Danish Intelligence Oversight Board

Annual report 2022

Danish Defence Intelligence Service (DDIS)

Contents

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 2022 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 oversight activities performed with regard to DDIS.

TET oversees 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 erasure 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 review 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 oversees compliance with the provisions of the PNR Act concerning

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

when the PNR Unit of the Danish National Police (RPNR) procures, processes and discloses information on behalf of DDIS. TET also oversees RPNR's procurement, processing and disclosure of information on behalf of DSIS, and TET's checks of RPNR are therefore discussed in TET's annual report on the oversight of DSIS in 2022.

Copenhagen, June 2023

Michael Kistrup
Chair of the Danish Intelligence Oversight Board

Introductory comments

As Denmark's foreign and military intelligence service, DDIS is tasked with the responsibility 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 perform this nationally important function, DDIS has very broad powers and capabilities under the law to procure information. In order to ensure due process protection for the individual citizen and business in Denmark, DDIS' wide powers are counterbalanced by rules that DDIS may not, without a court order, direct its intelligence obtaining capabilities at persons resident in Denmark or persons currently staying in Denmark.

In 2022, TET has carried out in-depth and intensive compliance reviews with regard to DDIS, including of DDIS' targeted procurement of information and handling of raw data with a focus on time stamping and erasure.

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

However, TET's review of DDIS in 2022 has been limited in relation to DDIS' procurement and disclosure of raw data as a result of the DDIS Commission's report of 13 December 2021.

Following a detailed examination of the DDIS Commission's report, on 2 February 2022, TET submitted a report to the Minister of Justice and the Minister of Defence on, among other things, the consequences that the DDIS Commission's report – in TET's view – may have for the independent monitoring of DDIS if the DDIS Commission's interpretation of the DDIS Act were to be used as a basis for the future reviews of DDIS.

In its report, TET also informed the Minister of Defence that it had decided to temporarily suspend all ongoing reviews concerning DDIS' obtaining of raw data and that TET would not initiate new reviews concerning DDIS' obtaining or disclosure of raw data until TET's scope of competence had been clarified. As a result, in 2022, nine out of 38 planned reviews of DDIS were not carried out, as TET was awaiting the decision of the Minister of Defence.

TET received the decision of the Minister of Defence on 16 January 2023. According to the decision, the Minister shares the DDIS Commission's view that TET's scope of competence does not include review of DDIS' obtaining and disclosure of raw data.

As a result, TET will organise its future review of DDIS in accordance with the decision of the Minister of Defence.

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

Finally, in 2022, DDIS has reported to TET on its extensive efforts to bring its IT infrastructure up to date, among other things with a view to ensuring increased compliance and support for DDIS' internal controls and TET's independent oversight.

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

Scale of TET's comments

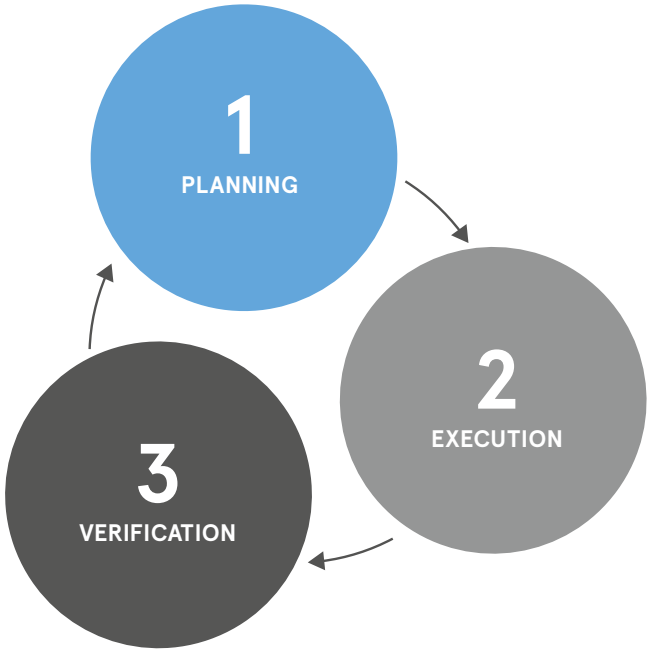
TET's comments are based on the following scale:

Comments	Background to comments
»[...] **does not give rise to any comments**«	Used when TET agrees with DDIS on how it is 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 DDIS 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 DDIS having demonstrated a willingness to ensure the necessary remedial action.

1. Oversight method

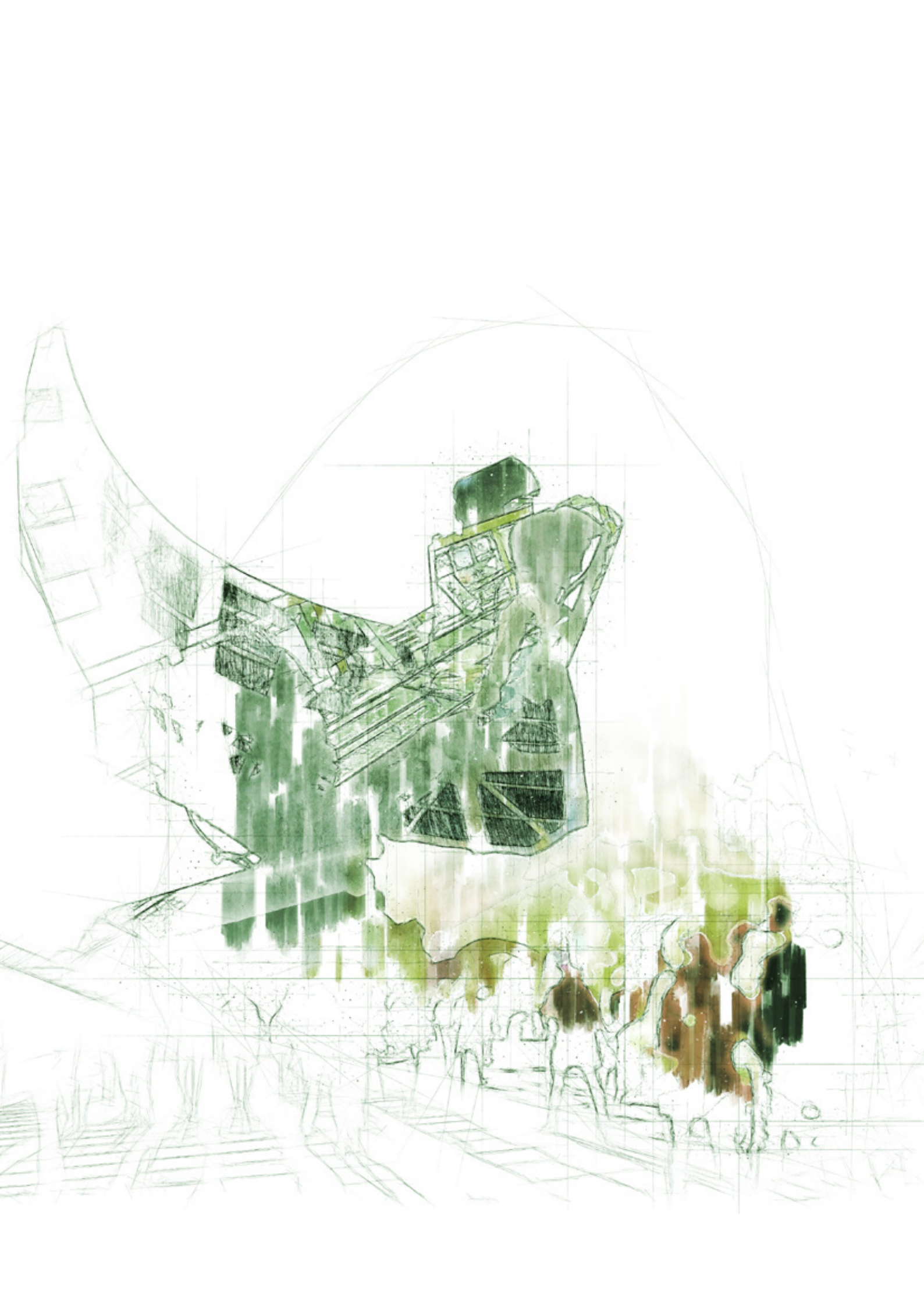
TET continuously works to improve the methods it uses in the planning and performance of its oversight of DDIS in order for the oversight to be as effective as possible within the framework set for the work of TET.

