



Danish Intelligence Oversight Board

Annual report 2023

Danish Defence Intelligence Service (DDIS)



TO THE MINISTER OF DEFENCE

The Danish Intelligence Oversight Board (TET) hereby submits its report on its activities concerning the Danish Defence Intelligence Service (DDIS) for 2023 in accordance with section 19 of the Danish Defence Intelligence Service (DDIS) Act (Consolidated Act No. 1287 of 28 November 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 aim of this annual report is to provide general information about the nature of the review activities performed with regard to DDIS.

TET reviews DDIS' compliance with the provisions of the DDIS 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 Security and Intelligence Service (DSIS) 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.

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

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 the PNR Unit of the Danish Police (PPNR) procures, processes and discloses information on behalf of DDIS. TET also reviews PPNR's procurement, processing and disclosure of information on behalf of DSIS, and TET's reviews of PPNR are therefore discussed in TET's annual report on the review of DSIS in 2023.

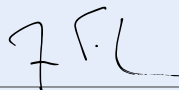
Copenhagen, May 2024



Pernille Christensen



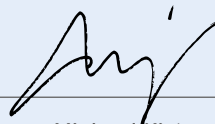
Henrik Udsen



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	15
3.2 Review of DDIS in 2023	18
3.2.1 Review of DDIS' targeted intelligence obtaining (SIGINT)	18
3.2.2 Reviews of DDIS' handling of raw data	19
3.2.3 Review of DDIS' raw data searches	20
3.2.4 Review of DDIS' collection of open source intelligence (OSINT)	21
3.2.5 Review of DDIS' electronic non-communications intelligence obtaining (ELINT)	22
3.2.6 Review of DDIS' deletion of information	22
3.2.7 Reviews concerning DDIS' computer network operations (CNO)	25
3.2.8 Review of DDIS' processing of information on drives	26
3.2.9 Review of DDIS' disclosure and processing of information in communication systems	26
3.2.10 Review of DDIS' other processing of information	26
3.2.11 Review of DDIS' internal compliance review	27
3.2.12 Follow-up on TET's reviews of DDIS in 2022	27
3.2.13 TET's technical reviews and mapping of DDIS' IT landscape	28
3.3 DDIS' briefing of TET	28
3.4 Subject access requests under sections 9 and 10 of the DDIS Act	29
3.4.1 Processing of requests by TET	29
3.4.2 Number of requests and processing time	29
3.5 DDIS' processing times in 2023	30
3.6 Cases submitted to the Minister of Defence for decision	30

APPENDIX

1. About Danish Defence Intelligence Service (DDIS)	35
2. About Danish Intelligence Oversight Board (TET)	37
2.1 TET's duties in relation to DDIS	38
2.2 TET's access to information held by DDIS	39
2.3 Responses available to TET	39
3. Legal framework	41
3.1 Procurement of information	41
3.1.1 About collection and obtaining of information, see section 3 of the DDIS Act	41
3.2 Internal processing of information	42
3.2.1 About internal processing of information, see sections 3e-5 of the DDIS Act	42
3.2.2 About deletion of information, see sections 6 and 6a of the DDIS Act	43
3.2.3 About security of processing, see sections 2-5 of the DDIS Executive Order on Security Measures	44
3.3 Disclosure of information	45
3.3.1 About disclosure of information, see section 7 of the DDIS Act	45
3.4 Legal political activity	46
3.4.1 About legal political activity, see section 8 of the DDIS Act	46
3.5 Rules on subject access requests etc.	48
3.5.1 About subject access requests, see sections 9 and 10 of the DDIS Act	48
3.6 Processing of passenger name records (PNR information) for DDIS	48
3.6.1 Request for information concerning natural persons resident in Denmark, see section 15(3) of the PNR Act	48
3.6.2 Obtaining of intelligence by PPNR for DDIS, see sections 4 and 16 of the PNR Act ...	49
3.6.3 PPNR's processing and disclosure of PNR information on behalf of DDIS, see sections 8, 10 and 15 of the PNR Act	49
3.6.4 Security of processing, see section 24 of the PNR Act	50

1. INTRODUCTORY COMMENTS

The intelligence-related activities of the Danish Defence Intelligence Service (DDIS) are directed at conditions abroad, and in that connection DDIS is charged with the responsibility of collecting, obtaining, processing, analysing and communicating intelligence concerning conditions abroad which is of importance to Denmark and Danish interests for the purpose of providing the intelligence basis for Danish foreign, security and defence policy and contributing to preventing and countering threats against Denmark and Danish interests. DDIS thus performs a vital function in ensuring a free, democratic and safe society. In order to be able to perform this nationally important function, DDIS has broad powers under the law to procure information. Confidentiality is therefore a fundamental prerequisite for DDIS' work as Denmark's foreign and military intelligence service.

TET's review activities contribute to the legitimisation of DDIS' activities by strengthening public confidence in the lawfulness of DDIS' activities. It is a prerequisite for effective and accurate compliance reviews that TET is given full, complete and timely access to DDIS' 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 DDIS. TET's reviews focused on DDIS' procurement, processing and deletion of information.

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 30 out of 33 planned reviews of the Danish Defence Intelligence Service (DDIS).

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 DDIS in 2023. For a full picture of TET's reviews of DDIS, the report should be read in its entirety.

- ▶ 21 out of 30 reviews of DDIS did not give rise to any comments. Of the remaining nine reviews, none gave rise to any comments on highly criticisable matters.
- ▶ TET found it criticisable
 - ▷ that DDIS processed 8 out of 30 randomly sampled files in an analytics system in violation of section 6(1) of the DDIS Act as the files were older than 15 years and as DDIS was not aware of whether new information relating to the same case had been procured within the past 15 years (section 3.2.6),
 - ▷ that DDIS processed 7 out of 15 randomly sampled files in a system for handling external communication in violation of section 6(1) of the DDIS Act as the files were older than 15 years and DDIS was not aware of whether new information relating to the same case had been procured within the past 15 years (section 3.2.6),
 - ▷ that DDIS processed 11 out of 30 randomly sampled files in an internal email system in violation of section 6(1) of the DDIS Act as the files were older than 15 years and as DDIS was not aware of whether new information relating to the same case had been procured within the past 15 years (section 3.2.6), and
 - ▷ that DDIS, in violation of section 6a(1) of the DDIS Act, had by mistake not deleted 107 emails which DDIS had stated would be deleted based on TET's review in 2022 (section 3.2.12).
- ▶ TET identified
 - ▷ that in 2 out of 39 cases reviewed (5 percent), DDIS had searched raw data in violation of DDIS legislation because DDIS had searched such data without the search being carried out on behalf of DSIS within the framework of a court order obtained by DSIS or because DDIS itself had not obtained a court order for such searches, see section 3(3) of the DDIS Act (section 3.2.3), and
 - ▷ that on the basis of 1 out of 6 reviewed requests from DSIS, DDIS had in seven cases carried out searches of raw data in violation of DDIS legislation as the searches were not time-limited in accordance with the court order obtained by DSIS (section 3.2.3).
- ▶ TET recommended that DDIS as soon as possible implement measures to ensure that information about persons resident in Denmark stored in a system for handling external communication and in an internal email system is deleted in accordance with section 6 of the DDIS Act.

In TET's assessment, considering the total amount of files stored in the systems, a significant amount of information about persons resident in Denmark is processed in violation of the time limit for deletion in section 6(1) of the DDIS Act.

TET's assessment is based on the fact that TET's reviews of the systems in both 2022 and 2023 showed that information was stored in violation of the time limit for deletion in section 6(1) of the DDIS Act and that DDIS does not currently perform internal legal compliance reviews or own reviews to ensure that information stored in the systems is deleted in accordance with section 6 of the DDIS Act.

Based on the review of DDIS' deletion of information, TET learned that DDIS generally has difficulties complying with the rules on deletion under section 6(1) of the DDIS Act in systems where personal information older than 15 years is stored.

TET further noted that the amount of information about persons resident in Denmark in the systems stored in violation of section 6(1) of the DDIS Act must be expected to increase as a significant amount of information will reach the 15-year time limit for deletion every year. DDIS should therefore consider how it will ensure compliance with section 6(1) of the DDIS Act in the future when an increasing number of its systems will contain information older than 15 years and when the total amount of information older than 15 years increases.

