The Danish Intelligence Oversight Board

Annual report 2018

Danish Defence Intelligence Service (DDIS)

Contents

To the Minister of Defence

The Danish Intelligence Oversight Board hereby submits its report on its activities concerning the Danish Defence Intelligence Service (*DDIS*) for 2018 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.

København, juni 2019

Michael Kistrup

Chairman of the Danish Intelligence Oversight Board

Foreword

The Danish Intelligence Oversight Board is a special independent monitoring body charged with overseeing that the Danish Defence Intelligence Service (*DDIS*) processes information about persons resident in Denmark in compliance with DDIS legislation. The Oversight Board was set up under the Danish Security and Intelligence Service (*DSIS*) Act (*lov om Politiets Efterretningstjeneste (PET)*), which – like the Danish Defence Intelligence Service (*DDIS*) Act (*lov om Forsvarets Efterretningstjeneste (FE)*) – entered into force on 1 January 2014.

The aim of this annual report is to inform about the nature of the oversight activities performed with regard to the Danish Defence Intelligence Service (*DDIS*). The report also provides information about the aspects which the Oversight Board has decided to examine more closely in 2018 and statistical data on the number of instances where the processing of personal information by the Danish Defence Intelligence Service (*DDIS*) has been found by the Oversight Board to be in violation of DDIS legislation. Furthermore, where relevant, the report includes a follow-up on the Oversight Board's checks in 2017.

Like in the preceding years, the Oversight Board has also in 2018 had particular focus on consolidating and strengthening the basis underlying its checks of the Danish Defence Intelligence Service (*DDIS*), the Danish Security and Intelligence Service (*DSIS*) and the Danish Centre for Cyber Security (*CFCS*), including by continuous development of the Oversight Board's risk and materiality assessment of the two intelligence services and CFCS as well as the standards and methods applied in the legal control thereof. It is of crucial importance to the Oversight Board that the individual checks are well-based and documented and that they are organised on the basis of an adequate professional and technical understanding from an intelligence perspective. Furthermore, in 2018, the Oversight Board has initiated various development projects for the purpose of securing more efficient system support for the Oversight Board's oversight activities.

In 2018, the Oversight Board carried out in-depth and intensive compliance checks with regard to DDIS's processing of information about natural and legal persons resident in Denmark. Like in the preceding years, the Oversight Board has given priority to checks with special focus on

DDIS's compliance with the legislation on procurement of information, on internal processing of information, including erasure, and on disclosure of information.

In addition, the Oversight Board has given priority to overseeing DDIS's compliance with the legislation on security measures (information security) in connection with processing of personal information. Finally, the Oversight Board has continued its work to identify and verify DDIS's system landscape at the server and component level.

The increased attention towards the indirect subject access request system attracted on the basis of the press coverage of the system at the beginning of the year has played a special role in the Oversight Board's checks in 2018. In 2018, the Oversight Board has received roughly four times as many indirect subject access requests as compared with the total number of requests since launching the system in 2014. The Oversight Board welcomes the increased attention towards the indirect subject access request system, but at the same time the Oversight Board must admit that the sudden increased interest in the system has resulted in pressure on the other oversight activities of the Oversight Board and on the processing time for indirect subject access requests. Section 1.5 provides a more detailed description of the Oversight Board's processing of requests under the indirect subject access request system in 2018.

In addition to the Oversight Board's general checks, the Oversight Board has in 2018 assessed the statutory basis for a practice between the Danish Defence Intelligence Service (*DDIS*) and the Danish Security and Intelligence Service (*DSIS*) where DSIS did not obtain a court order to intercept communications when requesting DDIS to perform raw data searches. The Oversight Board's assessment of this practice is described in more detail in section 2.

In 2018, the Oversight Board has broadened the scope of its cooperation with the Dutch Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), the Belgian Comité permanent de contrôle de services de renseignements et de sécurité (Committee I), the Norwegian Stortingets Kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget) and the Swiss Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND). The focus of this cooperation is to share experience with respect to oversight methods and to discuss legal subjects of mutual relevance. One of the results of this cooperation is that in November 2018, the five oversight and review bodies published a joint statement on strengthening cooperation between national intelligence oversight bodies. The statement is available on the Oversight Board's website.