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



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

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



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

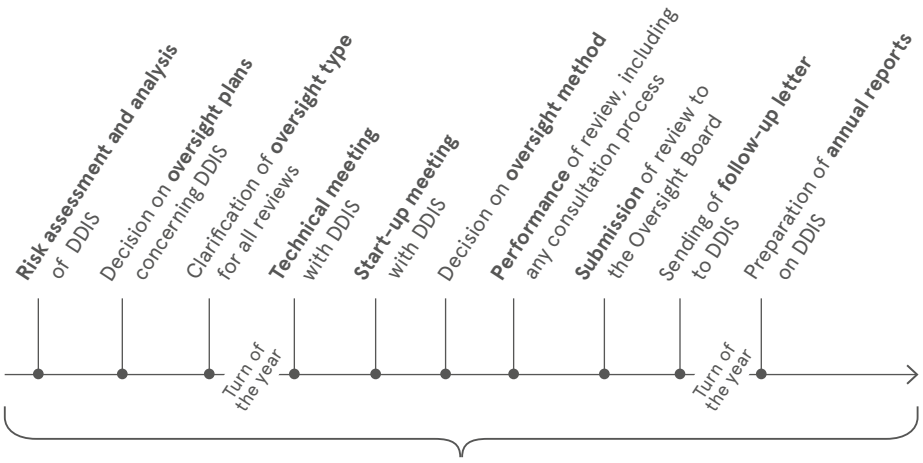
The reviews **2)** are conducted regularly throughout the year based on the DDIS oversight plan approved by TET. TET does not define the methods for the individual reviews in connection with the preparation of risk assessments and analyses, and the choice of method must thus be determined prior to initiating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

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

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

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

TET's activities include the following stages:



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

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

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

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

Furthermore, TET prepares a separate risk assessment and analysis specifically for TET's reviews in relation to 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 oversight methods, reference is made to the relevant standards published by TET, which are available on TET's website.

2. TET's review

2.1 Summary of TET's reviews in 2022

In 2022, TET has completed 25 out of 38 planned reviews of DDIS.

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

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

- 14 out of 24 reviews of DDIS did not give rise to any comments. Of the remaining ten reviews, none gave rise to any comments on highly criticisable matters.

- TET found the following criticisable:

  - That in 112 cases DDIS processed information in an internal mailing system which should have been erased pursuant to section 6(1) of the DDIS Act (section 2.2.7).

  - That in 117 cases DDIS processed information in a system for handling DDIS' external communication which should have been erased pursuant to section 6(2) of the DDIS Act (section 2.2.7).

- TET identified the following:

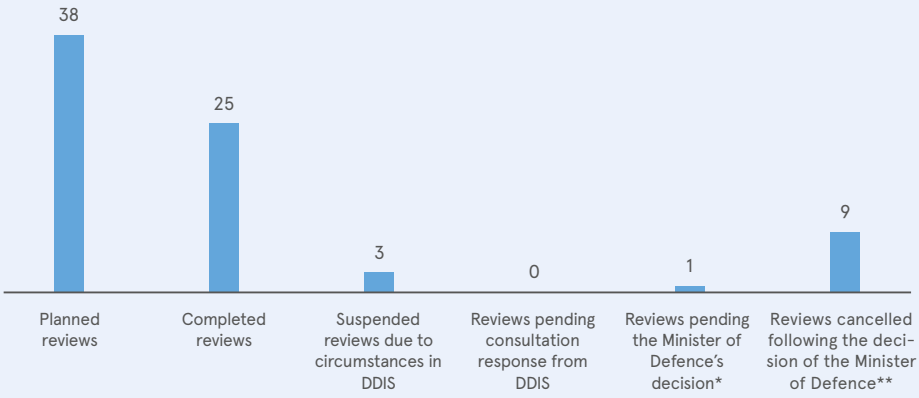
  - That in seven cases DDIS had obtained intelligence about persons resident in Denmark in violation of DDIS legislation. However, TET noted that DDIS itself discovered the obtaining of intelligence in violation of DDIS legislation on the same day as it was initiated and that DDIS immediately thereafter ceased the intelligence obtaining (section 2.2.1).

  - That DDIS in a raw data storage system failed to explain whether raw data complied with the time limit for erasure in section 6(2) of the DDIS Act. Considering the age of the system in question and information previously received from DDIS, TET found that raw data were stored in the system in violation of section 6(2) of the DDIS Act.

    TET noted that on the basis of the review DDIS presented a plan for erasure of raw data in the system with a view to ensuring that in future no raw data will be stored in violation of section 6(2) of the DDIS Act.

    In March 2023, DDIS informed TET that it had erased the raw data in question (section 2.2.2).

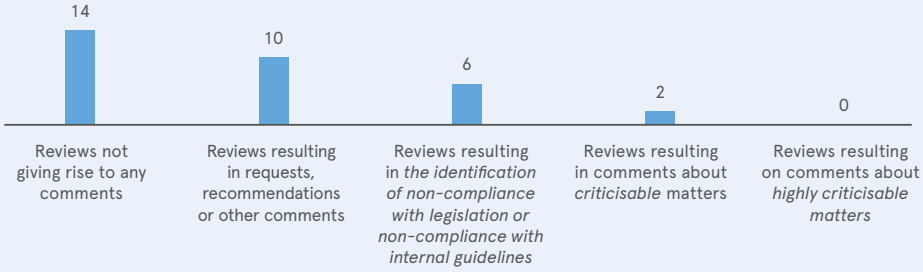
TET's reviews of DDIS in 2022



* TET's reviews of DDIS' security of processing based on the ISO/IEC 27001 standard, which was submitted to the Minister of Defence in 2022. Instead, TET has assessed the security of processing in connection with individual reviews (see section 2.2.9).

** TET's planned reviews of DDIS' obtaining of raw data, which has been cancelled as a result of the decision of the Minister of Defence of 16 January 2023 (see section 3).

Results of TET's review of DDIS in 2022



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

▷ That DDIS in a raw data storage system stores a large amount of raw data with time stamping errors.

In connection with the review, DDIS informed TET that there are no indications nor does DDIS expect that the raw data with an incorrect time stamping is older than 15 years, and that the raw data with an incorrect time stamping constitutes a relatively very small proportion of the total amount of raw data in the system.

TET recommended that DDIS carry out an assessment of when the raw data in the system with an incorrect time of obtaining should be erased, see section 6(2) of the DDIS Act.

In addition, TET found that the errors in the time stamping have resulted in a risk that DDIS' raw data searches may have shown information about persons resident in Denmark in violation of DDIS legislation.

After receiving TET's verification result, DDIS noted that the risk of the information in question being shown in violation of DDIS legislation in raw data searches is, in DDIS' assessment, very low or negligible.

TET noted that in 2021, DDIS introduced mitigating measures to ensure that the type of errors that constitute the majority of the errors found in the time stamping will not occur in the future, and in connection with the review in 2022, DDIS introduced mitigating measures to minimise the risk that the incorrect time stamping may lead to raw data being shown in violation of DDIS legislation.

In April 2023, DDIS informed TET that it had erased or corrected all raw data with an incorrect time stamping in the system (section 2.2.2).

- That in 11 out of 76 cases reviewed (14 percent) DDIS had performed raw data searches in violation of DDIS legislation (section 2.2.3).

- In one case, DDIS had not erased a case even though DDIS decided in 2019 that the case should be erased as there was no basis for extending the storage in accordance with section 6(3) of the DDIS Act.

  TET informed DDIS that DDIS' decision not to erase information about persons resident in Denmark must be made no later than at the expiry of the time limit for erasure under section 6(1) of the DDIS Act.

  Against this background, TET recommended that DDIS as soon as possible review parts of the archive in question in order to ensure compliance with section 6(1) of the DDIS Act (section 2.2.5).

- TET found it problematic that in 2022, TET was not able to carry out efficient reviews of a significant amount of information stored by DDIS in three drive structures, as a solution that enables searching the content of the drive structures had still not been established.

