not give rise to any comments.

3.2.6

Review 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 operative information on transit systems.

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

According to subsection (2), second sentence, of the provision, documents that are in final form may be stored in systems in which no logging is performed if deletion takes place within a shorter period specified by DSIS.

DSIS has set a shorter time limit for deletion under section 17(2), second sentence, of the DSIS Executive Order on Security Measures when preparing guidelines for DSIS' use of transit systems. If DSIS processes information for longer than the time limit set by DSIS, it will thus constitute a breach of section 17(2) of the DSIS Executive Order on Security Measures.

According to DSIS' guidelines, "confidentiality" 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 on a system where no logging is established (transit system) for longer than the time limit set by DSIS.

In 2023, TET performed reviews of DSIS' processing of information in transit systems by reviewing

- ▶ two of DSIS' shared drives,
- ▶ shared mailboxes on three of DSIS' networks,
- ▶ work stations in two of DSIS' departments, and
- ▶ six of DSIS' other transit systems.

Comments by TET

TET's review in 2023 of DSIS' processing of information in transit system gave rise to the following comments:

- ▶ TET found it criticisable that DSIS processed 30 out of 30 randomly sampled emails in a shared mailbox on one of DSIS' networks in violation of section 17, see section 18, of the DSIS Executive Order on Security Measures, as DSIS had exceeded the time limit set by DSIS for holding information in transit systems. Furthermore, TET found that the sample error rate of 100 percent would most likely apply to the remaining 4,180 emails in the mailbox that were older than 28 days. In connection with the review, DSIS stated that the emails in the mailbox have now been deleted. Finally, TET found it problematic that, due to internal misunderstandings in DSIS, DSIS stated in its consultation response regarding the corresponding review in 2022 that a solution for automatic deletion had been put into operation for the shared mailbox, even though this was not the case.

- ▶ TET found it criticisable that DSIS processed 24 out of 30 randomly sampled emails in a shared mailbox on one of DSIS' networks in violation of section 17, see section 18, of the DSIS Executive Order on Security Measures, as DSIS had exceeded the time limit set by DSIS for holding information in transit systems. Furthermore, TET found that the sample error rate of 80 percent most likely applies to the remaining 781 emails in the mailbox, which were older than 28 days.
- ▶ TET found it criticisable that DSIS processed 15 out of 30 randomly sampled emails in a shared mailbox on one of DSIS' networks in violation of section 17, see section 18, of the DSIS Executive Order on Security Measures, as DSIS had exceeded the time limit set by DSIS for holding information in transit systems. Furthermore, TET found that the sample error rate of 50 percent most likely applies to the remaining 625 emails in the mailbox, which were older than 28 days.
- ▶ TET found it criticisable that DSIS had not complied with its obligation to inform TET, see section 3(2) of the DSIS Executive Order, in relation to a transit system, considering that the transit system was transferred to DSIS in mid-2021, after which DSIS should have informed TET within four weeks, and that the transit system contained a not insignificant amount of sensitive information at the time of the transfer. TET also found that the purpose of section 3 of the DSIS Executive Order is, among other things, to ensure that information procured is processed in systems subject to a time limit for deletion under section 1(2) or section 2(1) and (2) of the DSIS Executive Order and in which it is possible to conduct effective reviews following indirect subject access requests. In DSIS' opinion, the provision in section 3(2) of the DSIS Executive Order must be interpreted to mean that DSIS is obliged to record as soon as possible information, which it has not been able to record within four weeks of receipt or provision. Against this background, TET found it problematic that DSIS had not logged the information in a journal or database for a period of two years from the receipt in mid-2021 until TET's review in August 2023; see section 3(1) of the DSIS Executive Order.
- ▶ TET found that DSIS processed 6 out of 30 randomly sampled files on one shared drive in violation of section 17, see section 18, of the DSIS Executive Order on Security Measures, as DSIS had exceeded the time limit set by DSIS for holding information in transit systems. However, the data basis for the review was incorrect, as a significant number of files that should not have been included in the review were mistakenly included, which is why the result of the review is not accurate in relation to DSIS' general compliance with the rules for processing information on the shared drive. TET found it positive that DSIS cleaned up the shared drive after the review.
- ▶ TET found that DSIS processed 4 out of 30 randomly sampled files on one shared drive in violation of section 17, see section 18, of the DSIS Executive Order on Security Measures, as DSIS had exceeded the time limit set by DSIS for holding information in transit systems. Furthermore, TET found that the sample error rate of 13 percent most likely applied to the remaining 17,240 files on the drive, which were older than 28 days. In connection with the review, DSIS stated that it has established logging of the shared drive, which does not fulfil the minimum requirements in section 17(1) of the DSIS Executive Order on Security Measures, but that, considering the nature of the information and the risks associated with the processing, the logging enables DSIS to reconstruct the processing to a relevant and proportionate extent.
- ▶ TET found that DSIS processed an email on a workstation in violation of section 17, see section 18, of the DSIS Executive Order on Security Measures, as DSIS had exceeded the time limit set by DSIS for holding information in transit systems. Furthermore,