Also, in April 2018, the secretariat of the Oversight Board visited the Swedish oversight bodies, Säkerhets- och integritetsskyddsnämnden (SIN) and Statens inspektion för försvarsunderrättelseverksamheten (SIUN), to share experience about various oversight methods.

In addition to the Oversight Board's close cooperation with specific oversight and review bodies, in December 2018 the Oversight Board participated in a joint European conference for oversight and review bodies in Paris, which was attended by 14 European countries.

Michael Kistrup

Chairman of the Danish Intelligence Oversight Board

1 The Oversight Board's oversight activities

1.1 Oversight method

The Oversight Board 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 Oversight Board's work.

The Oversight Board's oversight activities consist of three parts: planning, execution and verification. In addition, the Oversight Board regularly evaluates its work with all three elements.

The Oversight Board's planning of next year's compliance checks is based on an annual risk assessment of all processes and systems at DDIS. The purpose of the risk assessment is to assess the risk of non-compliance with legislation in relation to procurement, internal processing and disclosure of personal information about the groups of persons falling within the Oversight Board's scope of competence. On that basis, the Oversight Board prepares a risk analysis which forms the basis of the selection of the checks to be made in the coming year.

The purpose of the risk analysis is to ensure that the Oversight Board's 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 the Oversight Board'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 checked once every third year 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. Furthermore, the Oversight Board inspects systems which in connection with the risk assessment are deemed irrelevant to the Oversight Board's checks in order to check whether the relevance assessment is correct.

The Oversight Board's planning of next year's compliance checks is completed at the end of the preceding year in order for the experience gained from this year's checks to be included as part of the risk assessment and analysis.

The actual checks are conducted regularly throughout the year. As a general rule, the individual areas are checked by the secretariat of the Oversight Board. Based on a specific assessment, DDIS is requested to provide clarifying comments. The secretariat will then submit the results of the checks to the Oversight Board for its decision as to whether sufficient information has been obtained in each individual case or whether further details or discussions with DDIS are required.

The Oversight Board uses various methods to check the individual areas, including full checks, random checks, screening of content and interview-based checks. The Oversight Board's choice of method is based on the risk analysis of the area, experience from previous checks and the Oversight Board's findings in connection with the checks. Furthermore, prior to checking an

area not previously checked, the Oversight Board holds a start-up meeting with relevant DDIS employees in order to ensure an adequate professional and technical understanding of the area that will allow for the checks to be adjusted and adequately performed.

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

Prior to initiating its checks for a particular year, the Oversight Board will share its risk analysis and oversight plan with DDIS for the purpose of ensuring, among other things, openness about the Oversight Board's assessment of the situation at DDIS. The openness also allows DDIS to take into account the Oversight Board's checks in the organisation of its own internal controls, which contributes to the Oversight Board's checks and the internal controls collectively covering a larger part of DDIS's activities. Finally, the openness allows DDIS to dedicate sufficient resources to service the Oversight Board.

The Oversight Board performs verification by continuously mapping DDIS's system landscape at the server, component and application level in order to be able to make a complete risk assessment of all processes and systems of DDIS. Each year, the Oversight Board dedicates substantial resources to verify the data received from DDIS on its system landscape. The purpose of the verification is to ensure that the Oversight Board's checks are based on data from DDIS the correctness of which has been verified by the Oversight Board.

Furthermore, the Oversight Board has prepared a separate risk assessment and analysis specifically for the Oversight Board's checks in relation to DDIS under the indirect subject access request system, among other things for the purpose of ensuring that the Oversight Board's checks in connection with indirect subject access requests are effective and relevant. Against this background, the Oversight Board has initiated a development project for the purpose of securing more efficient system support for the Oversight Board's checks in 2019.

1.2 Oversight of DDIS in 2018

For the purpose of overseeing DDIS's compliance with the provisions of the DDIS Act when processing information about natural and legal persons resident in Denmark, the Oversight Board has carried out special checks in 2018 concerning DDIS's duty to inform (1.2.1) and carried out checks of DDIS's:

- electronic obtaining of raw data (SIGINT) (1.2.2),
- targeted electronic intelligence obtaining (SIGINT) (1.2.3),
- raw data searches (1.2.4),
- obtaining of human intelligence (HUMINT) (1.2.5),
- obtaining of imagery intelligence (IMINT) (1.2.6),
- electronic obtaining of non-communication (ELINT) (1.2.7),
- processing of information as foreign intelligence service (1.2.8),
- processing of information as military security service (1.2.9),
- disclosure of information to foreign partners (1.2.10),
- work stations (1.2.11),
- information security (1.2.12), and
- internal controls (1.2.13).