  In 2018, TET and DDIS entered into a dialogue about the need to establish a solution that enables searching the content of the drive structures, and in early 2020, DDIS initiated work to establish such a solution. However, in the first half of 2022, there was no progress in DDIS' project to establish such a solution, which TET found very unsatisfactory.

  In TET's assessment, DDIS continues to demonstrate a willingness to ensure that the criticised conditions are remedied, including that DDIS has allocated additional resources from the second half of 2022 to establish the solution, which is currently expected to be completed in 2023 (section 2.2.6).

- On the information available, TET was unable to assess whether DDIS had taken the appropriate security measures in two systems in accordance with section 3 of the DDIS Executive Order on Security Measures (section 2.2.9).

- In 2022, TET has finally processed requests from 34 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 five cases 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. 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. DDIS has on that basis erased the information (section 2.4.2).

2.2 Review of DDIS in 2022

For the purpose of reviewing DDIS' compliance with the provisions of the DDIS Act when processing information about natural and legal persons, TET has carried out reviews in 2022 of DDIS'

- targeted intelligence obtaining (SIGINT) (1.2.3),
- handling of raw data (2.2.2),
- raw data searches (2.2.3),
- computer network operations (CNO) (2.2.4),
- processing of information relating to physical intelligence obtaining (HUMINT) (2.2.5),
- processing of information on drives (2.2.6),
- processing of information in communication systems (2.2.7),
- disclosure of information to partners (2.2.8),
- security of processing (2.2.9), and
- internal controls (2.2.10).

Furthermore, in 2022, TET has completed

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

2.2.1 Reviews 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 2022, TET has performed regular reviews of DDIS' targeted intelligence obtaining directed at Danish-related selectors.

Comments by TET

TET identified that in seven cases, DDIS had obtained intelligence about persons resident in Denmark in violation of DDIS legislation. TET noted that DDIS itself discovered the obtaining of intelligence in violation of DDIS legislation on the same day as it was initiated and that DDIS immediately thereafter ceased the intelligence obtaining.

2.2.2 Reviews of DDIS' handling of raw data

Through its electronic intelligence obtaining (SIGINT), 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 erased 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 erase 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 2022, TET has performed reviews of two of DDIS' raw data storage system.

Comments by TET

TET found that DDIS failed to explain whether raw data in one of the systems reviewed complied with the time limit for erasure in section 6(2) of the DDIS Act. TET identified that raw data were stored in the system in violation of section 6(2) of the DDIS Act, considering the age of the system in question and information previously received from DDIS.

TET noted that on the basis of the review DDIS presented a plan for erasure of raw data in the system with a view to ensuring that in future no raw data would be stored in violation of section 6(2) of the DDIS Act.

In March 2023, DDIS informed TET that it had erased the raw data in question.

In connection with its review of the second of the raw data storage systems reviewed, TET identified that there were errors in the time stamping of a large amount of raw data stored in the system.

In connection with the review, DDIS informed TET that there are no indications nor does DDIS expect that the raw data with an incorrect time stamping is older than 15 years, and that the raw data with an incorrect time stamping constitutes a relatively very small proportion of the total amount of raw data in the system.

TET stated that in its assessment it is DDIS' responsibility at all times to be able to account for the processing of raw data in accordance with the time limit for erasure. If DDIS cannot present a correct time of obtaining of raw data and cannot otherwise prove that the raw data complies with the time limit for erasure, the raw data in question must therefore be erased as a general rule.

Against this background, TET recommended that DDIS carry out an assessment of when the raw data in the system with an incorrect time of obtaining should be erased, see section 6(2) of the DDIS Act.

In addition, TET found that the errors in the time stamping have resulted in a risk that DDIS' raw data searches may have shown information about persons resident in Denmark in violation of DDIS legislation.

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 erasing 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 erasing raw data
The time stamp will naturally form the starting point for the assessment of when raw data must be erased 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 raw data complies with the time limit for erasure.

After receiving TET's result of the review, DDIS noted that the risk of the information in question being shown in violation of DDIS legislation in raw data searches is, in DDIS' assessment, very low or negligible.

TET further noted that in 2021, DDIS introduced mitigating measures to ensure that the type of errors that constitute the majority of the errors found in the time stamping will not occur in the future, and that in 2022 DDIS introduced mitigating measures to minimise the risk that the incorrect time stamping may lead to raw data being shown in violation of DDIS legislation.

In April 2023, DDIS informed TET that it had reviewed the raw data with an incorrect time stamping in order to find out when the time limit for erasure expired. Thus, in DDIS' assessment, none of the data with an incorrect time stamping in the system in question had exceeded the time limit for erasure in section 6(2) of the DDIS Act. DDIS also informed TET that it had erased or corrected all raw data with an incorrect time of obtaining.

2.2.3 Reviews of DDIS' raw data searches

As described in section 1.2.1, DDIS procures very large amounts of unprocessed data (raw data), through its electronic obtaining – Signals Intelligence (SIGINT). 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.

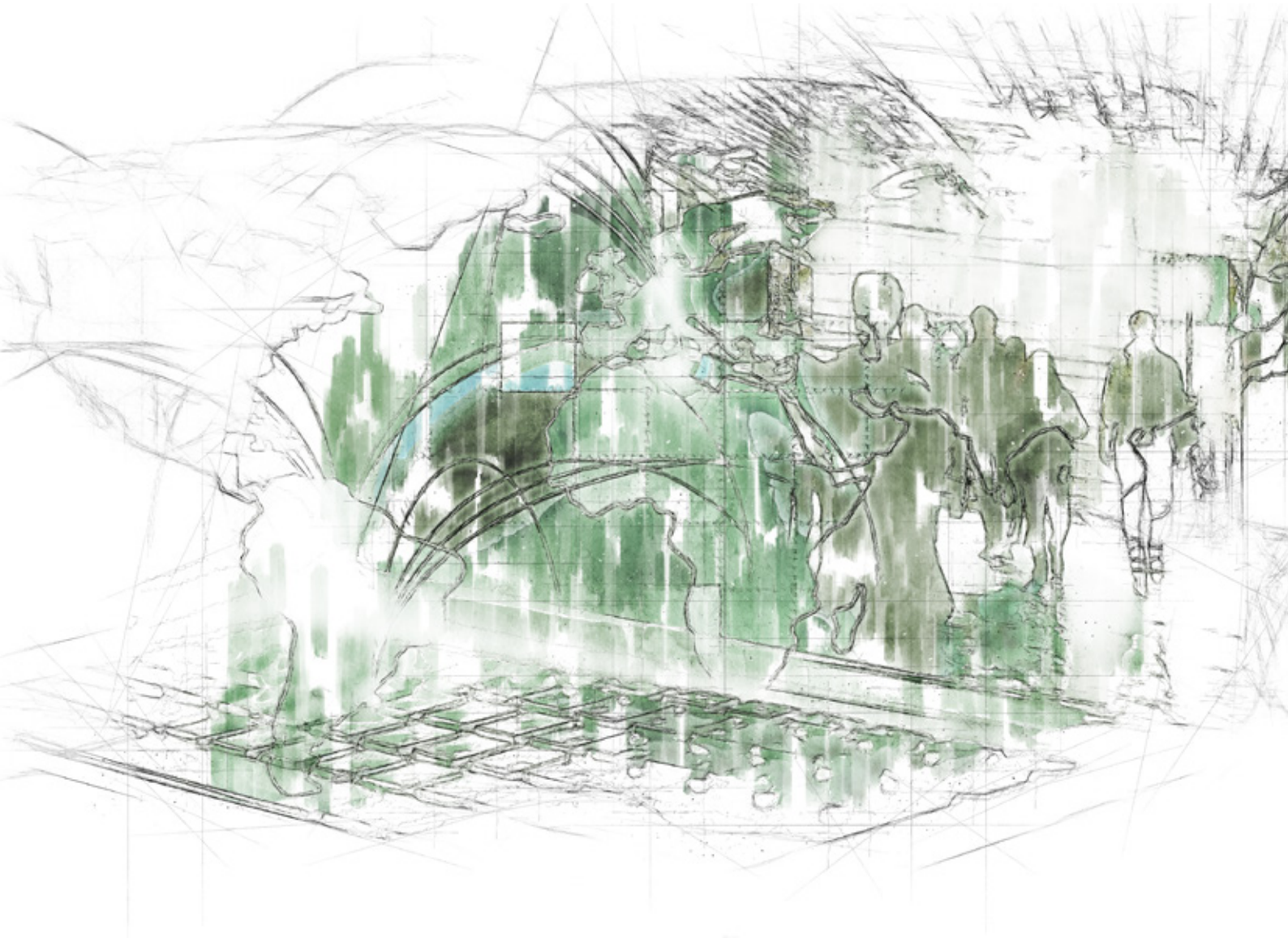
DDIS is not allowed to search raw data of its own motion if the result may be expected to be mainly information about identifiable persons resident in Denmark, unless the search is based on a court order obtained by DDIS, see section 3(3) of the DDIS Act. In addition, DDIS is allowed to make such searches 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 the result of which may be expected to be mainly 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 1.3 million raw data searches in 2022. In connection with DDIS' internal control, 333 searches targeting persons resident in Denmark have been identified, of which 37 cases (11 percent) have been identified by DDIS as raw data searches in violation of DDIS legislation.