Based on TET's reviews, DDIS stated that, as a result of the compliance reviews in 2022 and 2023, DDIS has initiated work on updating internal processes for deletion of information to ensure timely deletion across its systems. DDIS expects these processes to be finalised in 2024 (section 3.2.6).

- ▶ TET decided to cancel three planned reviews of DDIS' drive structures in 2023, as a solution for searching the contents of the drive structures was still not in place.

In TET's assessment, DDIS had in 2023 taken any possible steps to promote the establishment of the solution that were possible for DDIS and that the delay was due to challenges with external deliverables (section 3.2.8).

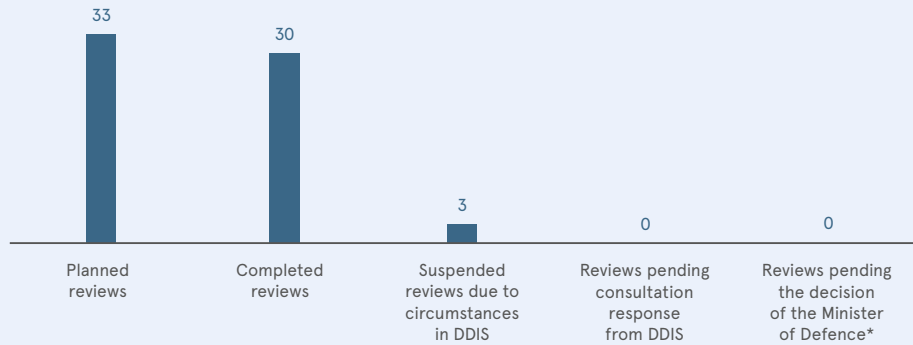
- ▶ TET found that DDIS was unable to provide the requested information for systems and databases central to DDIS' processing of raw data, as in DDIS' assessment TET's request would currently draw on more resources than the relevant departments had available.

In TET's assessment, it was not expedient in relation to TET's organisation of its review of DDIS that DDIS was not able to provide the requested information, as the information is necessary for TET to make an informed assessment of which parts of DDIS' systems should be subject to external review (section 3.2.13).

- ▶ In 2023, TET processed requests from 22 natural or legal persons to review if DDIS was processing information about them in violation of DDIS legislation. In that connection, TET found that in one case DDIS had processed information about the persons in question in violation of the conditions of processing in section 4(1) or 5(1) of the DDIS Act, as DDIS no longer found it necessary to process the information. On that basis, DDIS has deleted the information. In this connection, it should be noted that DDIS 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).

In addition, in 2023, TET and DDIS discussed the interpretation of the concept of raw data in the DDIS Act in relation to a number of specific reviews. The discussions have centred on two separate issues relating to the concept of raw data in the situation where the content of the data in question has been procured from sources that must be considered open sources within the meaning of the DDIS Act, for example information made available on the internet. The discussions have shown that TET and DDIS disagree on the interpretation of the DDIS Act in two areas. At the request of TET, DDIS has therefore submitted the interpretation issues to the Minister of Defence for a decision. On 20 February 2024, the Minister of Defence decided that DDIS must follow TET’s interpretation on one of the issues, while the other interpretation issue is still awaiting the Minister’s decision (section 3.6).

TET’s review of DDIS in 2023



*But see section 3.6

Results of TET’s review of DDIS 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 DDIS in 2023

For the purpose of reviewing DDIS' compliance with the provisions of the DDIS Act when processing information about natural and legal persons, TET carried out reviews in 2023 of DDIS'

- ▶ targeted intelligence obtaining (SIGINT) (section 3.2.1),
- ▶ handling of raw data (section 3.2.2),
- ▶ raw data searches (section 3.2.3),
- ▶ open source intelligence obtaining (OSINT) (section 3.2.4),
- ▶ electronic non-communications intelligence obtaining (ELINT) (section 3.2.5),
- ▶ deletion of information (section 3.2.6),
- ▶ network operations (CNO) (section 3.2.7),
- ▶ processing of information on drives (section 3.2.8),
- ▶ disclosure and processing of information in communication systems (section 3.2.9),
- ▶ other processing of information (section 3.2.10), and
- ▶ internal compliance review (3.2.11).

Furthermore, in 2023, TET completed

- ▶ follow-up on its reviews of DDIS in 2022 (section 3.2.12), and
- ▶ technical reviews and mapping of DDIS' IT landscape (section 3.2.13).

3.2.1

Review of DDIS' targeted intelligence obtaining (SIGINT)

DDIS uses Signals Intelligence (SIGINT) for targeted intelligence obtaining based on a number of different selectors, e.g. telephone numbers and email addresses.

The SIGINT activities are carried out at permanent intelligence obtaining facilities as well as at temporary facilities set up abroad. SIGINT requires extensive and technically complex IT systems to process the obtained material, which is due to the fact that the volume of communication is increasing at a tremendous rate, while new technologies are constantly being developed.

DDIS' compliance with intelligence obtaining legislation means in relation to electronic intelligence obtaining directed at a person resident in Denmark that such obtaining must be based on a court order obtained by DDIS, see section 3(3) of the DDIS Act, or at the request of DSIS based on a court order obtained by DSIS. In these situations, the intelligence obtaining must always take place within the framework set by the court order.

Intelligence obtaining under section 3(3) of the DDIS Act is conditional on the person who is the target of intelligence obtaining being physically located in Denmark and on the existence of specific reasons to believe that the person is engaging in activities that may involve or increase a threat of terrorism against Denmark and Danish interests.

In 2023, TET performed regular reviews of DDIS' targeted intelligence obtaining directed at Danish-related selectors.

Comments by TET

TET's review of DDIS' targeted intelligence obtaining in 2023 did not give rise to any comments.

3.2.2

Reviews of DDIS' handling of raw data

Through electronic intelligence obtaining, DDIS procures very large amounts of non-processed data (raw data). Raw data is characterised by the fact that until the data is subjected to processing, it is not possible to determine what information is contained therein.

As a general rule, raw data procured by DDIS must be deleted no later than 15 years after the time of obtaining, see section 6(2) of the DDIS Act. The processing rules under the DDIS Act do not otherwise apply to raw data until the data has been processed and can no longer be categorised as raw data.

In addition, DDIS has the possibility of extracting information from raw data by searching it, for example for information regarding specific selectors, e.g. telephone numbers and email addresses.

It is crucial that while raw data is being obtained as well as afterwards that it is being handled in a way that ensures the integrity of the information contained therein, including in particular the correct time stamping of raw data. Correct time stamping of raw data means that DDIS may search or delete raw data in accordance with section 3(3) of the DDIS Act, see section 3a(3) and section 6(2) of the DDIS Act, respectively.

In 2023, TET performed reviews of one of DDIS' raw data storage system.

What is the importance of time stamping raw data?

When DDIS obtains raw data, this data will typically include a time stamp indicating when the raw data in question was obtained.

Time stamping of raw data is important for how DDIS can ensure that it complies with the rules of the DDIS Act for searching raw data and deleting raw data.

THE IMPORTANCE OF TIME STAMPING WHEN SEARCHING RAW DATA

DDIS' activities are aimed at matters abroad, and therefore, as a general rule, no searches are made in raw data directed at persons resident in Denmark.

When DDIS in certain cases nevertheless searches raw data directed at persons resident in Denmark, such searches will always be based on a court order obtained by DDIS or DSIS. The court orders will often contain a specific time frame within which the measure must be carried out.

In order to comply with the content of the court orders, DDIS will set a time limit on the searches made on the basis of the court order.

However, if there are errors in the time stamping of the raw data being searched, there is a risk that the search will show data that in reality relates to a different period than the one DDIS is entitled to search according to the court order.

THE IMPORTANCE OF TIME STAMPING WHEN DELETING RAW DATA

The time stamp will naturally form the starting point for the assessment of when raw data must be deleted under section 6(2) of the DDIS Act. However, if raw data does not have a reliable time stamp, this may give rise to doubt as to how long the raw data in question may be stored.

However, depending on the circumstances, it may also in other ways be possible to verify that DDIS complies with the time limit for deletion of raw data.

Comments by TET

TET's review of DDIS' handling of raw data in 2023 did not give rise to any comments.