Summary of the Oversight Board's checks in 2018

In 2018, the Oversight Board came into possession of information indicating that in its checks of DDIS, the Oversight Board has been provided with incomplete or misleading information about one of DDIS's intelligence obtaining systems. Considering the seriousness of the matter, the Oversight Board initiated a special check of DDIS in order to clarify the correctness of the information and whether DDIS has adequately informed the Oversight Board. The check showed, see section 1.2.1, that DDIS has not complied with the duty to regularly inform the Oversight Board about all important issues concerning DDIS's processing of information about persons resident in Denmark, as prescribed by the DDIS Act, as DDIS has not informed the Oversight Board about a number of matters concerning one of DDIS's intelligence obtaining systems. The Oversight Board finds DDIS's failure to inform the Oversight Board unacceptable.

The Oversight Board's checks concerning DDIS's procurement of information about persons resident in Denmark verified, see sections 1.2.2-1.2.3 and sections 1.2.5-1.2.7, DDIS's general compliance with the legislation on procurement, including that DDIS applies a general criterion of legitimacy in its electronic intelligence obtaining.

However, the Oversight Board's check of DDIS's electronic obtaining of raw data, see section 1.2.2, identified risks that DDIS's obtaining via an inspected system is capable of being targeted at persons resident in Denmark in violation of DDIS legislation. In connection with its check, the Oversight Board has made a number of recommendations to DDIS concerning the mentioned risks, including initiated a closer dialogue with DDIS on the matter.

Furthermore, the check concerning DDIS's targeted electronic intelligence obtaining, see section 1.2.3, showed that in one case DDIS did not timely inform a foreign partner of the expiry of a court order obtained pursuant to section 3(3) of the DDIS Act.

The Oversight Board's check of DDIS's raw data searches, see section 1.2.4, showed that in 13 percent of the cases sampled DDIS had performed raw data searches in violation of DDIS legislation. In the Oversight Board's assessment, the said raw data searches in violation of DDIS legislation were in all cases in the nature of negligent acts, including 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.

In the Oversight Board's opinion, DDIS still has a challenge when performing raw data searches in relation to its compliance with the legislation on procurement of information about persons resident in Denmark. The Oversight Board notes, however, that the error rate has been reduced in comparison to the result of the checks of the area in 2017 and that DDIS has devoted considerable attention to reducing the number of errors, including by intensifying its internal controls within the area and strengthening and targeting employee training.

The Oversight Board's checks of DDIS's internal processing of information about persons resident in Denmark, including the provision on legal political activity, verified, see sections 1.2.8-1.2.9 and section 1.2.11, DDIS's general compliance with the legislation in this regard. However, the check of selected work stations, see section 1.2.11, showed that in two cases information about persons resident in Denmark had not been stored in accordance with DDIS's internal guidelines in this

regard. Furthermore, on the basis of the check of DDIS's processing of information as military security service, see section 1.2.9, DDIS has informed the Oversight Board that specific information about a number of persons resident in Denmark would be erased as the information was no longer relevant to process for the performance of DDIS's activities as military security service.

The Oversight Board's checks of DDIS's disclosure of information to foreign partners, see section 1.2.10, verified DDIS's compliance in all cases with the legislation on disclosure of information.

The Oversight Board's checks of DDIS's information security, see section 1.2.12, showed that a realistic timetable has been set for DDIS's implementation of the ISO 27001 standard, that sufficient full-time resources are allocated to driving DDIS's implementation and subsequent management of ISO 27001 and that DDIS is allocating the required resources to the project. Furthermore, the check showed that DDIS is on a par with comparable organisations within the majority of the areas in the ISO 27001 standard. The Oversight Board finds it important, however, that DDIS follows the Oversight Board's recommendations in order to ensure full implementation of the ISO 27001 standard.

The check of DDIS's internal controls, see section 1.2.13, showed that at the general level DDIS's organisation and performance of the internal controls were satisfactory.

1.2.1 Special checks concerning DDIS's duty to inform

The Oversight Board regularly and of its own motion checks DDIS's compliance with the provisions of sections 3-8 of the DDIS Act and statutory regulations issued thereunder. In order to ensure that the Oversight Board has the best possibilities of planning its checks, it follows from the explanatory notes to the DDIS Bill that DDIS must keep the Oversight Board informed of all important issues concerning DDIS's processing of information about natural and legal persons resident in Denmark.