In 2022, TET has 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.

Comments by TET

TET identified that DDIS in 11 of the 76 cases reviewed (14 percent) had performed raw data searches in violation of DDIS legislation as DDIS had not performed such data searches on behalf of DSIS within the framework of a court order obtained by DSIS and DDIS had not obtained a court order for such searches, see section 3(3) of the DDIS Act.

In 6 out of the 11 cases, the searches in violation of DDIS legislation were also identified by DDIS in its internal control. The remaining 5 searches in violation of DDIS legislation were not comprised by DDIS' internal controls.

2.2.4 Review 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, closed internet forums, IT systems and computers.

In addition, DDIS can support 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 monitor the use of force, but the processing of information about persons resident in Denmark and the handling of raw data that may be carried out in connection with an operation.

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

In 2022, TET has carried out a review of DDIS' use of CNO, focusing on DDIS' handling of raw data obtained in that connection.

Comments by TET

TET's review of DDIS' computer network operations did not give rise to any comments.

2.2.5 Review of DDIS' processing of information relating to physical intelligence obtaining (HUMINT)

DDIS engages in physical obtaining of human intelligence by the use of handling officers who obtain intelligence from other persons or sources – also known as Human Intelligence (HUMINT).

Human intelligence obtained by DDIS through the use of handling officers is generally subject to the same processing rules as those applying to other information obtained by DDIS. However, DDIS maintains a particularly high level of security and secrecy regarding the sources it uses.

In 2022, TET has carried out a review of DDIS' processing of information in one of its archives used for holding information obtained by physical obtaining.

Comments by TET

TET identified that in one case, DDIS had not erased a case even though DDIS had decided in 2019 that the case should be erased as there was no basis for extending the storage in accordance with section 6(3) of the DDIS Act.

TET informed DDIS that the service's decision not to erase information about persons resident in Denmark must be made no later than at the expiry of the time limit for erasure under section 6(1) of the DDIS Act. Against this background, TET recommended that DDIS as soon as possible review parts of the archive in question in order to ensure compliance with section 6(1) of the DDIS Act.

In continuation of the review, TET and DDIS have discussed the requirements for DDIS' notification of TET in connection with the extension of the storage period for information about persons resident in Denmark under section 6(3) of the DDIS Act. In this connection, TET has informed DDIS that TET still finds that the briefing must as a minimum enable TET to identify the information in question and the specific circumstances on which DDIS' assessment is based. Where, in DDIS' assessment, the grounds for not erasing are no longer expected to exist, TET also needs to be informed thereof.

2.2.6 Review of DDIS' processing of information on drives

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

In 2022, TET had planned to carry out compliance reviews with respect to four different drive structures in DDIS.

Comments by TET

TET found it problematic that with respect to three of DDIS' drive structures containing a considerable amount of information TET was unable to carry out an effective review of DDIS' processing of information as a solution enabling searches in the content of the drive structures had still not been established.

In order for DDIS to ensure compliance with the provisions of the DDIS Act and for TET to be able to carry out a satisfactory review thereof, TET found it to be necessary to establish possibilities for searching the content of the drive structures. This applies, for example, to erasure of data on persons resident in Denmark, see section 6(1) of the DDIS Act, and in relation to citizens' indirect subject access requests under section 10 of the DDIS Act. In its assessment, TET has, among other things, given weight to the scope and duration of the processing carried out.

In 2018, TET and DDIS entered into a dialogue about the need to establish a solution that enables searching the content of the drive structures, and in early 2020, DDIS initiated work to establish such a solution. However, in the first half of 2022, there was no progress in DDIS' project to establish such a solution, which TET found very unsatisfactory.

In TET's assessment, DDIS has demonstrated a willingness to ensure that the criticised conditions are remedied, including that DDIS has allocated additional resources from the second half of 2022 to establish the solution, which is currently expected to be completed in 2023.

TET's review of DDIS' processing of information in an additional drive structure did not give rise to any comments.

2.2.7 Reviews of DDIS' processing of information in communication systems

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 uses various communication or mailing systems that enable employees in different parts of DDIS to exchange information.

In 2022, TET carried out compliance reviews with regard to DDIS' processing of information in an internal mailing system and a system for handling external communication.

TET's review of the two systems focused on communications received more than 15 years prior to the review.

Against this background, TET requested DDIS to consider a number of questions regarding the communication found in cases where, in TET's assessment, the communication had contained information about persons resident in Denmark. Among other things, DDIS was asked to consider whether the information in the communication in question should have been erased, see section 6(1) of the DDIS Act, including whether new information had been procured within the last 15 years relating to the same case.

DDIS informed TET with respect to both systems that the communications which TET had asked questions about could be erased right away as they had been sent or received before 1 January 2008. In connection with TET's consultation, DDIS did not respond to TET's question as to whether, in DDIS' assessment, the information should have been erased.

As far as the internal mailing system was concerned, DDIS informed TET that in its general assessment it was not necessary to store the emails in question in the mailing system. In that connection, DDIS did not examine the emails in question in order to specifically assess whether they all contained information about persons resident in Denmark. Furthermore, DDIS did not specifically assess whether new information relating to the same case has been obtained within the past 15 years to the effect that the information in question should not have been erased.

As regards the system for handling external communication, in DDIS' general assessment, the continued storage of the information in question in the system was not necessary. In that connection, DDIS did not assess specifically whether the information contained information about persons resident in Denmark. Furthermore, DDIS did not specifically assess whether new information relating to the same case has been obtained within the past 15 years to the effect that the information in question should not have been erased.

Comments by TET

TET found it criticisable that in 112 cases DDIS processed information in an internal mailing system which should have been erased pursuant to section 6(1) of the DDIS Act as, in TET's assessment, the information in question related to persons resident in Denmark. In TET's assessment, the information should have been erased in 2017, 2019, 2020, 2021 and 2022, respectively.

TET found it criticisable that in 24 cases, DDIS processed information in a system for handling DDIS' external communication which should have been erased pursuant to section 6(1) of the DDIS Act as, in TET's assessment, the information in question related to persons resident in Denmark, and in 93 cases processed information which should have been erased pursuant to section 6(2) of the DDIS Act. In TET's assessment, the information should have been erased in 2019, 2020 and 2022, respectively.

For the information subject to the time limit for erasure in section 6(1) of the DDIS Act, TET assumed that no new information has been procured within the last 15 years relating to the same case, as DDIS had failed in connection with TET's consultation to inform TET that this was the case.

2.2.8 Reviews of DDIS' disclosure of information to partners

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 2022, TET carried out reviews of two systems used by DDIS to disclose information to partners.