3.2.3

Review of DDIS' raw data searches

DDIS procures very large amounts of unprocessed data (raw data) through electronic obtaining. Raw data is characterised by the fact that, until the data is subjected to processing, it is not possible to determine what information is contained therein. Part of DDIS' processing is done by searching for specific information contained in the raw data.

DDIS is not allowed to search raw data of its own motion if the result may be expected to be mainly information about identifiable persons resident in Denmark, unless the search is based on a court order obtained by DDIS, see section 3(3) of the DDIS Act. In addition, DDIS is allowed to make such searches at the request of DSIS, where such requests are based on a court order obtained by DSIS. In these situations, the raw data search must always take place within the framework set by the court order. By way of example, raw data searches based on court orders relating solely to a specific period must be limited in time to that specific period.

If DDIS searches raw data of its own motion where the result is likely to mainly be information about identifiable persons resident in Denmark, without DDIS having a lawful basis for the search, the search in question will be in violation of DDIS legislation. Reasons for raw data searches being in violation of DDIS legislation may include the failure to time limit searches according to court orders, the failure to sort out Danish-related selectors (e.g. telephone numbers) before performing an overall search on a wide range of selectors, typing errors or searches on selectors, which were no longer used by a target person.

According to DDIS' estimate, DDIS has performed about 700,000 raw data searches in 2023 of which 303 searches targeting persons resident in Denmark were identified in connection with DDIS' internal compliance review. Of the 303 searches, it is DDIS' assessment that it in 25 cases (8 percent) has performed raw data searches in violation of DDIS legislation.

In 2023, TET performed regular reviews of DDIS' raw data searching.

Based on logs from DDIS' systems used for raw data searches, TET initially subjected DDIS' raw data searches to computer filtration for the purpose of isolating the searches that

may be related to Denmark and then sort out false positives (raw data searches which in a computer filtering process came up as Danish-related but which on examination turn out not to be). Computer filtration is necessary because, as mentioned, the Danish-related searches only represent a relatively small part of the total number of raw data searches performed by DDIS.

Of the identified Danish-related searches performed by DDIS, TET performed regular reviews and, based on a specific assessment, requested DDIS' clarifying comments.

In addition, in 2023, TET carried out a targeted review of DDIS's raw data searches based on a DSIS request.

Comments by TET

TET's review of DDIS' raw data searches gave rise to the following comments:

- ▶ TET found that in two of the 39 cases reviewed (5 percent), DDIS had performed raw data searches in violation of DDIS legislation because DDIS had not performed such data searches on behalf of DSIS within the framework of a court order obtained by DSIS or because DDIS itself had not obtained a court order for such searches, see section 3(3) of the DDIS Act. The searches were performed in 2022 and 2023, respectively.
- ▶ TET found that, based on 1 out of 6 reviewed requests from DSIS, DDIS had performed raw data searches in violation of DDIS legislation in seven cases, as the searches were not time-limited in accordance with the court order obtained by DSIS. The searches were performed in 2022.

In all cases, the searches in violation of DDIS legislation had also been identified by DDIS in its internal control.

3.2.4

Review of DDIS' collection of open source intelligence (OSINT)

DDIS' collection of intelligence via open sources – also referred to as Open Source Intelligence (OSINT) – includes advanced and systematic collection of information from the internet, for example communication in open online forums, as well as print media, television etc.

DDIS may collect information from open sources when the information may be of importance to DDIS' intelligence activities aimed at foreign affairs or when the information is necessary for DDIS' other activities. Collection differs from electronic obtaining in that DDIS may, on its own initiative, carry out targeted collection of information against persons resident in Denmark, provided that the above requirements are met.

In 2023, TET carried out a review of one of DDIS' systems for collection of open source intelligence.

Comments by TET

TET's review of DDIS's collection of intelligence from open sources in 2023 did not give rise to any comments.

As part of DDIS' electronic obtaining (SIGINT), DDIS conducts non-communications intelligence obtaining, such as radar signals – also known as Electronic Intelligence (ELINT).

In relation to ELINT, DDIS' compliance with the rules on intelligence obtaining means that information relating to persons resident in Denmark may generally only come into DDIS' possession by chance unless the person falls within the scope of section 3(3) of the DDIS Act.

In 2023, TET reviewed one of DDIS' systems used for ELINT.

Comments by TET

TET's review of DDIS' use of ELINT in 2023 did not give rise to any comments.

According to section 6(1) of the DDIS Act, DDIS must delete information about persons resident in Denmark procured as part of its intelligence-related activities when no new information has been procured within the past 15 years which in substance relates to the same case.

A complex rule of deletion

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

“Unless otherwise provided by law or statutory regulation, the Danish Defence Intelligence Service must delete information about natural and legal persons resident in Denmark procured as part of the activities of the Danish Defence Intelligence Service pursuant to section 1(1) when no new information has been procured within the past 15 years relating to the same case.”

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

- 1) whether the information has been procured as part of DDIS' activities under section 1(1) of the DDIS Act,
- 2) whether the person in question is currently resident in Denmark, and
- 3) whether new information has subsequently been procured which in substance relates to the same case.

In relation to the first criterion, information procured before the DDIS Act came into force on 1 January 2014 will not necessarily be identifiable as having been procured as part of DDIS' activities under section 1(1) of the DDIS Act, as DDIS was not required to make such identification before its entry into force, which is why DDIS' systems do not necessarily support a marking or categorisation of procured information.

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

In relation to the third criterion, DDIS processes information across many different systems, and the analytical and technical complexity of the work rarely makes it meaningful to divide the work into cases as it is known from other administrative authorities. It is therefore difficult to determine whether new information relates to an existing case, as DDIS does not generally work with cases in the classic sense.

The practical challenges which, in TET's opinion, are associated with compliance with the time limit for deletion in section 6(1) of the DDIS Act can partly be met by DDIS by, to the greatest extent possible, providing system support for handling compliance with the provision, including by ensuring relevant metadata on DDIS' information and a centrally managed audit across DDIS' IT infrastructure.

In 2023, TET reviewed DDIS' compliance with section 6(1) of the DDIS Act by reviewing DDIS'

- ▶ processing of data in an analytics system,
- ▶ processing of data in a system for handling external communications,
- ▶ processing of data in an internal email system, and
- ▶ processing of data generated by a specific operation.

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

In relation to the above reviews, the information covered by TET's reviews could in DDIS' assessment be deleted as it was all older than 15 years, see section 6(1) of the DDIS Act, and as the information was not necessary to safeguard important interests with regard to the performance of DDIS' intelligence-related activities, see section 6(3) of the DDIS Act.

As regards TET's review of a specific operation, it could not be assessed on the basis of the review carried out by TET whether the randomly sampled files contained information about persons resident in Denmark. DDIS was therefore requested to comment on this in a consultation. However, DDIS did not perform an assessment of whether the files contained information about persons resident in Denmark, but deleted them with reference to section 6(1) of the DDIS Act.

Comments by TET

TET's review of DDIS' deletion of information in 2023 gave rise to the following comments:

- ▶ TET found it criticisable that DDIS processed 8 out of 30 randomly sampled files in an analytics system in violation of section 6(1) of the DDIS Act as the files were older than 15 years and as DDIS was not aware of whether new information relating to the same case had been procured within the past 15 years.

DDIS had stated that it had not reviewed the files individually for resource reasons, as the files were all older than 15 years and could still be deleted in DDIS' opinion.

Furthermore, TET found that the sample error rate of 27 percent was very likely to apply to the remaining 324 files that made up the population of TET's sample, which

is why TET recommended that DDIS either delete the files or assess whether it can still legally process the files in accordance with section 6 of the DDIS Act.

- ▶ TET found it criticisable that DDIS processed 7 out of 15 randomly sampled files in a system for handling external communication in violation of section 6(1) of the DDIS Act as the files were older than 15 years and as DDIS was not aware of whether new information relating to the same case had been procured within the past 15 years.

DDIS had stated that, for resource reasons, it had not assessed this specifically, as the files in question were older than 15 years and could still be deleted in DDIS' opinion.

Furthermore, TET found that the sample error rate of 47 percent was very likely to apply to the remaining 116 files that made up the population of TET's sample, which is why TET recommended that DDIS delete the files or assess whether it can still legally process the files in accordance with section 6 of the DDIS Act.