In 2018, the Oversight Board came into possession of information indicating that in its checks of DDIS, the Oversight Board has been provided with incomplete or misleading information about one of DDIS's intelligence obtaining systems.

Considering the seriousness of the matter, the Oversight Board initiated a special check of DDIS in order to clarify the correctness of the information and whether DDIS has adequately informed the Oversight Board.

Based on the new information available to the Oversight Board, the Oversight Board also revised its already scheduled checks in 2018 of the intelligence obtaining system in question in order to check whether the system fulfils the conditions of the DDIS Act for obtaining of information. The results of these checks are described in more detail in section 1.2.2.

For the purpose of overseeing DDIS's compliance with its duty to inform, the Oversight Board carried out inspections of DDIS which included, among other things, interviewing selected DDIS employees. Based on the check, the Oversight Board requested DDIS to provide a detailed account of a number of matters.

! **Comments by the Oversight Board**

The Oversight Board's special check concerning DDIS's duty to inform showed that DDIS has not complied with the duty to regularly inform the Oversight Board about all important issues concerning DDIS's processing of information about persons resident in Denmark, as prescribed by the DDIS Act, as DDIS has not informed the Oversight Board about a number of matters concerning one of DDIS's intelligence obtaining systems.

In the Oversight Board's opinion, DDIS's information about the matters in question would have been of essential importance to the Oversight Board's planning and performance of its past checks of the intelligence obtaining system in question. Thus, DDIS should already in connection with the first check have informed the Oversight Board about these matters, which it did not. The Oversight Board finds DDIS's failure to inform the Oversight Board unacceptable.

1.2.2 Checks of DDIS's electronic obtaining of raw data (SIGINT)

In its electronic intelligence obtaining – also called Signal Intelligence (SIGINT) – DDIS collects very large amounts of non-processed data, also known as raw data, which are characterised by the fact that until processed, it is not possible to determine what information is contained in these data.

DDIS's compliance with intelligence obtaining legislation means in relation to electronic obtaining of raw data that such obtaining must be for legitimate reasons as regards DDIS's intelligence-related activities directed at conditions abroad and that any intelligence which concerns persons resident in Denmark is received by DDIS only by chance.