TET found that DSIS processed a physical document in a steel cabinet in violation of section 6a(5) of the DSIS Act.

- ▶ TET found that DSIS had not complied with its duty to inform, see section 15 of the DSIS Executive Order, in relation to the establishment of two transit systems in view of the fact that the transit systems in question are essential to DSIS' processing of personal data. It should be noted that TET and DSIS are in dialogue about the interpretation of the scope of the duty to inform and the practical implementation thereof.

TET's other reviews of DSIS' processing of information in transit systems in 2023 did not give rise to any comments.

3.2.7

Review of DSIS' internal compliance review

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

In 2023, TET performed a review of DSIS' internal compliance review. The review comprised all internal compliance reviews carried out by DSIS in 2022 and DSIS' planning of the same for 2024.

In November 2023, DSIS informed TET about DSIS'

- ▶ risk analysis concerning compliance with statutory requirements,
- ▶ notice about internal compliance review outlining the reviews that DSIS will implement in 2024, and
- ▶ review plan for 2024.

In addition, in 2023, DSIS regularly updated TET on its internal compliance review, see section 3.3.

Comments by TET

TET's review of DSIS' internal compliance review does not give rise to any comments. TET found that DSIS' organisation and performance of its internal compliance review were satisfactory, including that DSIS has ensured that the controls are well-documented and that the random reviews fairly present the audit results. Furthermore, DSIS regularly followed up on the results of its internal compliance review. Finally, there was a high degree of consistency between TET's and DSIS' risk analyses concerning the risk of DSIS non-compliance with legislation, which are prepared independently of each other.

3.2.8

Review of DSIS' security clearance cases

As a national security authority, DSIS must advise and assist public authorities and private individuals on security issues, including vetting of individuals. DSIS thus carries out

vetting at the request of the relevant authority when persons are being considered for authorisation to access classified documents.

In 2023, TET carried out reviews of DSIS' security clearance cases.

Comments by TET

TET's review of 'DSIS' security clearance cases did not give rise to any comments.

3.2.9

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 Danish 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 deletion 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, review cases, etc. In addition, DSIS stores a large amount of material, which falls 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.

In 2023, TET carried out a review of DSIS' compliance with the rules on material subject to legal deposit, etc. by reviewing three systems in which material covered by the rules on material subject to legal deposit and material falling within the scope of the shredding ban is held.

Comments by TET

TET's review of DSIS' compliance with the rules on material subject to legal deposit etc. in 2023 in two of the three systems did not give rise to any comments.

TET and DSIS are still in dialogue about the result of the review of one of the three systems. The result of the review will be discussed in TET's annual report for 2024.

3.2.10

Review of DSIS' security of processing

In 2023, in connection with its other reviews, TET carried out a review of DSIS' compliance with the rules on security of processing in the DSIS Executive Order on Security Measures.

Concerning 11 reviews, TET had questions to DSIS regarding specific security measures.