Comments by TET

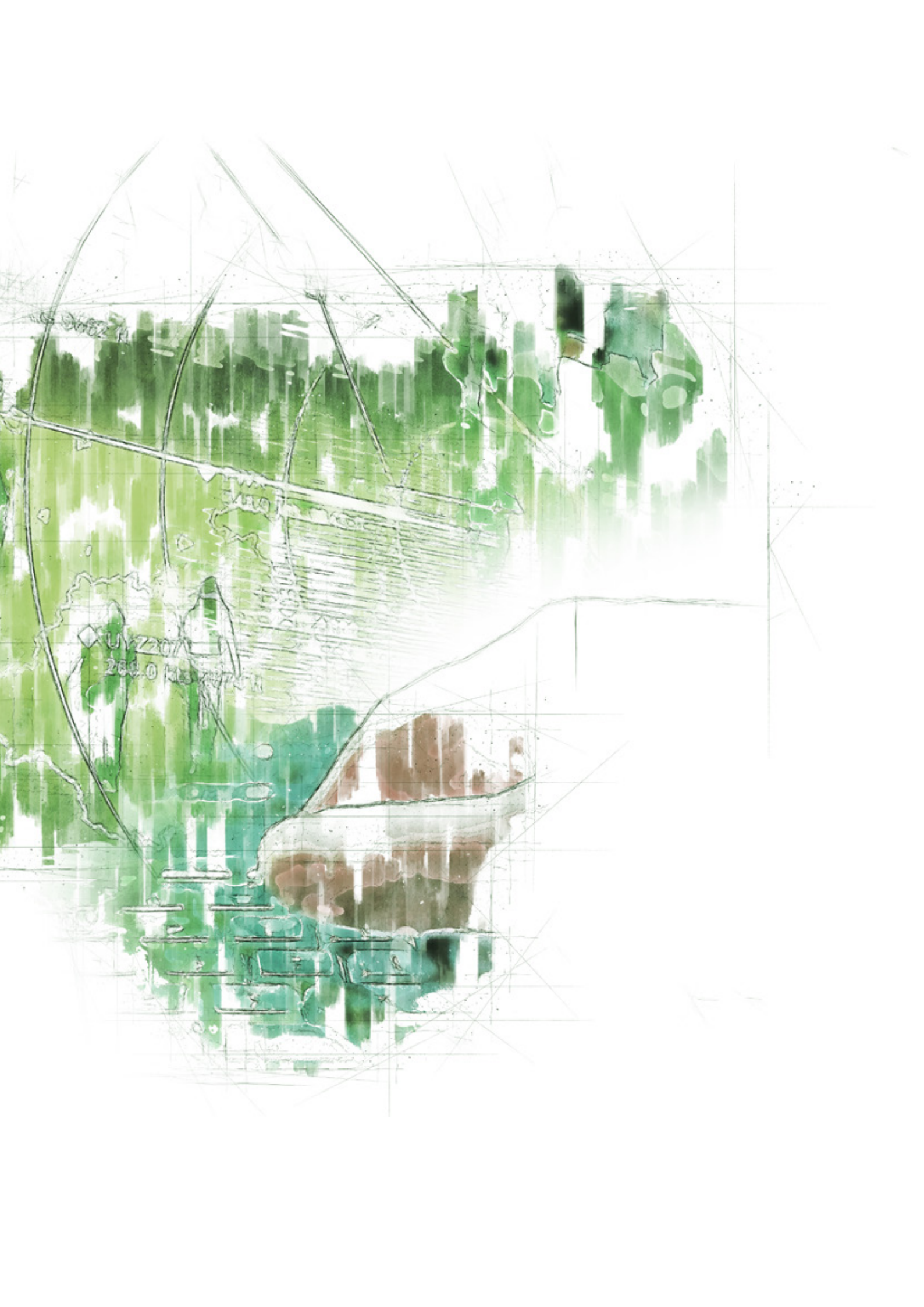
TET's reviews of DDIS' disclosure of information to partners did not give rise to any comments.

2.2.9 Review of DDIS' compliance with the rules on security of processing

Under section 3 of Executive Order No. 1028 of 11 July 2018 on security measures to protect personal information being processed by the Danish Defence Intelligence Service (DDIS) (the DDIS Executive Order on Security Measures), DDIS must implement appropriate technical and organisational security measures to protect information about persons resident in Denmark against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other unlawful processing in violation of the DDIS Act.

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

In connection with its security of processing review in 2021 (previously referred to by TET as information security review), DDIS has informed TET that, in its opinion, there may be



doubt as to the extent to which the implementation of the ISO/IEC 27001 standard should be subject to TET's review. The results of the reviews are described in more detail in TET's annual report on its review of DDIS in 2021 (section 1.2.8).

In a letter dated 3 May 2022, DDIS has requested the Minister of Defence to decide whether TET in its reviews of DDIS' security of processing can use the ISO/IEC 27001 standard to fulfil the overall obligations set out in section 3 of the DDIS Executive Order on Security Measures.

Against this background, TET's review of DDIS' security of processing in 2022 has not, as in previous years, been based on the ISO/IEC 27001 standard, as TET is still awaiting the decision of the Minister of Defence with respect to TET's request of 3 May 2022.

However, in relation to two systems in 2022, TET has asked detailed questions about how DDIS ensures that the processing in the systems in question is in accordance with the requirements of section 3 of the DDIS Executive Order on Security Measures.

In this regard, TET has asked DDIS to state:

- What measures DDIS has taken to ensure that the processing of data in the systems is in accordance with section 3 of the DDIS Executive Order on Security Measures.
- Whether DDIS has conducted a risk assessment of the security of processing of data processed in the systems.

DDIS has referred to its initiatives in the ISO/IEC 27001 area, which also contains a number of requirements for security of processing, as documentation for the measures taken by DDIS to ensure the level of security of processing.

Furthermore, DDIS has stated that in its opinion section 3 of the DDIS Executive Order on Security Measures does not contain a legal obligation for DDIS to perform risk assessments at system level when establishing systems within the existing IT infrastructure. After the review, DDIS has stated that in its assessment, the measures implemented by DDIS across the system portfolio can generally be assumed to meet the requirements of section 3 of the DDIS Executive Order on Security Measures.

Comments by TET

TET stated that it does not agree with DDIS' assessment that it was not the intention of section 3 of the DDIS Executive Order on Security Measures to lay down specific legal requirements for DDIS' security of processing.

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

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

Against this background, TET assessed that DDIS, in the cases where DDIS processes data, is obliged to make an assessment of which measures can provide an adequate level of security. The assessment will need to take into account the risks presented by the

processing and the nature of the data to be protected, taking into account the state of the art and the costs involved in their implementation. Once DDIS has completed the assessment, it will then be obliged to ensure that the relevant measures are implemented for the processing in question.

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

In TET's assessment, the fact that the Executive Order does not provide for a more specific implementation of the requirements that must be met, corresponding to the previously applicable Executive Order No. 528 of 15 June 2000 on security measures to protect personal information being processed on behalf of the public administration (the Executive Order on Security Measures), does not mean that DDIS is not obliged to ensure adequate security of processing in accordance with the framework provision in section 3 of the DDIS Executive Order on Security Measures.

On the information available, TET was unable to assess whether DDIS had taken the appropriate security measures in two systems in accordance with section 3 of the DDIS Executive Order on Security Measures.

After the review, DDIS informed TET that its response should be understood to mean that the measures implemented across the system portfolio can, in DDIS' assessment, generally be assumed to meet the requirements of section 3 of the DDIS Executive Order on Security Measures.

Based on the review, DDIS informed TET that it disagrees with TET's assessment and will therefore submit the matter to the Minister of Defence for a decision.

DDIS' compliance with the rules on security of processing will continue to be a focus point for TET.

2.2.10 Review of DDIS' internal review

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

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

In May 2022, DDIS has informed TET about its

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

In addition, DDIS has regularly informed TET about its internal reviews.

Comments by TET

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

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

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

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

TET has reviewed the information which DDIS agreed to erase in connection with TET's reviews in 2021 as well as DDIS' follow-up on the requests and recommendations made by TET to DDIS on the basis of TET's reviews in 2021. 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 2021. In 2022, TET followed up with DDIS on an ongoing basis regarding the status of the activities that had not yet been completed by DDIS.

Comments by TET

TET's follow-up on the review of DDIS in 2021 showed that in one case DDIS had not yet taken the actions that it had informed TET that it would based on TET's reviews in 2021. DDIS informed TET in connection with the review that this work is still ongoing.

After the reviews was concluded, DDIS informed TET that the work in question has now been completed.