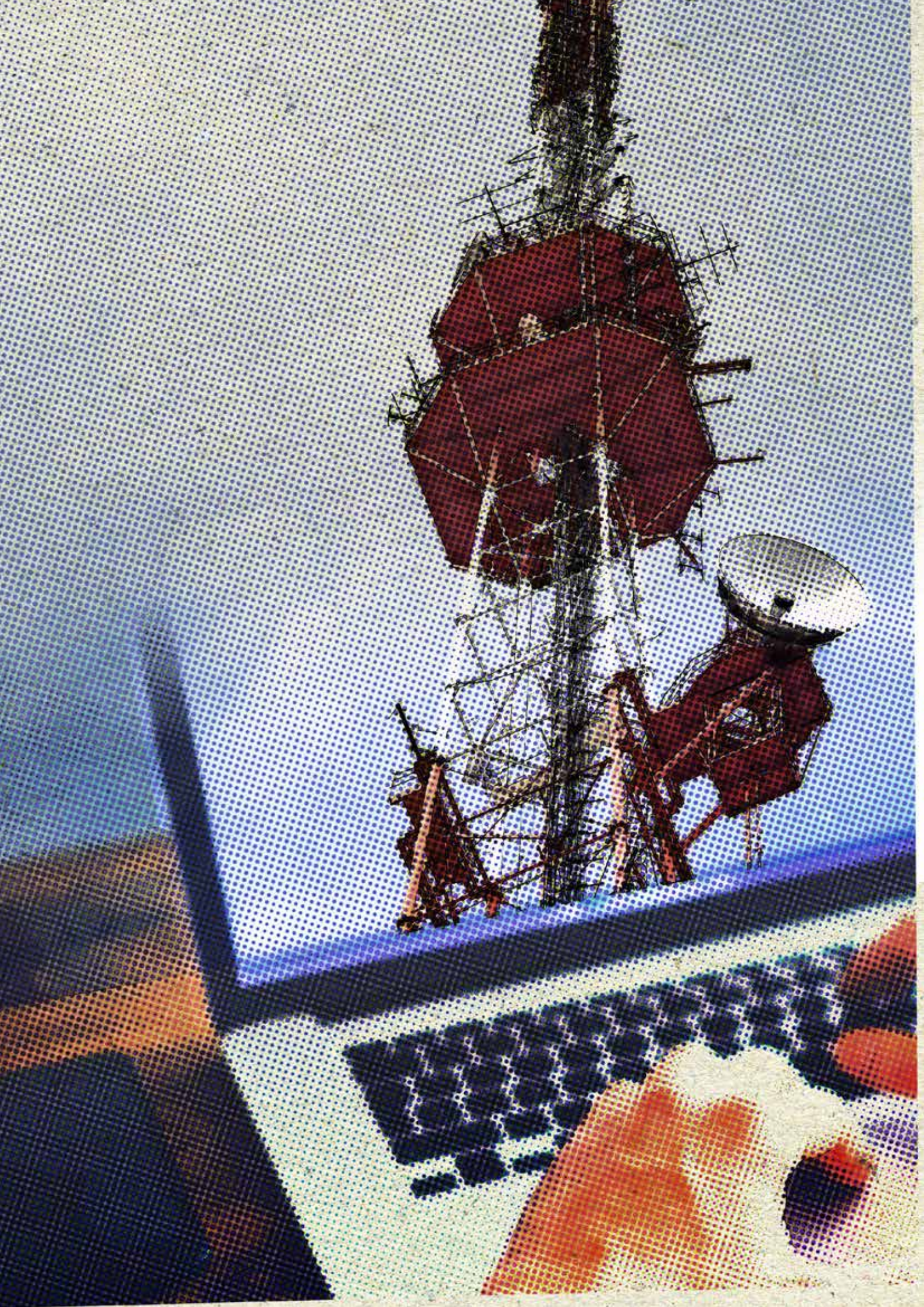
For the purpose of its compliance check, in 2018 the Oversight Board carried out an inspection at DDIS's premises where a specified intelligence obtaining system was inspected. At the inspection, DDIS answered questions from the Oversight Board concerning the technical set-up of the system and DDIS's information handling procedures concerning information about persons resident in Denmark.

Furthermore, in 2018 the Oversight Board had discussions with DDIS about its use of a number of additional intelligence obtaining systems.

! **Comments by the Oversight Board**

The Oversight Board's checks concerning DDIS's obtaining of electronic raw data verified that in the organisation thereof DDIS applies a general criterion of legitimacy and that as a general rule information concerning persons resident in Denmark is received by DDIS only by chance.

However, the Oversight Board's check identified risks that DDIS's obtaining via the inspected system is capable of being targeted at persons resident in Denmark in violation of DDIS legislation. In connection with its check, the Oversight Board has made a number of recommendations to DDIS concerning the mentioned risks, including initiated a closer dialogue with DDIS on the matter.



1.2.3 Checks of DDIS's targeted electronic intelligence obtaining (SIGINT)

DDIS carries out targeted electronic intelligence obtaining based on a number of different selectors, e.g. telephone numbers and email addresses.

DDIS's compliance with intelligence obtaining legislation means in relation to electronic intelligence obtaining targeted 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 the Danish Security and Intelligence Service (*DSIS*) based on a court order obtained by DSIS.

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.

For the purpose of its compliance check, in 2018 the Oversight Board performed random checks concerning Danish-related selectors incorporating DDIS's targeted electronic intelligence obtaining systems as well as selectors belonging to all persons in respect of whom the Oversight Board has obtained a court order pursuant to section 3(3) of the DDIS Act to obtain data by interception of communications. Furthermore, the Oversight Board checked that DDIS ceased the obtaining of information about persons resident in Denmark when the court order against the relevant persons expired. The Oversight Board checked logs for the selectors sampled.

! **Comments by the Oversight Board**
The Oversight Board's regular random checks concerning DDIS's targeted electronic intelligence obtaining, including pursuant to section 3(3) of the DDIS Act, verified DDIS's general compliance with the legislation on procurement but in one case DDIS did not timely inform a foreign partner about the expiry of a court order obtained pursuant to section 3(3) of the DDIS Act.