Comments by TET

TET's review of DSIS' compliance with the rules on security of processing in 2023 gave rise to the following comments:

- ▶ Based on three reviews in shared mailboxes, TET learned that DSIS generally had difficulties complying with the time limit set by DSIS for holding information in transit systems, see section 17, cf. section 18, of the DSIS Executive Order.
- ▶ TET found that DSIS should prepare a risk assessment of whether information from a pre-production environment is accidentally or unlawfully destroyed, lost or altered as well as against unauthorised disclosure, abuse or other unlawful processing.
- ▶ TET found that DSIS should establish a server-level logging solution where material deleted following compliance reviews from two systems is held, in accordance with section 17, see section 18, of the DSIS Executive Order on Security Measures.
- ▶ TET found that DSIS should establish and conduct an ongoing evaluation and test of the security level of processing in three databases.

3.2.11

Follow-up on TET's reviews of DSIS in 2022

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

In its annual report on the review of DSIS in 2022 (section 2.2), TET described a number of reviews which revealed that DSIS was holding information that should have been deleted because the information was no longer necessary for DSIS in the performance of its activities.

In 2023, TET followed up on its review of DSIS in 2022.

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

Based on the review in 2022, TET also recommended DSIS to make changes or submit specific briefings within two areas. In addition, based on the review in 2022, DSIS indicated that it would initiate measures or submit briefings within seven areas.

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

Comments by TET

TET's follow-up on its review of DSIS in 2022 gave rise to the following comments:

- ▶ TET found that DSIS had not implemented three of TET's recommendations. With regard to TET's recommendation from 2020, DSIS has continuously investigated the possibility of implementing it. For technical reasons, it has so far not been possible for DSIS to comply with the recommendation, but DSIS has informed TET that it would like to enter into a dialogue about possible alternative solutions.
- ▶ TET noted that in 13 cases, DSIS had implemented TET's recommendations and measures, which DSIS had stated that it would implement or submitted briefings, and that in one case, DSIS had decided not to implement a specific measure, which DSIS had stated that it would implement, but to implement an alternative measure instead.

2020	2021	2022	2023
	TET recommendation		
	TET recommendation		
	TET recommendation		
	DSIS measures		Alternative implemented
	DSIS measures		Implemented
	TET's request for briefing		Implemented
	DSIS measures		Implemented
		TET recommendation	Implemented
		TET recommendation	Implemented
		DSIS submission of briefing	Implemented
		DSIS measures	Implemented
		DSIS measures	Implemented
		DSIS measures	Implemented
		DSIS submission of briefing	Implemented
		DSIS measures	Implemented
		DSIS measures	Implemented

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.

3.2.12

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 2023 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 review of DSIS that DSIS' overall IT infrastructure is known to TET so that its review can be targeted at the parts of the infrastructure which pose the greatest risk of processing in violation of DSIS legislation.

In 2023, TET performed verification reviews and inspections by reviewing

- ▶ databases for the purpose of clarifying whether all DSIS databases are known to TET,
- ▶ file servers for the purpose of clarifying whether all DSIS file shares are known to TET, and
- ▶ mapping DSIS' server infrastructure.

- ▶ TET found reason to note that DSIS' response to TET's consultation question on DSIS' servers of 31 May 2023 had a number of shortcomings. Against this background, TET requested that DSIS in future responses to similar consultation questions ensure that all business systems of which the servers in question are a part are correctly stated in the response.

TET's verification reviews in 2023 of file servers and mapping of DSIS's server infrastructure did not give rise to any comments.

3.3

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 delete information which has reached the time limit for deletion of 15 years under section 9(1)
- ▶ DSIS' decisions under section 1(4) of the DSIS Executive Order not to delete files which have reached the time limit for deletion of ten years under section 1(2)
- ▶ DSIS' decisions under section 2(2) of the DSIS Executive Order to increase time limits for deletion 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 deletion 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 compliance review 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

In 2023, DSIS regularly informed TET of:

- ▶ DSIS' decisions under section 9(2) of the DSIS Act not to delete information which has reached the time limit for deletion of 15 years under section 9(1)
- ▶ DSIS' decisions under section 1(4) of the DSIS Executive Order not to delete files which have reached the time limit for deletion of ten years under section 1(2)
- ▶ DSIS' decisions under section 2(2) of the DSIS Executive Order to increase time limits for deletion 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 September 2022, 21 November 2023, 22 November 2023 and 23 November 2023, 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 control regarding section 4 of the DSIS Act
- ▶ DSIS' internal control regarding section 10 of the DSIS Act
- ▶ DSIS' internal control of information in transit systems
- ▶ DSIS' internal control of logging in specified systems
- ▶ DSIS' internal control of searches in specified systems
- ▶ DSIS' internal control of deletion of PNR information
- ▶ DSIS' internal control of processing of information about legal political activity
- ▶ DSIS' internal control of material classified as TOP SECRET
- ▶ DSIS' audits
- ▶ DSIS' internal control of registration of files in electronic systems
- ▶ DSIS' internal control of deletion in selected systems

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

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

3.4.1 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 delete 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.

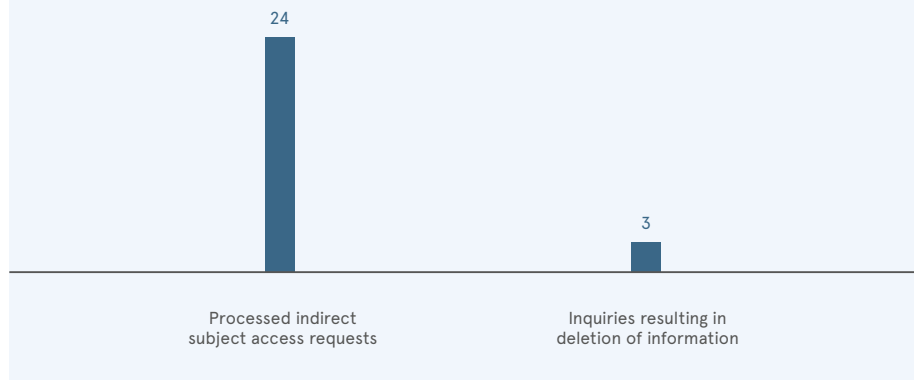
3.4.2 Number of requests and processing time

In 2023, TET received subject access requests from 24 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 three 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. DSIS has on that basis deleted the information. 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.

In 2023, the average processing time for the processed requests was 107 days, 54 days of which were DSIS' processing time. Compared with 2022, the average processing time decreased by 65 days. In 2023, a number of the indirect subject access request cases were suspended pending TET and DSIS' clarification concerning the search in a specific system. These cases therefore had a longer case processing time in DSIS.

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 the process are presented to TET at monthly meetings where it decides how to respond to the requests.

Indirect subject access requests



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, that the IT systems must facilitate efficient searches in the relevant systems and deletion of information at data-level.

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 with a view to ensuring that TET's reviews in connection with indirect subject access requests are effective and relevant. TET's reviews cover a number of central systems in DSIS. However, in TET's assessment, the reviews should cover an additional five systems, which, for various reasons, are not currently covered, which affects the completeness of TET's reviews. TET and DSIS are in dialogue about a joint clarification of the scope of the indirect subject access request system, including which systems are covered by the system and what technical requirements for search functions can be imposed on DSIS' systems.

Systems that should be covered by TET's investigations, but currently is not



3

Systems in which it is not technically possible to conduct efficient searches



1

System currently out of operation due to defect



1

System identified by TET as relevant. TET and DDIS are currently in dialogue about search functions in the system

3.5

DSIS' processing times in 2023

In 2023, TET submitted 24 legal consultations to DSIS in connection with its review activities. DSIS responded to 16 of TET's consultation questions within the specified deadline and eight after the specified deadline. DSIS' average delay in responding to consultation questions after the stated deadline was eight working days.

DSIS has previously faced challenges with long processing times when responding to TET's consultation questions. In 2022, TET and DSIS developed a new process for handling consultations to support DSIS in responding to TET's consultation questions within the agreed deadline. In 2023, DSIS responded to the majority of TET's consultation questions within the agreed deadline, and the average delay has been limited. TET finds it very positive that DSIS has not experienced any challenges with case processing times in 2023 when responding to TET's consultation questions.

3.6

Reviews of PPNR in 2023

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

PPNR'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 PPNR.