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

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 2022 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 oversight of DDIS that TET has knowledge of DDIS' overall IT infrastructure so that its reviews can be targeted at the parts of the infrastructure which pose the greatest risk of processing in violation of DDIS legislation.

In 2022, TET has performed validation reviews and inspections of DDIS' IT infrastructure by inspecting a number of systems, which, in TET's immediate assessment, should not form part of TET's general reviews, in order to clarify whether the immediate assessment thereof was correct.

2.3 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 erase information which has reached the time limit for erasure 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.

DDIS has kept TET informed of its use of the provisions.

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

2.4.1 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 erase 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.

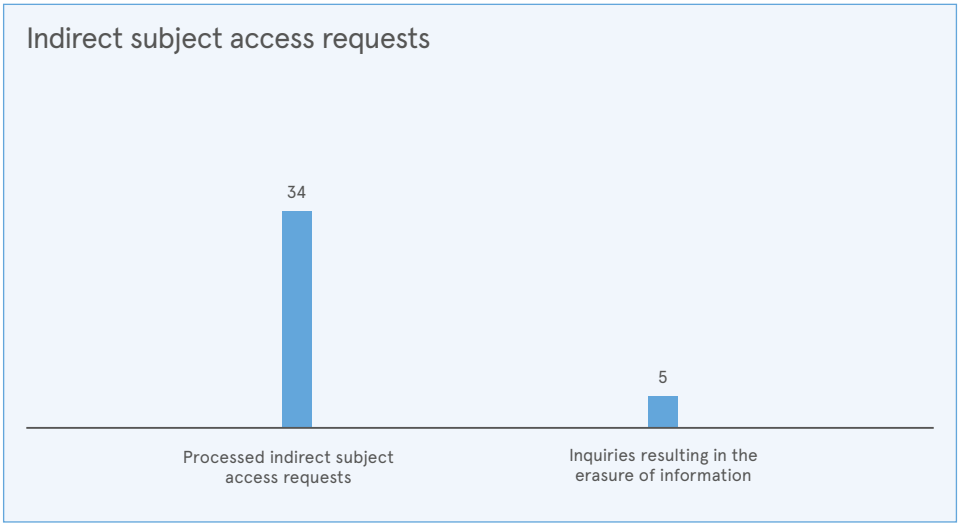
If special circumstances weigh in favour of doing so, TET may order DDIS to inform a natural or legal person of the information which DDIS is processing about them or inform them whether DDIS is processing information about them. Where TET receives a subject access request, TET will find out which information, 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.

2.4.2 Number of requests and processing time

In 2022, TET received subject access requests from 34 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 five cases 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. 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. DDIS has on that basis erased the information.

The average processing time for the processed requests was 199 days, 18 days of which were DDIS' processing time. Compared with 2021, the average processing time decreased by one day.



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.

In 2019, TET identified two systems in DDIS which should be subject to TET's reviews, but where it was not technically possible to conduct effective reviews of DDIS' processing of information (see TET's annual report for 2021, section 1.4.2). By the end of 2021, DDIS has established the possibility to carry out effective reviews in one of the systems in question, and the system has therefore been subject to TET's reviews in 2022. TET expects that a possibility will be established during the course of 2023 to carry out effective reviews of the other system.

2.5 DDIS' processing times in 2022

In 2022, TET submitted 14 legal consultations to DDIS in connection with its review activities. DDIS has responded to seven of TET's consultation questions within the specified deadline and seven after the specified deadline. DDIS' average processing time for responding to consultation questions that were responded to after the deadline was 33 working days.

3. Decision by the Minister of Defence regarding TET's competence to review DDIS' obtaining of raw data

Through its electronic intelligence obtaining, DDIS procures very large amounts of non-processed data, so-called raw data. Raw data is characterised by the fact that it is not possible to determine what information is contained in this data without further processing.

According to the DDIS Act and the legislative history of the Act, the special nature of raw data must be taken into account when applying the provisions of the Act.

Thus, when DDIS obtains raw data, the obtaining is only subject to a general requirement of legitimacy, as, in connection with the obtaining, DDIS is not aware of the specific content of the individual raw data obtained.

Similarly, the general rules of the DDIS Act on disclosure of information do not apply if DDIS discloses raw data to partners. However, according to the legislative history of the Act, disclosure of raw data should be based on a balancing of the need to disclose against the risks that may be involved.

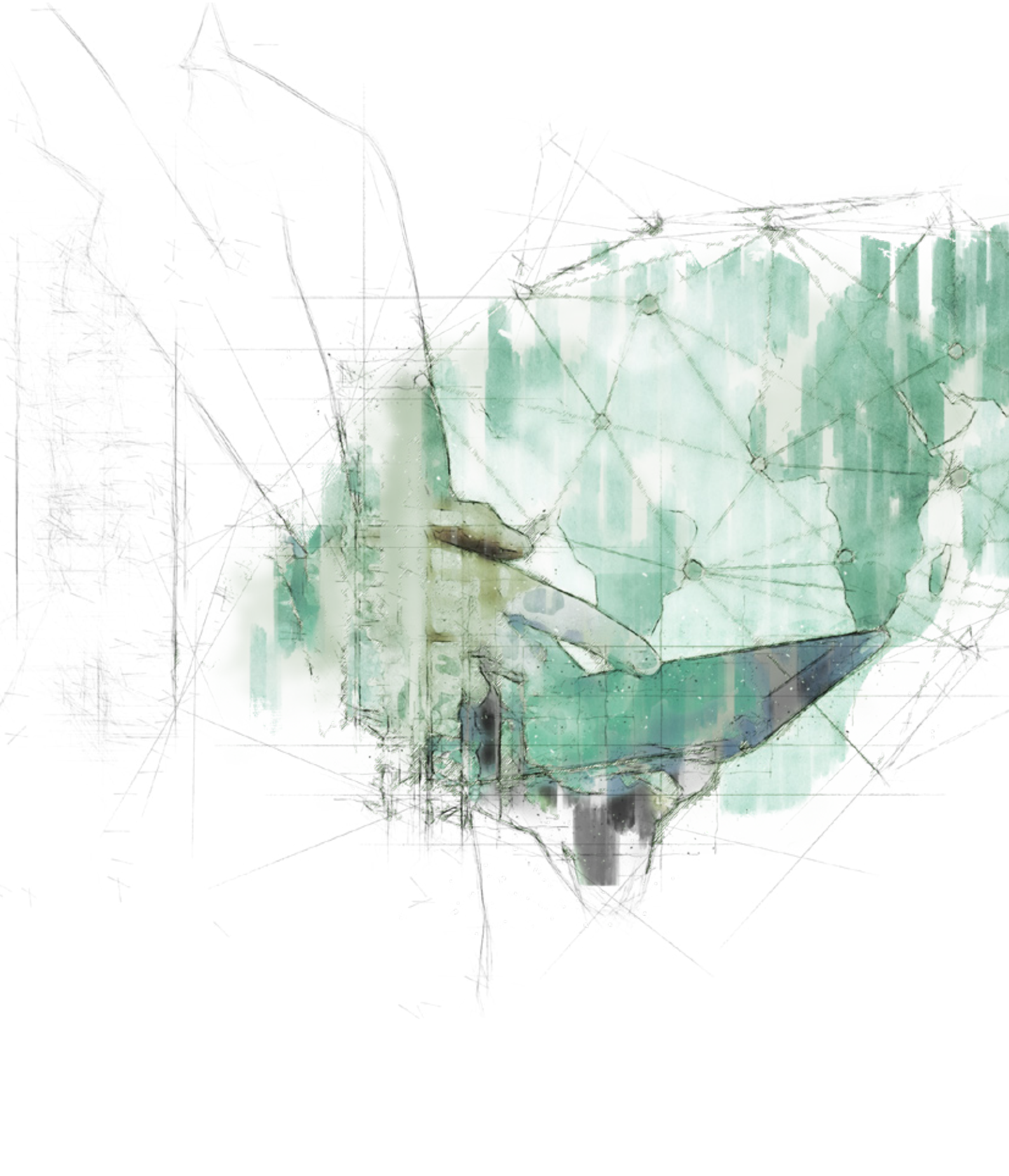
Based on TET's special review of DDIS, which was submitted to the Minister of Defence on 21 August 2020, the Minister of Justice appointed a commission on 21 December 2020 to investigate certain matters covered by TET's review of DDIS.