1.2.4 Checks of DDIS's raw data searches

It follows from the principle in section 3 of the DDIS Act on procurement of information that 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 subsection (3) of the provision. In addition, if so requested by the Danish Security and Intelligence Service (*DSIS*), DDIS will be allowed to make such searches on the basis of DSIS legislation.

For the purpose of its compliance check, in 2018 the Oversight Board performed random checks of DDIS's raw data searches, including among other things searches on selectors used in targeted electronic intelligence obtaining activities pursuant to section 3(3) of the DDIS Act. Furthermore, the Oversight Board checked that DDIS had not continued its intelligence obtaining by searching in raw data about persons resident in Denmark after the court order against the relevant persons had expired.

Based on logs from DDIS's systems used for raw data searches, the Oversight Board initially subjected DDIS's 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 as 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, the Oversight Board regularly performed random checks and, based on a specific assessment, requested DDIS's clarifying comments.

The Oversight Board has also engaged in an ongoing dialogue with DDIS about DDIS's internal controls within the area, including securing the right underlying data basis for both the Oversight Board's and DDIS's checks and methods for the calculation of error rates.

The Oversight Board's error rate is calculated on the basis of the number of times DDIS has performed raw data searches in violation of DDIS legislation among the searches sampled by the Oversight Board in 2018.

! **Comments by the Oversight Board**

The Oversight Board's regular checks concerning DDIS's raw data searches showed that in 13 percent of the cases sampled DDIS had performed raw data searches in violation of DDIS legislation as DDIS had performed such data searches of its own motion although the result may be expected to be mainly information about persons resident in Denmark and without DDIS having obtained a court order for such searches, see section 3(3) of the DDIS Act.

In the Oversight Board's assessment, the said raw data searches in violation of DDIS legislation were in all cases in the nature of negligent acts, including 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.

In the Oversight Board's opinion, DDIS still has a challenge when performing raw data searches in relation to its compliance with the legislation on procurement of information about persons resident in Denmark. The Oversight Board notes, however, that the error rate has been reduced in comparison to the result of the checks of the area in 2017 and that DDIS has devoted considerable attention to reducing the number of errors, including by intensifying its internal controls within the area and strengthening and targeting employee training.

In addition to the said searches in violation of DDIS legislation, the Oversight Board has in 2018 assessed the statutory basis for a practice between the Danish Defence Intelligence Service (*DDIS*)

In the Oversight Board's opinion, DDIS still has a challenge when performing raw data searches in relation to its compliance with the legislation on procurement of information about persons resident in Denmark. The Oversight Board notes, however, that the error rate has been reduced in comparison to the result of the checks of the area in 2017 [...]

and the Danish Security and Intelligence Service (*DSIS*) where DSIS did not obtain a court order to obtain data by interception of communications when requesting DDIS to perform raw data searches. On 28 June 2018, the Oversight Board informed DSIS and DDIS that in the Oversight Board's view, the practice in question was not warranted under the DSIS Act or the DDIS Act. Based on the Oversight Board's assessment, DSIS and DDIS decided on 4 July 2018 to end the practice in question. The Oversight Board's investigation of the matter is described in more detail in section 2 of this annual report.

1.2.5 Checks of DDIS's physical obtaining of human intelligence (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).

DDIS's compliance with intelligence obtaining legislation requires in relation to human intelligence that, as a general rule, intelligence concerning already known and identified persons resident in Denmark may be received by DDIS only by chance, unless the data subject falls within the scope of section 3(3) of the DDIS Act, or unless the human intelligence is obtained at the request of the Danish Security and Intelligence Service (*DSIS*).

For the purpose of checking this aspect, in 2018 the Oversight Board reviewed specific human intelligence about persons resident in Denmark.

! **Comments by the Oversight Board**
The Oversight Board's check of DDIS's obtaining of human intelligence verified DDIS's compliance with the legislation regarding procurement of information.

1.2.6 Checks of DDIS's obtaining of imagery intelligence (IMINT)

DDIS procures and analyses images – also called Imagery Intelligence (IMINT) – from various sensors which generate images of objects or areas by means of optical, electronic, digital or via other visualisation means.

DDIS's compliance with the legislation regarding procurement of information means in relation to imagery intelligence that, as a general rule, intelligence concerning persons resident in Denmark may be received by DDIS only by chance, unless the data subject falls within the scope of section 3(3) of the DDIS Act, or unless the imagery intelligence is obtained at the request of the Danish Security and Intelligence Service (*DSIS*).