In 2023, TET performed reviews of PPNR's processing of information about airline passengers on behalf of DSIS and DDIS by reviewing

- ▶ data searches on behalf of DSIS,
- ▶ disclosures of information to DDIS, and
- ▶ the obtaining of information from foreign partners on behalf of DSIS and DDIS.

Comments by TET

TET's reviews in 2023 of PPNR's processing of information about airline passengers on behalf of DSIS and DDIS did not give rise to any comments.

3.7

Cases submitted to the Minister of Justice for decision

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

At the end of each compliance review, TET issues a statement to DSIS describing the results of the review. The statement may also contain a description of one or more measures, which DSIS should take in TET's opinion. If DSIS decides not to comply with a recommendation issued by TET in a statement in exceptional cases, DSIS must notify TET and without

undue delay submit the matter to the Minister of Justice for a decision. If the Minister of Justice decides not to comply with the recommendation from TET, the Government must notify the Parliamentary Intelligence Services Committee. The responses available to TET towards DSIS are described in more detail in section 2.3 of the Appendix and in section 19 of the DSIS Act.

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

QUESTION	DATE OF SUBMISSION	STATUS
<p>Whether TET has authority to review DSIS' deletion of material obtained under the rules of the Danish Administration of Justice Act.</p> <p>The submission was made on the basis of a number of TET's reviews in 2022, which gave rise to doubts as to how the rules on the destruction of material obtained under section 791 of the Danish Administration of Justice Act interact with the rules on deletion in section 9 of the DSIS Act and section 2(2) and (3) of the DSIS Executive Order.</p>	4 July 2023	Awaiting the decision of the Minister of Justice.
<p>Whether TET can review whether DSIS complies with the national security standard for information security ISO 27001 in connection with reviewing DSIS's compliance with the DSIS Executive Order on Security Measures.</p> <p>Discussed in more detail in TET's annual report for 2022 (section 2.2.10).</p>	27 June 2022	Awaiting the decision of the Minister of Justice.
<p>Whether the DSIS Act and the DSIS Executive Order apply to the processing of information in a database made available to DSIS by another agency.</p> <p>The matter was mistakenly not addressed in TET's annual report for 2022. Therefore, see this report (section 3.7.1).</p>	14 December 2021	<p>Decided by the Minister of Justice on 2 June 2022.</p> <p>The Minister of Justice found that the DSIS Act and the DSIS Executive Order do not apply to the processing of information in a database made available to DSIS by another agency solely for the purpose of DSIS processing the information contained therein.</p>
<p>Whether time limits for deletion for databases, see section 2(2) of the DSIS Executive Order, should be calculated from the time of entry.</p> <p>Discussed in more detail in TET's annual report for 2021 (section 3).</p>	TET has not been informed when DSIS submitted the case to the Minister of Justice.	<p>Decided by the Minister of Justice on 1 November 2021.</p> <p>Resulted in clarification of the DSIS Executive Order (e.g. amended provision in section 2(2)).</p>
<p>Whether the DSIS Act with accompanying comments and subsequent Executive Order should be understood to mean that personal information which DSIS no longer considers necessary for the performance of its activities must be deleted, see sections 7(1) and 8(1) of the DSIS Act, cf. section 5(5) of the Data Protection Act, even if the information is included in a document whose other information is still necessary for DSIS.</p> <p>Discussed in more detail in TET's annual report for 2016 (section 5).</p>	12 May 2015	<p>Decided by the Minister of Justice on 23 September 2016.</p> <p>Resulted in clarification of the DSIS Act (e.g. new provision in section 9a).</p>

In 2018, TET criticised that DSIS had had a special database since 2012 for which DSIS had not set a time limit for deletion, but for which DSIS expected to set a time limit for deletion longer than five years (see TET's annual report for 2018, section 1.2.7).

In connection with TET's review of the database in question in 2020, TET received a briefing from DSIS on 3 April 2020, which stated, among other things, that DSIS did not consider itself the data controller of the database.

In connection with its review, TET found that – despite its repeated criticism – DSIS had not clarified the legal framework for the database in question in the period from TET's review in 2018 until 3 April 2020. In this connection, TET consulted another agency in 2020 about the database (see TET's annual report for 2020, section 1.2.7).