- ▶ TET found it criticisable that DDIS processed 11 out of 30 randomly sampled emails in an internal email system in violation of section 6(1) of the DDIS Act as the emails were older than 15 years and as DDIS was not aware of whether new information relating to the same case had been procured within the past 15 years.

DDIS had stated that, for resource reasons, it had not assessed this specifically, as the emails in question were older than 15 years and could still be deleted in DDIS' opinion.

Furthermore, TET found that the sample error rate of 37 percent would most likely apply to the remaining 1,089 emails that made up the population of TET's sample, which is why TET recommended that DDIS delete the emails in question or assess whether DDIS can still legally process the files in accordance with section 6 of the DDIS Act.

- ▶ TET assessed that, considering the total amount of files stored in DDIS' system for handling external communication and internal email system, there would be a significant amount of information about persons resident in Denmark that would be processed in violation of the time limit for deletion in section 6(1) of the DDIS Act.

TET's assessment is based on the fact that TET's reviews of the systems in both 2022 and 2023 showed that information was stored in violation of the time limit for deletion in section 6(1) of the DDIS Act and that DDIS does not currently perform internal legal compliance reviews or own reviews to ensure that information stored in the systems is deleted in accordance with section 6 of the DDIS Act.

In continuation thereof, TET noted that the amount of information about persons resident in Denmark in the systems in question stored in violation of section 6(1) of the DDIS Act must be expected to increase, as a significant amount of information will reach the time limit for deletion of 15 years every year.

- ▶ TET recommended that DDIS as soon as possible implement measures to ensure that information about persons resident in Denmark stored in the system for handling external communication and in the internal email system is deleted in accordance with section 6 of the DDIS Act.

- ▶ Based on the review of DDIS' deletion of information in 2023, TET learned that DDIS generally has difficulties complying with the rules on deletion under section 6(1) of the DDIS Act in systems where personal information older than 15 years is stored.

DDIS should consider how it will ensure compliance with section 6(1) of the DDIS Act in the future when an increasing number of its systems will contain information older than 15 years and when the total amount of information older than 15 years increases.

- ▶ Based on TET's reviews, DDIS stated that, as a result of TET's reviews in 2022 and 2023, DDIS has initiated work on updating internal processes for deletion of information to ensure timely deletion across its systems. DDIS expects these internal processes to be finalised in 2024.
- ▶ TET found that there was no basis for criticising DDIS for storing 77 files procured in a specific operation which were older than 15 years, as TET could not conclude from the reviews carried out that the files contained information about persons resident in Denmark.

DDIS had stated that it had not reviewed the 77 files individually for resource reasons, as the files were all older than 15 years and could still be deleted in DDIS' opinion.

TET found it problematic that DDIS had not considered whether the 77 files contained information about persons resident in Denmark, despite the fact that TET had explicitly requested DDIS to do so.

3.2.7

Reviews concerning DDIS' computer network operations (CNO)

DDIS' network intelligence obtaining – also known as Computer Network Exploitation (CNE) – is active electronic intelligence obtaining against computer networks, typically requiring a DDIS employee to gain access to closed internet forums, IT systems and computers.

In addition, DDIS supports the Danish military with offensive military cyber operations – also known as cyber-attacks or Computer Network Attacks (CNA) – where the purpose may be to attack an adversary's digital infrastructure.

TET does not perform reviews of DDIS's offensive military cyber operations, as the operations are carried out under the provisions of the Defence Act. However, TET may perform reviews of the processing of information about persons resident in Denmark and the handling of raw data that may be carried out by DDIS prior to or after the operation.

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

In 2023, TET carried out compliance reviews of a system used by DDIS in connection with DDIS' CNO.

Comments by TET

TET's review of DDIS' use of CNO in 2023 did not give rise to any comments.

DDIS uses drives to store information in connection with many different parts of its activities.

In 2023, TET planned to carry out compliance reviews with respect to three different drive structures in DDIS.

Comments by TET

TET decided to cancel three planned reviews of DDIS' drive structures in 2023, as a solution enabling searches in the content of the drive structures had still not been established.

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

DDIS is involved in bilateral and multilateral partnerships with foreign intelligence services for the purpose of sharing intelligence information. Information about obtaining methods, technologies, capacities and specific intelligence is exchanged for the purpose of DDIS ultimately receiving information from the partners which to a wide extent forms part of DDIS' analysis and, thereby, of a significant part of the products which DDIS prepares.

DDIS also discloses information to national partners, such as DSIS and other authorities in the areas under the Ministry of Defence.

In connection with the disclosure, DDIS uses various communication systems, which often also include the possibility of processing data, such as storing copies of incoming and outgoing communications.

In 2023, TET performed reviews of four of DDIS' communication systems.

Comments by TET

TET's review of DDIS' disclosure and processing of information in communication systems in 2023 did not give rise to any comments.

DDIS processes, including stores, information about persons resident in Denmark in a large number of very different systems.

In 2023, TET performed a review of one of DDIS' systems used to process data.

Comments by TET

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

DDIS performs regular internal compliance review of its compliance with specific parts of the DDIS Act. For the organisation of its internal compliance review, DDIS each year prepares a risk analysis of its compliance with legal requirements and a plan for internal compliance reviews in the following year. DDIS must regularly inform TET of the organisation of its internal compliance reviews and their results, including by submitting its risk analysis and review plan.

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

In September 2023, DDIS informed TET about its

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

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

Comments by TET

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

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

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

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

Comments by TET

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

- ▶ TET found it criticisable that DDIS, in violation of section 6 a(1) of the DDIS Act, had by mistake not deleted 107 emails which DDIS had informed TET that it would based on TET's reviews in 2022.
- ▶ TET is still waiting to receive information from DDIS that five measures which DDIS had informed TET would be implemented in connection with TET's review in 2022 have been implemented.

DDIS' 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 DDIS' IT landscape and works continuously to ensure up-to-date knowledge of DDIS' systems.

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

In 2023, TET performed verification reviews of DDIS' IT infrastructure by

- ▶ reviewing two DDIS networks,
- ▶ mapping DDIS' server infrastructure, and
- ▶ mapping DDIS' databases for storing raw data.

Comments by TET

TET's mapping of databases for storing raw data gave rise to the following comments:

- ▶ TET found that DDIS was not able to provide the requested information for key systems and databases for DDIS' processing of raw data as in DDIS' assessment TET's enquiry would currently draw on more resources than the relevant departments had available.

In TET's assessment, it was not expedient in relation to TET's organisation of its review of DDIS that DDIS was not able to provide the requested information, as the information is necessary for TET to make an informed assessment of which parts of DDIS' systems should be subject to external review.

TET's reviews of networks and mapping of DDIS' server infrastructure in 2023 did not give rise to any comments.

3.3

DDIS' briefing of TET

According to the explanatory notes to the DDIS Bill, DDIS must keep TET informed of its exercise of powers under a number of provisions of the Act. More specifically, DDIS must thus inform TET of the following matters:

- ▶ DDIS' decisions under section 6(3) of the DDIS Act not to delete information which has reached the time limit for deletion of 15 years under subsections (1) and (2),
- ▶ all important issues concerning DDIS' processing of information about natural and legal persons resident in Denmark, and
- ▶ new administrative guidelines issued in pursuance of section 1(5), section 4(3) and section 5(3) of the Act.

In 2023, DDIS kept TET regularly informed about the following:

- ▶ Important issues regarding DDIS' processing of information about natural and legal persons resident in Denmark

3.4 Subject access requests under sections 9 and 10 of the DDIS Act

3.4.1 Processing of requests by TET

When a natural or legal person resident in Denmark requests TET to review if DDIS is processing information about them in violation of DDIS legislation, TET will examine the matter at DDIS' 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 DDIS, but TET will endeavour to identify all information, which DDIS 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, DDIS is processing information about the data subject in violation of DDIS legislation. If TET concludes that this is the case, TET will order DDIS to delete the information. When TET has verified that DDIS is no longer processing information about the data subject in violation of DDIS legislation, TET will send a reply to the data subject's request.