TET received the DDIS Commission's report on 14 December 2021.

In its report of 2 February 2022, TET noted in particular that the DDIS Commission had interpreted the DDIS Act to the effect that section 3 of the Act does not cover DDIS' obtaining of raw data and that the obtaining of raw data by DDIS thus falls outside the scope of TET's oversight powers.

In order to clarify the differences between the DDIS Commission's interpretation of the DDIS Act and the interpretation which has so far formed the basis of TET's oversight of DDIS, TET conducted a detailed analysis of the DDIS Commission's report.

In TET's assessment, the DDIS Commission's interpretation contradicts the practice that has existed between TET, DDIS and the Ministry of Defence since 2015, as TET has performed



regular reviews of DDIS' obtaining of raw data without such reviews having given rise to any comments.

Furthermore, in TET's assessment, a narrowing down of the review of DDIS in accordance with the interpretation of the DDIS Commission would be contrary to the practice of the European Court of Human Rights in *Big Brother Watch and Others v. The United Kingdom* and *Centrum för Rättvisa v. Sweden*.

It is crucial for TET that there is clarity and openness about the area of competence of TET and the obligations imposed on DDIS under the DDIS Act. This is due to both the consideration for DDIS, which must be able to organise its activities accordingly, and the consideration for the public, which must have the opportunity to gain insight into the framework for DDIS' activities and TET's oversight thereof.

Against this background, TET found it necessary, together with the Minister of Defence, to clarify the uncertainty about the interpretation of the DDIS Act that had arisen in connection with the DDIS Commission report.

On 2 February 2022, TET forwarded its comments on the DDIS Commission report to the Minister of Justice and the Minister of Defence and requested the Minister of Defence to decide which interpretation of the DDIS Act is to be used as a basis for TET's reviews of DDIS in the future, including in particular:

- Whether the area of competence of TET under section 15 of the DDIS Act includes DDIS' obtaining and disclosure of raw data.

- Whether DDIS is obliged to secure data in accordance with the rules of the DDIS Executive Order on Security Measures for systems that are solely or mainly used for handling raw data.

TET received the decision of the Minister of Defence on 16 January 2023.

In the decision, the Minister of Defence has, among other things, stated

- that TET is not required to review that DDIS' obtaining and disclosure of raw data complies with the requirements laid down in the DDIS Act, and

- that DDIS is not obliged to comply with the rules on security of processing in the DDIS Executive Order on Security Measures when storing raw data.

TET will organise its reviews accordingly.

Therefore, TET's reviews of DDIS will in future be organised in such a way that TET will no longer assess whether DDIS' obtaining complies with a general requirement of legitimacy or whether DDIS, in connection with the disclosure of raw data, has weighed the need to disclose data against the risks that may be involved.

Furthermore, TET's review of DDIS' security of processing will in future not include raw data stored by DDIS, as DDIS is not obliged to comply with the rules of the DDIS Executive Order on Security Measures when storing raw data.

TET will continue to oversee compliance with all other areas that are included in TET's review under section 15 of the DDIS Act, including

- that information relating to persons resident in Denmark has come into DDIS' possession by chance, which includes, among other things, that DDIS does not carry out targeted obtaining or searches in raw data obtained about persons resident in Denmark without a court order,

- that raw data is erased no later than 15 years from the time of obtaining, see section 6(2) of the DDIS Act, unless DDIS has specifically decided not to erase in accordance with section 6(3), and

- that DDIS for data which is not raw data, in accordance with the DDIS Executive Order on Security Measures, implements the necessary measures to prevent information about persons resident in Denmark against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse, etc.

Appendix

1. About Danish Defence Intelligence Service (DDIS)

The 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 Danish Defence Intelligence Service (DDIS) Act (the DDIS 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 oversee that the processing of the 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.

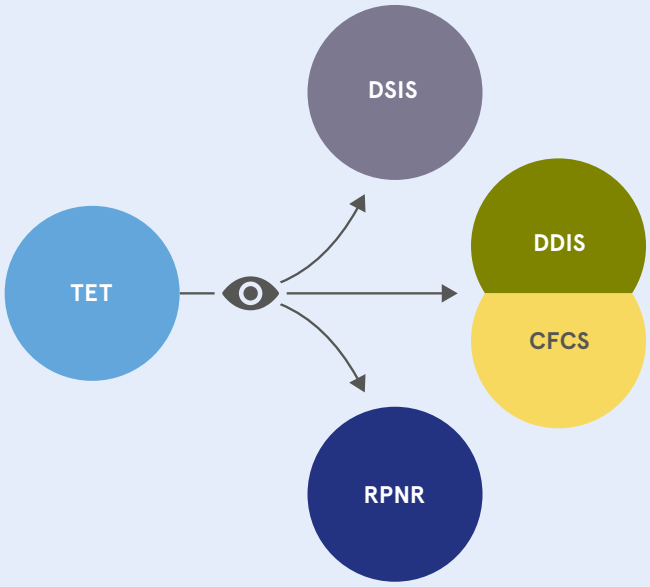
Appendix

2. Danish Intelligence Oversight Board (TET)

TET's activities

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

The Danish Intelligence Oversight Board (TET) is an independent monitoring body charged with overseeing that DSIS, DDIS, CFCS and the PNR Unit of the Danish National Police (RPNR) process personal information in compliance with DSIS, DDIS, CFCS and RPNR legislation.



TET is completely autonomous and is thus not subject to the directions of the Ministry of 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 2022:

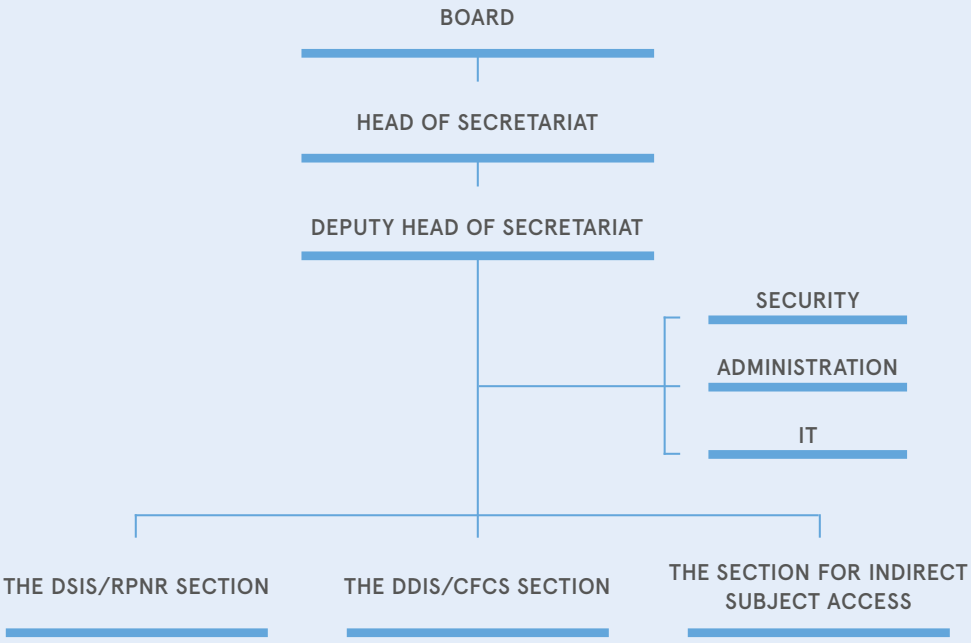
- High Court Judge Michael Kistrup, High Court of Eastern Denmark (Chair)
- Legal Chief Pernille Christensen, Local Government Denmark
- Professor Henrik Udsen, University of Copenhagen
- Professor Rebecca Adler-Nissen, University of Copenhagen
- Director Jesper Fisker, Danish Cancer Society

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

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

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

Organisation 2022



2.1 TET's duties in relation to 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,
- internal processing of information, including time limits for erasure 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 RPNR procures, processes and discloses information on behalf of DDIS.