TET also found that DSIS disagreed with TET's interpretation of section 2(2) of the DSIS Executive Order, including whether the DSIS Act and the DSIS Executive Order applied to the processing of information in the database made available to DSIS by another agency solely for the purpose of DSIS' processing of information therein. On that basis, TET requested DSIS to submit the case to the Minister of Justice for a decision, which DSIS subsequently did.

The Minister of Justice decided the case on 2 June 2022 and found that the DSIS Act and the DSIS Executive Order did not apply to the processing of information in the database made available to DSIS by another agency solely for the purpose of DSIS' processing of information in the database.

Appendix

1. ABOUT DANISH SECURITY AND INTELLIGENCE SERVICE (DSIS)

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 reviewing 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.

2. ABOUT DANISH INTELLIGENCE OVERSIGHT BOARD (TET)

TET'S ACTIVITIES

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

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

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

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

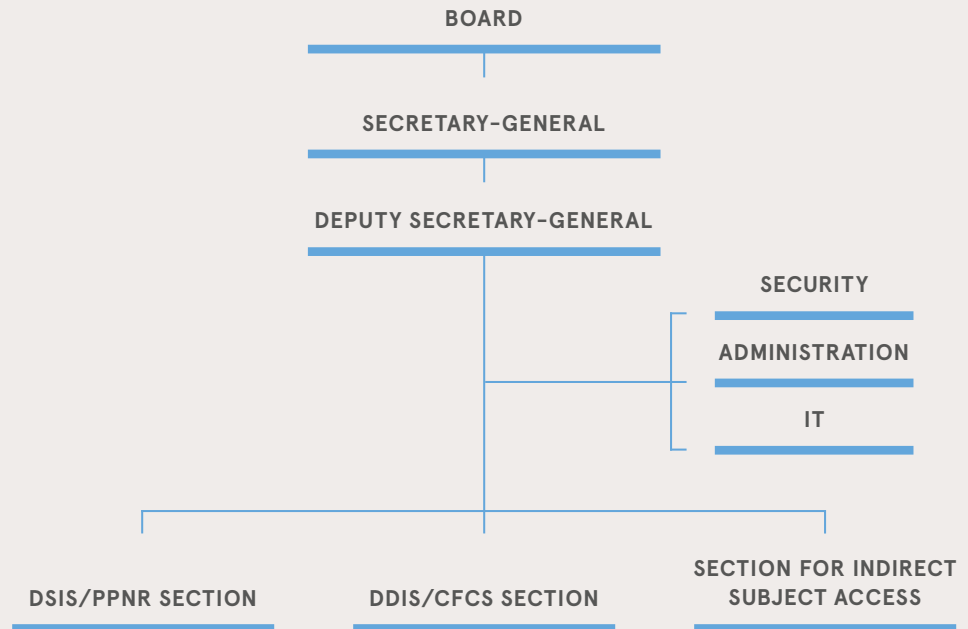
TET had the following members as at the end of 2023:

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

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

TET is supported by a secretariat, which is subject solely to the instructions from TET in the performance of its duties. TET recruits its own secretariat staff and decides which educational and other qualifications the relevant candidates must have. At the end of 2023, the secretariat consisted of a head of secretariat, who is in charge of the day-to-day management, a deputy, three lawyers, two IT consultants and an administrative employee.

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



2.1

TET's duties in relation to 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 deletion 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 PPNR procures, processes and discloses information on behalf of DSIS.

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

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 review activities and request the presence of a DSIS representative to give an account of current processing activities.