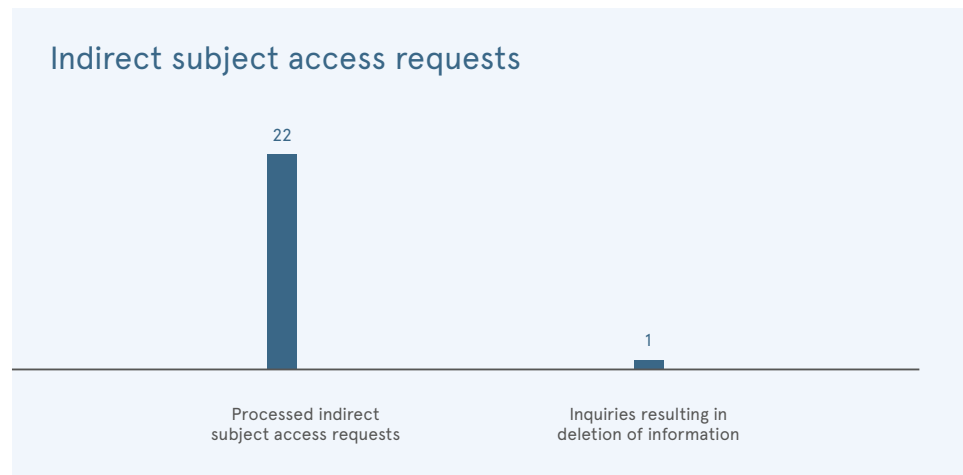
If special circumstances weigh in favour of doing so, TET may order DDIS to inform a natural or legal person of the information which DDIS is processing about them or inform them whether DDIS is processing information about them. Where TET receives a subject access request, TET will find out which information, if any, DDIS is processing about the data subject and will obtain DDIS' 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 DDIS 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 22 natural or legal persons, asking TET to review if DDIS was processing information about them in violation of DDIS legislation. In that connection, TET found that in one case DDIS had processed information which no longer met the conditions of processing in section 4(1) or 5(1) of the DDIS Act as DDIS no longer found it necessary to process the information. DDIS has on that basis deleted the information. In this connection, it should be noted that DDIS 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 97 days, 20 days of which were DDIS' processing time. Compared with 2022, the average processing time decreased by 102 days.

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



It should be noted that in order for TET to perform its duties in connection with the indirect subject access request system, information about natural and legal persons resident in Denmark must be stored in IT systems facilitating efficient consultations.

TET prepares a separate risk assessment and analysis specifically for its activities in relation to DDIS 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 key DDIS systems. However, in TET's assessment, the reviews should include one additional system which is not currently covered as it is not technically possible to search it, which affects the completeness of TET's reviews.

3.5

DDIS' processing times in 2023

In 2023, TET submitted 16 consultations to DDIS in connection with its review activities. DDIS responded to 14 of TET's consultation questions within the specified deadline and two after the specified deadline. DDIS' average delay in responding to consultation questions after the stated deadline was five working days.

3.6

Cases submitted to the Minister of Defence for decision

As part of its review of DDIS, TET may issue statements to DDIS in which TET may, among other things, express its opinion on whether DDIS complies with the rules of the DDIS Act. At the end of each compliance review, TET issues a statement to DDIS describing the results of the review. The statement may also contain a description of one or more measures which DDIS should take in TET's opinion. If DDIS decides not to comply with a recommendation issued by TET in exceptional cases, DDIS must notify TET and without undue delay submit the matter to the Minister of Defence for a decision. If the Minister of Defence decides not to comply with the recommendation from TET in exceptional cases, the Government must notify the Parliamentary Intelligence Services Committee. The responses available to TET towards DDIS are described in more detail in section 2.3 of the Appendix and in section 16 of the DDIS Act.

On two occasions in 2023, DDIS submitted questions about the interpretation of the DDIS Act to the Minister of Defence, as there was disagreement between DDIS and TET about the interpretation of the legislation. On 20 February 2024, the Ministry of Defence decided one of the questions:

Status of news articles

In 2023, TET and DDIS discussed the interpretation of the concept of raw data in the DDIS Act in relation to a number of specific reviews.

The discussions have shown that TET and DDIS disagreed on whether news articles collected by DDIS without prior review of the content of the news article should be considered raw data until such time as a DDIS employee may conduct a more detailed review.

On this basis, on 3 October 2023, TET requested DDIS to submit the questions of interpretation to the Minister of Defence for a decision. On 23 October 2023, DDIS submitted the relevant questions to the Minister.

The immediate consequence of news articles being considered raw data would be that DDIS would not be obliged to comply with the processing rules in sections 4 and 5 of the DDIS Act in relation to the storage of news articles and that the content of news articles would no longer be covered by TET's reviews under section 10 of the DDIS Act.

On 20 February 2024, the Minister of Defence ruled on the interpretation question regarding the status of news articles as raw data. The Minister of Defence found, in accordance with TET's interpretation, that unread news articles received via news subscriptions cannot be categorised as raw data within the meaning of the DDIS Act.

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

QUESTION	DATE OF SUBMISSION	STATUS
<p>Whether news articles collected by DDIS without prior review of the content of the news article should be considered raw data.</p> <p>Discussed in more detail in this annual report (section 4).</p>	23 October 2023	<p>Decided on 20 February 2024.</p> <p>The Minister of Defence found that unread news articles received via news subscriptions cannot be categorised as raw data within the meaning of the DDIS Act.</p>
<p>Whether DDIS, in connection with its compliance with section 3 of the DDIS Executive Order on Security Measures, is obliged to assess for each of its systems which measures can provide an adequate level of security.</p> <p>Discussed in more detail in TET's annual report for 2022 (section 2.2.9).</p>	4 August 2023	Awaiting the decision of the Minister of Defence.
<p>Whether, when interpreting section 3 of the DDIS Executive Order on Security Measures, TET can use the ISO 27001 standard, which has been chosen as the state security standard, to fulfil the overall obligations for DDIS in relation to security of processing set out in the Executive Order.</p> <p>Discussed in more detail in TET's annual report for 2021 (section 1.2.8).</p>	2 May 2022	Awaiting the decision of the Minister of Defence.
<p>Whether TET's area of competence under section 15 of the DDIS Act includes DDIS' obtaining and disclosure of raw data, and whether the rules of the DDIS Executive Order on Security Measures apply to raw data.</p> <p>Based on the DDIS Commission's report, TET independently requested the Minister of Defence to take a position on the interpretation of the DDIS Act. Therefore, the submission was not made pursuant to section 16 of the DDIS Act.</p> <p>Discussed in more detail in TET's annual report for 2022 (section 3).</p>	2 February 2022	<p>Decided on 16 January 2023.</p> <p>The Minister of Defence found</p> <ul style="list-style-type: none"> ▶ that TET is not required to review that DDIS' obtaining and disclosure of raw data complies with the requirements of the DDIS Act, and ▶ that DDIS is not obliged to secure raw data in accordance with the DDIS Executive Order on Security Measures, as the Executive Order does not apply to raw data.

Appendix

1. ABOUT DANISH DEFENCE INTELLIGENCE SERVICE (DDIS)

Danish Defence Intelligence Service (DDIS) is tasked with the main responsibility of acting as:

- ▶ Denmark's foreign and military intelligence service,
- ▶ Denmark's military security service, and
- ▶ national IT security authority.

DDIS' intelligence-related activities are directed at conditions abroad, and in that connection DDIS is charged with the responsibility of collecting, obtaining, processing, analysing and communicating intelligence concerning conditions abroad which is of importance to the security of Denmark and Danish interests for the purpose of providing an intelligence-based framework for Danish foreign and defence policy and contributing to preventing and countering threats against Denmark and Danish interests.

In the context of DDIS' work as foreign and military intelligence service, the term Danish interests should be interpreted broadly and may include political, military and economic areas as well as technical-scientific information of significance to national security, the national economy, etc.

DDIS is an all source intelligence service, which means that it engages in all types of intelligence obtaining. At the overall level, this includes the following intelligence obtaining disciplines:

- ▶ Signals Intelligence (SIGINT): Electronic obtaining of different types of signals, including data transfers between computer networks, telecommunications, etc. The SIGINT activities are carried out at permanent intelligence obtaining facilities in Denmark or facilities abroad.
- ▶ Computer Network Exploitation (CNE): Electronic intelligence obtaining from computer networks. The CNE activities typically require DDIS to obtain access to closed internet forums, IT systems and computers, which requires considerable IT-technical insight.
- ▶ Human Intelligence (HUMINT): Physical intelligence obtaining from human sources. The HUMINT activities are carried out by a DDIS employee, also known as a handling officer, who collects or obtains intelligence from other persons, which is typically done by persuading the source to disclose information, which he or she was not supposed to disclose.
- ▶ Imagery Intelligence (IMINT): Intelligence based on images obtained from different sensors.
- ▶ Open Source Intelligence (OSINT): Sophisticated and systematic collection of intelligence from open sources, typically publicly available information from the internet etc.