TET must oversee 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 oversight, including whether to perform full reviews or random samplings, which aspects of the activities are to be given special priority and the extent to which TET wishes to raise a matter of its own motion. No specific guidelines have been provided for TET's performance of its oversight functions, except that – according to the legislative history of the Act – TET must for example carry out 3-5 inspections of DDIS each year in the course of its own motion compliance checks.

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

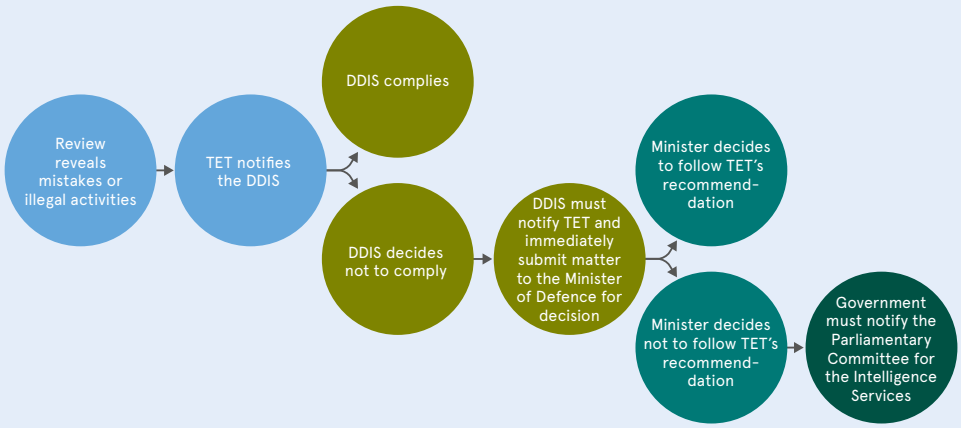
TET may require DDIS to provide any information and material of importance to TET's activities, and TET is entitled at any time to access any premises where the information being processed may be accessed or where technical facilities are being used. TET may furthermore require DDIS to provide written statements on factual and legal matters of importance to TET's oversight 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 information. If DDIS decides not to comply with a recommendation issued by TET in exceptional cases, DDIS must notify TET and immediately submit the matter to the Minister of Defence for a decision. If the Minister of Defence decides not to follow the recommendation of TET in exceptional cases, the Government must notify the Parliamentary Intelligence Services Committee.

Responses available for TET



TET must inform the Minister of 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, to investigate whether DDIS is processing information about that person in violation of DDIS legislation, TET may order DDIS to erase 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 oversight 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 oversight 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 erase information under the indirect subject access request system.

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

Appendix 3. Legal framework

1) The Danish 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).

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

3.1 Procurement of information

3.1.1 About collection and obtaining of information, see section 3 of the 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 oversight of the provision, the legislative history of the DDIS Act specifies that the oversight in particular includes a check 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 erasure 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 erase 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, erasure 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 erasure 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 erased, regardless of whether the time limit for erasure 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 checks 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 erase 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).

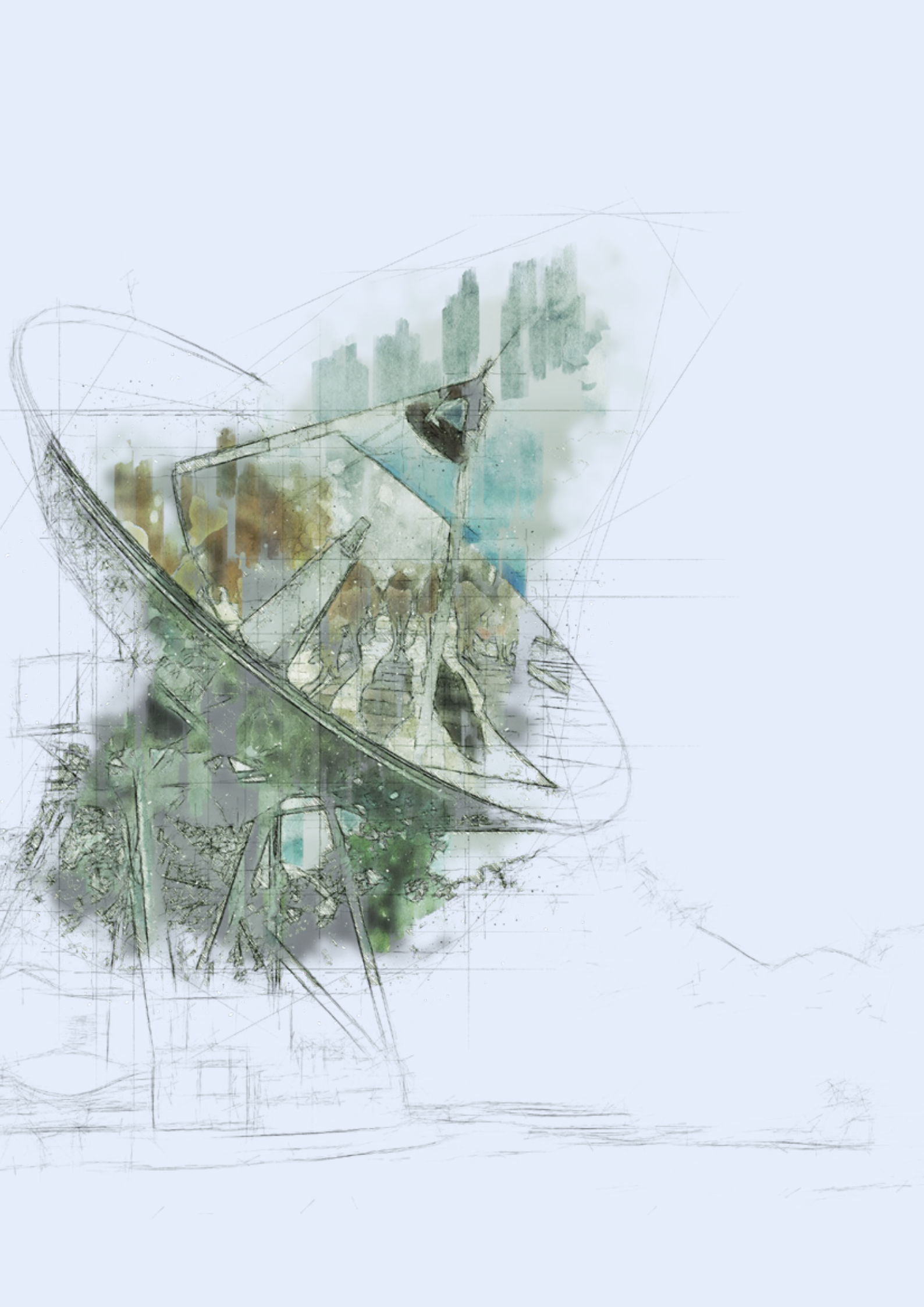
In the notes to the individual provisions of the Bill, it is specified with regard to section 6a(2) that the provision concerns erasure at data-level whereas the provision in subsection (1) concerns erasure at case- and document-level. DDIS is thus not required to erase information at data-level even 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 erasure has not yet expired. The proposed amendment further means that TET may still check in connection with its random checks whether a file or document, etc. as a whole meets the above-mentioned conditions of processing but that as a general rule DDIS will not be required to erase individual pieces of information which form part of documents etc. which are to be retained, in connection with such random checks. However, DDIS will still be required to erase 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 erase information. Such rules must be observed by DDIS, which means that DDIS is precluded from erasing the information as section 6 of the DDIS Act prescribes that DDIS' obligation to erase 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 the DDIS Act, 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 oversee 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 oversee 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 erased. 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 check 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 oversight of DDIS' processing of information about natural and legal persons resident in Denmark, TET must also check, 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 erase 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 RPNR 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 RPNR 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, RPNR may request the PNR units of other EU member states to disclose PNR information or the result of the processing of such information where DDIS believes that the information may be of significance to the performance of its activities directed at conditions abroad.

3.6.3 RPNR'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, RPNR 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 RPNR 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, RPNR 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, RPNR 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.

3.6.4 Security of processing, see section 24 of the PNR Act

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

1) Collection

2) Search

3) Changes

4) Disclosure

5) Masking and unmasking

6) Erasure

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

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

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

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

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

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

Members of the Danish Intelligence Oversight Board

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

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