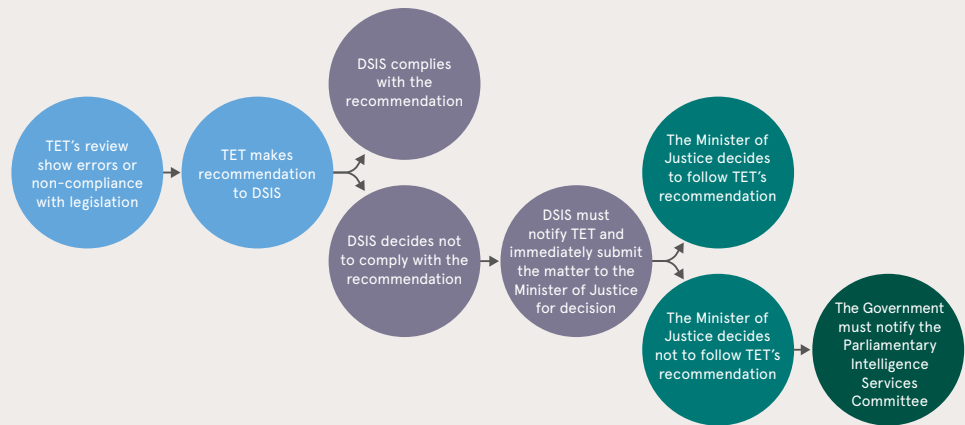
DSIS has made office premises available to TET for TET to make its own searches in DSIS' IT systems.

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. At the end of each review, TET issues a statement to DSIS describing the results of the review. The statement may also contain

a description of one or more measures, which DSIS should take in TET's opinion. If DSIS decides not to comply with a recommendation issued by TET in exceptional cases, DSIS must notify TET and without undue delay submit the matter to the Minister of Justice for a decision. If the Minister of Justice decides not to comply with the recommendation of TET, the Government must notify the Parliamentary Intelligence Services Committee.



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 delete 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 review 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 review 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 delete information under the indirect subject access request system.

TET submitted its most recent annual report on its activities to the Minister of Justice in June 2023. The annual report was submitted to the Parliamentary Intelligence Services Committee and then published in November 2023.

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 as most recently amended by Act No. 2601 of 28 December 2021).
- 7) Executive Order on the PNR Unit's processing of PNR information (Executive Order No. 1035 of 29 June 2020 as most recently amended by Executive Order No. 2562 of 17 December 2021).

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.

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

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 deletion 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 delete 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, deletion 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 deletion 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 delete 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 deleting the information as section 9 of the DSIS Act prescribes that DSIS' obligation to delete 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 deletion 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 deletion of personal information.

Thus, section 1 of the DSIS Executive Order provides that DSIS must delete 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, deletion 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(2) of the DSIS Executive Order, DSIS must lay down a time limit for deletion 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 deletion 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 deletion 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 deletion 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 deleted 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 deletion, 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 deleted, regardless of whether the time limit for deletion 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 reviews 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 delete 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 deletion at data-level whereas the provision in subsection (1) concerns deletion at case- and document-level. DSIS is thus not required to delete 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 deletion has not yet expired. Furthermore, it is emphasised that TET may still review in connection with its random reviews 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 delete individual pieces of information which form part of documents etc. which are to be retained, in connection with such random reviews. However, DSIS will still be required to delete 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' deletion 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), see 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 deleted 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 deleted, 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 deleted – 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 deleted. 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 deleted within a relatively short time limit set by DSIS.

3.2.4

About internal compliance review, 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 deletion, 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 confidentiality, 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 deleted. 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 review 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-review, 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 review 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 review of DSIS' processing of information about natural and legal persons, TET must also review, 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 delete 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 review under subsection (1) that DSIS processes information which no longer meets the conditions in sections 7(1) and 8(1), such information must be deleted, 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 PPNR 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 review performed under section 13(1) of the DSIS Act, TET will thus review if PPNR 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

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

3.6.1

Obtaining of intelligence by PPNR 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 PPNR 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, PPNR 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

PPNR'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, PPNR 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 PPNR 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, PPNR 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, PPNR 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

Security of processing, see section 24 of the PNR Act

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

- 1) Collection
- 2) Search
- 3) Changes

- 4) Disclosure
- 5) Masking and unmasking
- 6) Deletion

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), PPNR 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 in PPNR, TET will – in connection with its security of processing review activities – contact the Danish Data Protection Agency for the purpose of clarifying to which extent the Agency intends to review or has reviewed security of processing compliance in PPNR.

Annual report 2023

Danish Security and Intelligence Service

Published by the Danish Intelligence Oversight Board, May 2024

Layout + illustrations: Eckardt ApS

Portrait photographs: Lars Engelgaard / Sophie Kalckar

The publication is available on TET's website at www.tet.dk



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