DDIS' role as military security service is to protect the Danish military against espionage,

sabotage, terrorism and other crime. This protection includes, among other things, employees, equipment and buildings in Denmark and abroad. As military security service, DDIS also acts as the national security authority in the areas under the Ministry of Defence.

DDIS is also tasked with providing a military Computer Network Operations (CNO) capability to the Danish military. In the context of the CNO capability, DDIS supports the Danish military by providing intelligence on an adversary or by attacking the adversary's digital infrastructure. A decision to use the CNO capability offensively is made in the same way as decisions to deploy other military force, including with the involvement of the Danish Parliament.

The legal framework for DDIS' activities is essentially laid down in the DDIS with the related executive order and the PNR Act. The DDIS Act governs, among other things, DDIS' responsibilities and the procurement, internal processing and disclosure of personal information.

DDIS is also subject to external supervision by the National Audit Office, the courts, the Parliamentary Ombudsman and the Parliamentary Intelligence Services Committee.

DDIS' role as the national IT security authority falls outside the scope of the DDIS Act. Instead, the role is governed by Act No. 713 of 25 June 2014 on the Centre for Cyber Security, as amended (the CFCS Act), which entered into force on 1 July 2014. Under this Act, TET must also review that the processing of the Danish Centre for Cyber Security (CFCS) of personal information is in compliance with DDIS legislation, and submit an annual report in this regard to the Minister of Defence.

CFCS, which is a part of DDIS, is the national IT security authority and the national centre of competence within the area of cyber security. The role of CFCS is to contribute to protecting the digital infrastructure in Denmark and strengthening Danish cyber resilience. In this role, CFCS has a particular focus on countering advanced cyber-attacks against Danish public authorities and private businesses performing nationally important functions.

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.

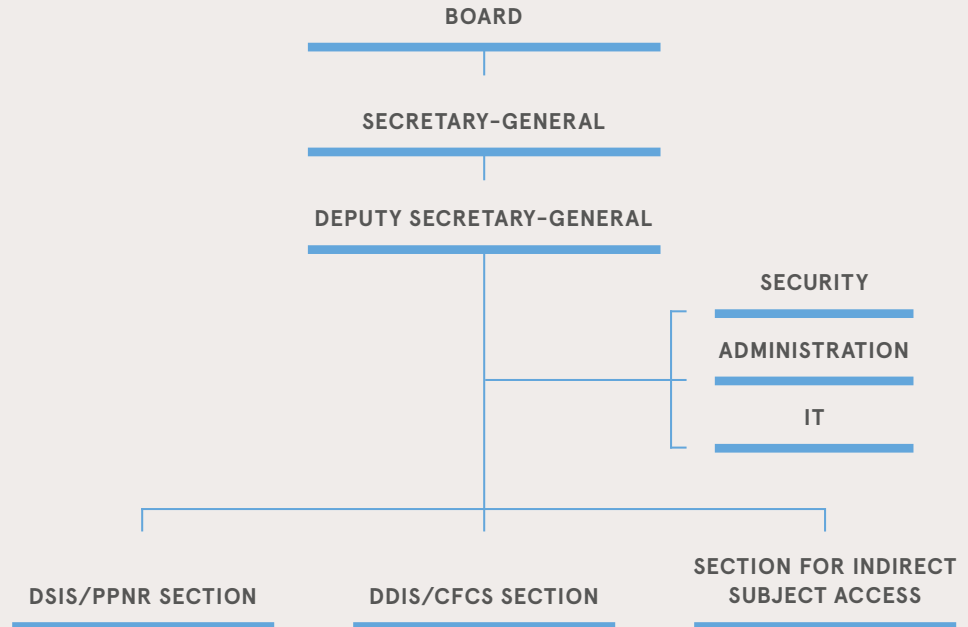
TET had the following members as at the end of 2023:

- ▶ 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 DDIS

The DDIS Act provides that upon receipt of a complaint or of its own motion, TET must review DDIS compliance with the relevant provisions of the DDIS Act and statutory regulations issued thereunder in its processing of information about natural and legal persons resident in Denmark – meaning persons with a qualified connection to Denmark. TET reviews DDIS' 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 DSIS 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 DDIS.

TET must review by way of compliance reviews that DDIS processes information about natural and legal persons resident in Denmark in compliance with DDIS legislation, and TET thus has no mandate to review whether DDIS carries out its activities in an appropriate manner, including how DDIS' resources are prioritised, as these aspects are to be determined by DDIS itself based on an intelligence 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 3-5 inspections of DDIS each year in the course of its compliance reviews.

At the request of a natural or legal person resident in Denmark, TET will also investigate whether DDIS is processing information about the data subject in violation of DDIS 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 DDIS 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 DDIS legislation or whether information is being processed in compliance with DDIS legislation.

2.2

TET's access to information held by DDIS

TET may require DDIS 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 DDIS to provide written statements on factual and legal matters of importance to TET's review activities and request the presence of a DDIS representative to give an account of current processing activities.

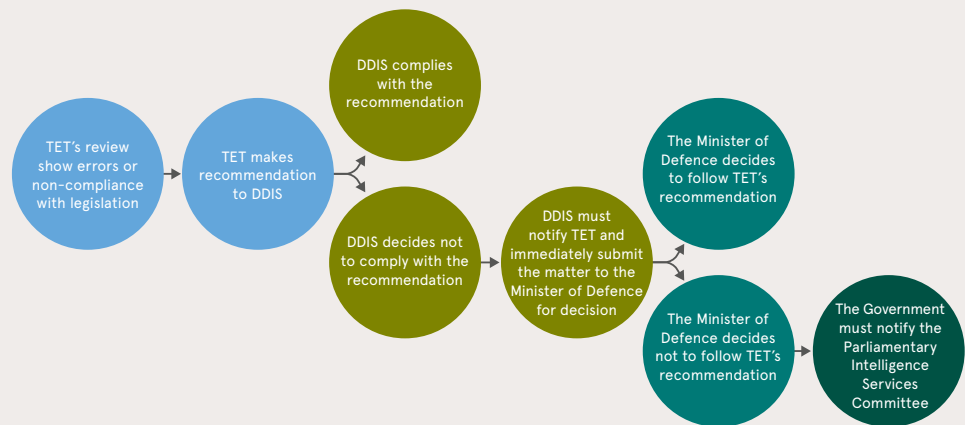
DDIS has made office premises available to TET for TET to make its own searches in DDIS' IT systems.

2.3

Responses available to TET

TET generally has no authority to order DDIS to implement specific measures in relation to data processing. However, TET may issue statements to DDIS providing its opinion on matters such as whether DDIS' complies with the rules concerning processing of infor-

mation. At the end of each review, TET issues a statement to DDIS describing the results of the review. The statement may also contain a description of one or more measures, which DDIS should take in TET's opinion. If DDIS decides not to comply with a recommendation issued by TET in exceptional cases, DDIS must notify TET and without undue delay submit the matter to the Minister of Defence for a decision. If the Minister of Defence decides not to comply with the recommendation of TET, the Government must notify the Parliamentary Intelligence Services Committee.



TET must inform the Minister of Defence 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 resident in Denmark, to investigate whether DDIS is processing information about that person in violation of DDIS legislation, TET may order DDIS to delete any information which, in the opinion of TET, is being processed by DDIS in violation of DDIS legislation.

Each year, TET submits a report on its activities to the Minister of Defence. The report, which is available to the public, provides general information about the nature of the review activities performed with regard to DDIS. 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 DDIS, 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 personal information has been found to be processed by DDIS in violation of DDIS legislation, including the number of instances where TET has ordered DDIS to delete information under the indirect subject access request system.

TET submitted its most recent annual report on its activities to the Minister of Defence 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 Defence Intelligence Service (DDIS) Act (Consolidated Act No. 1287 of 28 November 2017, as amended (most recently by Act No. 1706 of 27 December 2018) (the DDIS Act).
- 2) Executive Order on security measures to protect personal information being processed by the Danish Defence Intelligence Service (DDIS) (Executive Order No. 1028 of 11 July 2018) (the DDIS Executive Order on Security Measures).
- 3) 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).
- 4) 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 DDIS Act

Under section 3(1) of the DDIS Act, DDIS is authorised to collect and obtain information which may be of importance to the performance of its intelligence-related activities and DDIS is entitled in those activities directed at conditions abroad to include information on natural and legal persons resident in Denmark and persons currently staying in Denmark. As far as its other activities are concerned, DDIS may collect and obtain information, which is necessary for the performance of its activities, see section 3(4) of the Act. The most important purpose of this provision is to emphasise that in its intelligence-related activities directed at conditions abroad DDIS is entitled to collect and obtain data, including raw data, among other things through electronic and physical obtaining, so long as those data are deemed at the time of collection and obtaining to be of potential importance to DDIS' intelligence-related activities. The obtaining of information must be based on legitimate reasons, which in relation to raw data obtaining means that a general criterion of legitimacy is applied.

According to the explanatory notes to the DDIS Bill concerning this provision, DDIS is only allowed to include in its electronic obtaining activities so-called chance findings about persons resident in Denmark, while in connection with its physical obtaining activities DDIS may procure such information without it being in the nature of chance findings. However, DDIS is not allowed of its own motion to actively initiate physical obtaining against an already known and identified person who is resident in Denmark, but currently staying abroad. Such targeted intelligence obtaining is subject to a request from DSIS, unless the conditions in section 3(3) of the Act are satisfied.

Subsection (3) of the provision authorises DDIS to initiate targeted obtaining of intelligence about a natural person resident in Denmark if such person is not physically located in Denmark and there are specific reasons to believe that the person in question is engaging in activities that may involve or increase a threat of terrorism against Denmark and Danish interests. The provision departs from the general premise of the DDIS Act, which provides that information about persons resident in Denmark may be received by DDIS only by chance. If the intelligence obtaining activities involve interception of communications, DDIS must obtain a court order in this regard.

With regard to review of the provision, the legislative history of the DDIS Act specifies that the review in particular includes a review to verify that information in connection with electronic obtaining which concerns natural and legal persons resident in Denmark has been obtained by DDIS either by chance or at the request of DSIS, including, if necessary, by court order. This means in relation to the general relevance requirement applying to DDIS' obtaining of raw data that TET does not monitor this. The reason for this is that it is not yet possible at the time of obtaining of the raw data to determine whether it includes information about persons resident in Denmark.

The term *natural persons resident in Denmark* means Danish nationals, Nordic nationals and other foreign nationals with residence in Denmark if the person in question is registered with the National Register, as well as asylum seekers having their (known) residence in Denmark for more than six months, while *legal persons resident in Denmark* means parties, associations, organisations, businesses, etc. which due to the location of their head offices etc. predominantly have ties to this country.

According to the explanatory notes to the provision, it will not change the fundamental allocation of responsibilities and mode of cooperation between DSIS and DDIS. This means, among other things, that DDIS will share all information obtained under the provisions with DSIS. If a court order is available to DSIS based on the provisions of the Administration of Justice Act, those provisions will continue to form the basis of DDIS' targeted intelligence obtaining.

The DDIS Act does not apply to Greenland and the Faroe Islands, and any procurement and processing of information by DDIS on Greenlandic and Faroese territory therefore falls outside the scope of the provisions of the DDIS Act. TET is thus not competent to monitor this. This differs from the state of the law in relation to the DSIS Act, which is brought into force by Decree for both Greenland and the Faroe Islands, and the CFCS Act, which is brought into force by Degree for Greenland.

3.2 Internal processing of information

3.2.1 About internal processing of information, see sections 3e-5 of the DDIS Act

Under section 3e(1)-(7) of the DDIS Act, a number of general data protection principles apply to DDIS' processing of information collected and obtained about natural and legal persons resident in Denmark.

According to the explanatory notes to the DDIS Bill, the same general data protection principles etc. will generally apply to the determination of which fundamental conditions

must be satisfied by DDIS when processing personal information as those applying to other Danish authorities when processing personal information.

Under sections 4(1) and 5(1) of the Act, DDIS is allowed to process any information about natural and legal persons resident in Denmark if:

- 1) consent has been obtained from the data subject,
- 2) processing may be assumed to be of importance to the performance of DDIS' activities under section 1(1) (as intelligence service) and section 1(4) ("other activities" entrusted to DDIS), or
- 3) processing is necessary for the performance of DDIS' activities under section 1(2) (as military intelligence service).

In its electronic intelligence obtaining, DDIS obtains very large amounts of information which at the time of obtaining is made up of non-processed data. Such data are known as "raw data" and are characterised by the fact that until processed, including, if necessary, decryption and translation, it is not possible to determine what information may be retrieved from these data. Processing is thus a precondition to understanding the nature of the contents and determining if the information obtained is relevant to DDIS' intelligence-related and analytical work.

According to the legislative history of the DDIS Act, the provisions of the Act on processing and disclosure in principle apply to raw data, which contain personal information, but in the practical administration of the provisions regard must be had to the special nature of those raw data. This means that the provisions of the Act on internal processing and disclosure of information and about legal political activity may only be meaningfully applied to raw data when those data have been processed (so as to no longer be raw data). In the understanding of the principles of the former Data Protection Act on good processing practice and security of processing in relation to DDIS' obtaining and processing of raw data, regard must therefore be had to the special nature of those data. This means that for the requirement of legitimacy in the raw data obtaining in section 5(2) of the former Data Protection Act, which has been carried over in section 3e(2) of the DDIS Act, a general requirement of legitimacy must be applied with regard to the raw data obtaining, as such obtaining must be for legitimate reasons. In addition, the provision also means that the raw data obtained by DDIS must be used for the purposes for which they have been obtained, and may not be held longer than dictated by the purpose.

3.2.2

About deletion of information, see sections 6 and 6a of the DDIS Act

Under section 6 of the DDIS Act, unless otherwise prescribed by law or statutory regulation, DDIS must delete information about natural and legal persons resident in Denmark, which has been procured in the course of DDIS' intelligence-related activities where no new information has been procured within the last 15 years relating to the same case. However, deletion of such information will not be required if the information is necessary to safeguard important interests with regard to the performance of DDIS' intelligence-related activities. According to the explanatory notes to the Bill concerning this provision, which only covers information about natural and legal persons resident in Denmark, which has been procured in the course of DDIS' intelligence-related activities, the provision lays down an overall time limit for deletion of information held by DDIS.

It follows from the provision in section 6a(1) that when DDIS becomes aware in connection with its activities that cases or documents, etc. no longer meet the conditions of processing in section 4(1) and section 5(1), they must be deleted, regardless of whether the time limit for deletion of information in section 6(1) has expired, but that DDIS is not required beyond that to review its cases and documents, etc. on a regular basis 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 6a(1) that the term “activities” is to be understood in the broad sense as encompassing all the tasks that DDIS is engaged in. Thus, by way of example, in addition to operational activities, the term also includes DDIS’ tasks in connection with indirect subject access requests, see section 10 of the Act, and random reviews performed by TET.

It follows from the provision in section 6a(2) that notwithstanding the provisions of section 3e, sections 4-5 and section 6(1) and (3), DDIS is not required to delete information which does not meet the conditions of processing in sections 4(1) and 5(1) if the information forms part of documents etc. which otherwise meet the above-mentioned conditions of processing, but see section 10(2).

In the notes to the individual provisions of the Bill, it is specified with regard to section 6a(2) that the provision concerns deletion at data-level whereas the provision in subsection (1) concerns deletion at case- and document-level. DDIS is thus not required to delete information at data-level even if DDIS becomes aware in connection with its activities that a specific piece of information no longer meets the conditions of processing in sections 4(1) and 5(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. The proposed amendment further means 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 DDIS 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, DDIS will still be required to delete information if it is established that it has been procured in violation of section 3 of the Act.

In other parts of DDIS legislation, including in particular Danish archiving law, there are rules, which mean that DDIS is not allowed to delete information. Such rules must be observed by DDIS, which means that DDIS is precluded from deleting the information as section 6 of the DDIS Act prescribes that DDIS’ obligation to delete information does not apply if otherwise prescribed by law or statutory regulation.

3.2.3

About security of processing, see sections 2-5 of the DDIS Executive Order on Security Measures

According to section 4(2) and section 5(2) of the DDIS Act, the Minister of Defence may lay down more detailed rules on DDIS’ processing of information about natural and legal persons resident in Denmark. Executive Order No. 1028 of 11 July 2018 (Executive Order on security measures to protect personal information being processed by the Danish Defence Intelligence Service (DDIS)) (the DDIS 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 DDIS 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 4(2) and 5(2) of the DDIS 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 DDIS Executive Order on Security Measures is interpreted in accordance therewith.

Under section 2 of the DDIS Executive Order on Security Measures, individuals, companies, etc. performing work for DDIS or DDIS' data processors and having access to information may process this information only on instructions from DDIS, unless otherwise provided by law or statutory regulation. No particular formal requirements apply to those instructions, which may therefore – depending on the circumstances – be implied into a particular job title or follow from the fact that DDIS authorises an employee or others to access particular information. The requirement that the person etc. in question may only process information in accordance with DDIS' instructions means, among other things, that the person etc. may not process information for other purposes than those laid down by DDIS – including for own purposes – and that the person etc. in question may not process information on instructions from other parties than DDIS.

Under section 3 of the DDIS Executive Order on Security Measures, DDIS must implement appropriate technical and organisational security measures to protect information against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other unlawful processing in violation of DDIS legislation, and the same applies to DDIS' data processors. For information which is being processed for DDIS and is of special interest to foreign powers, measures must be implemented to allow destruction or disposal in case of war or the like, see section 4 of the DDIS Executive Order on Security Measures.

When DDIS makes information available for processing by a processor, DDIS must ensure that the processor is able to implement the technical and organisational security measures mentioned in sections 3 and 4 of the DDIS Executive Order on Security Measures and must review that this is done, see section 5(1) of the DDIS Executive Order on Security Measures. If a controller makes information available for processing by a processor, the parties must conclude a written agreement, see section 5(2) of the DDIS Executive Order on Security Measures.

3.3 Disclosure of information

3.3.1 About disclosure of information, see section 7 of the DDIS Act

Section 7 of the DDIS Act on disclosure of information provides in subsection (1) that DDIS is allowed to disclose information to DSIS 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 DSIS is due to the close connection between the spheres of activity of the two intelligence services.

Under subsection (2), DDIS is further allowed to disclose personal information about a natural person resident in Denmark to Danish administrative authorities (other than DSIS), private individuals and organisations, foreign authorities and international organisations subject to the conditions for internal processing in sections 3e and 4 of the DDIS 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

- 1) explicit consent has been obtained from the data subject,
- 2) disclosure is made to safeguard private or public interests which clearly outweigh the interests of confidentiality, including the interests of the data subject,
- 3) 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
- 4) if disclosure is necessary for the performance of the activities of a person or business on behalf of the public authorities.

For DDIS' disclosure of information about legal persons resident in Denmark to Danish administrative authorities other than DSIS, private individuals and organisations, foreign authorities and international organisations, section 7(3) of the Act provides that the conditions for internal processing in sections 3e(1)-(5) and (7) and section 5 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 7(2) and (3) are supplemented by a condition in subsection (4) to the effect that DDIS will be allowed to disclose information under subsections (2) and (3) only if the disclosure is deemed to be sound based on a specific assessment in each individual case.

According to the explanatory notes to the Bill concerning section 7(4), 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 DDIS' former internal guidelines on cooperation with foreign intelligence services and the like – must include clear provisions on the conditions for disclosure of identifiable personal information to foreign partners. TET will be given an opportunity to review DDIS' compliance with such rules.

3.4

Legal political activity

3.4.1

About legal political activity, see section 8 of the DDIS Act

Section 8 of the DDIS 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 DDIS. Subsection (2) provides, however, that the provision in subsection (1) does not preclude DDIS 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 DDIS from including information about the leadership of political associations and organisations when processing information about such associations and organisations.

With regard to political activity, the explanatory notes to the DDIS Bill concerning section 8 state that this generally means 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, DDIS is allowed to process information about a person's legal political activity if there are other factors, which mean that a person has attracted DDIS' interest. If the person in question has already become the focus of DDIS in connection with the performance of its activities, DDIS 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 directed at the Danish military. In each individual case, DDIS 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), DDIS 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 DDIS' 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 DDIS 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.

According to the explanatory notes to the Bill concerning the provision in subsection (3), it will be a central responsibility for TET to ensure that information about a person's legal political activity in the form of participation as a leader of a political organisation or association is processed only to the extent that this is deemed necessary for a meaningful processing of information about the organisation or association.

3.5

Rules on subject access requests etc.

3.5.1

About subject access requests, see sections 9 and 10 of the DDIS Act

Under section 9 of the DDIS Act, natural and legal persons are not entitled to access information processed by DDIS about them or entitled to know whether DDIS is processing information about them. If special circumstances weigh in favour of doing so, however, DDIS may decide to grant full or partial access to such information.

Under section 10 of the DDIS Act, natural and legal persons resident in Denmark are allowed to request TET to review if DDIS is processing information about them in violation of DDIS 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 DDIS to grant full or partial access to the information in the same way as under section 9.

Section 10 of the DDIS Act thus establishes an indirect subject access request system, meaning that as part of its review of DDIS' processing of information about natural and legal persons resident in Denmark, TET must also review, if so requested by such a data subject, if DDIS is processing information about the data subject in violation of DDIS legislation. As part of this indirect subject access request system, TET is entitled among other things to order DDIS to delete information which, in the opinion of TET, DDIS is processing in violation of DDIS legislation. TET will verify that DDIS is not processing information about the data subject in violation of DDIS legislation and then notify the data subject. According to the explanatory notes to the DDIS 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 DDIS 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 DDIS legislation or whether information is being processed in compliance with DDIS legislation.

A person who has received a reply from TET under section 10 of the DDIS Act is not entitled to receive a reply to a new request until six months after the most recent reply.

3.6

Processing of passenger name records (PNR information) for DDIS

3.6.1

Request for information concerning natural persons resident in Denmark, see section 15(3) of the PNR Act

DDIS' intelligence-related activities are directed at conditions abroad, see section 1(1), 2nd sentence, of the PNR Act.

As a general rule, therefore, DDIS is not allowed to engage in targeted intelligence obtaining about persons resident in Denmark. However, there are a number of exceptions

to the general rule, including in connection with DDIS' physical obtaining and obtaining pursuant to section 3(3) of the DDIS Act.

Under section 15(3) of the PNR Act, DDIS is only allowed to request the PNR authority to provide PNR information about natural persons resident in Denmark if the information concerns specified persons and DDIS believes that the information must be assumed to be of significance to the performance of DDIS' activities directed at conditions abroad. The requirement to processing is thus stricter than the other provisions of the PNR Act concerning DDIS, according to which it is only a requirement that the PNR information may be of significance to DDIS' activities.

The restriction provided in section 15(3) of the PNR Act applies correspondingly in relation to a number of the provisions of the PNR Act, including sections 4, 10 and 16 of the PNR Act.

3.6.2 Obtaining of intelligence by PPNR for DDIS, see sections 4 and 16 of the PNR Act

Under section 4(3)(iii) of the PNR Act, airlines must disclose PNR information, if so requested by PPNR in each case, where DDIS believes that the information may be of significance to the performance of its activities directed at conditions abroad.

Further, under section 16(3)(iii) 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 DDIS believes that the information may be of significance to the performance of its activities directed at conditions abroad.

3.6.3 PPNR's processing and disclosure of PNR information on behalf of DDIS, 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 DDIS under paras (i) - (iv) of section 10 for as long as it is necessary to inform DDIS 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 DDIS 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. (iii) of section 10 of the PNR Act, PPNR is allowed to process PNR information where DDIS believes that the information may be of significance to the performance of its activities directed at conditions abroad. If the PNR information concerns natural persons resident in Denmark, DDIS is only allowed under section 15(3) of the PNR Act to request such information if the information concerns specified persons and DDIS believes that the information must be assumed to be of significance to the performance of DDIS' activities directed at conditions abroad.

Moreover, under section 15(2) of the PNR Act, PPNR must, if so requested by DDIS, disclose PNR information or the result of the processing of such information to DDIS as soon as possible where DDIS believes that the information may be of significance to the performance of its activities directed at conditions abroad.

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 Defence 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