DDIS's procurement of imagery intelligence was in 2018 checked by engaging in discussions with the members of DDIS's staff responsible for this area and with DDIS's legal department.

! **Comments by the Oversight Board**
The Oversight Board's check of DDIS's imagery intelligence verified DDIS's compliance with the legislation regarding procurement of information.

1.2.7 Checks of DDIS's electronic obtaining of non-communication (ELINT)

As part of DDIS's electronic intelligence obtaining (SIGINT), DDIS obtains non-communication, e.g. radar signals – also known as Electronic Intelligence (ELINT).

DDIS's compliance with the legislation regarding procurement of information means in relation to ELINT that, as a general rule, intelligence concerning persons resident in Denmark may be received by DDIS only by chance, unless the data subject falls within the scope of section 3(3) of the DDIS Act, or unless the intelligence is obtained at the request of the Danish Security and Intelligence Service (*DSIS*).

DDIS's procurement of information through the obtaining of non-communication was in 2018 checked by engaging in discussions with the members of DDIS's staff responsible for this area and with DDIS's legal department.

! **Comments by the Oversight Board**
The Oversight Board's check of DDIS's obtaining of non-communication verified DDIS's compliance with the legislation regarding procurement of information.

1.2.8 Checks of DDIS's processing of information as foreign intelligence service

DDIS processes, including stores, information about persons resident in Denmark as part of DDIS's performance of its activities as foreign intelligence service.

In 2018, the Oversight Board regularly drew random samples from DDIS's electronic analysis and documentation systems as well as other systems concerning information on persons resident in Denmark.

! **Comments by the Oversight Board**
The Oversight Board's checks of DDIS's processing of information as part of DDIS's performance of its activities as foreign intelligence service verified DDIS's compliance with the legislation on procurement, internal processing and disclosure of information and on legal political activity.

1.2.9 Checks of DDIS's processing of information as military security service

DDIS performs its activities as military security service within the area of the Danish Ministry of Defence. The role as military security service includes a number of tasks, including vetting of staff to the Danish military, checking the general security conditions on the premises of the Danish military and investigating specific cases concerning security threats in the Danish military.

In 2018, the Danish Oversight Board performed a random check of information being processed by DDIS in connection with DDIS's performance of its activities as military security service.

! **Comments by the Oversight Board**

The Oversight Board's checks of DDIS's processing of information as part of DDIS's performance of its activities as military security service verified DDIS's compliance with the legislation on procurement, internal processing and disclosure of information and on legal political activity.

On the basis of the check, DDIS has informed the Oversight Board that specific information about a number of persons resident in Denmark would be erased as the information was no longer relevant to process for the performance of DDIS's activities as military security service.

1.2.10 Checks of DDIS's disclosure of information to foreign 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's analysis and, thereby, of a significant part of the products which DDIS prepares for its customers.

DDIS's compliance with the legislation regarding disclosure of information means in relation to foreign partners that information about persons resident in Denmark may be disclosed by DDIS only where the conditions of disclosure in section 7(2) and (3) of the DDIS Act are satisfied. Moreover, DDIS has established various internal rules for disclosure of information about persons resident in Denmark, including that legal approval must have been obtained before disclosure to a partner.

In 2018, the Oversight Board performed regular random checks of DDIS's disclosure to foreign partners of information about persons resident in Denmark.

! **Comments by the Oversight Board**

The Oversight Board's checks of DDIS's disclosure of information to foreign partners verified DDIS's compliance in all cases with the legislation on disclosure of information.

> The Oversight Board's checks of DDIS's processing of information as part of DDIS's performance of its activities as foreign intelligence service verified DDIS's compliance with the legislation on procurement, internal processing and disclosure of information and on legal political activity.

1.2.11 Checks of DDIS work stations

In 2018, the Oversight Board performed a check of a number of staff work stations, focusing on the staff's processing of information about persons resident in Denmark, including their knowledge of the rules in this area.

Within two DDIS sections, the Oversight Board checked a number of randomly chosen work stations, including their drives, email system folders, external storage devices and documents in hard copy and, similarly, DDIS carried out a supplementary check of central internal shared drives and mailboxes. In connection with the random checks performed of the information held on the work stations, the Oversight Board asked questions to the individual staff members in question about their knowledge of the legislation on processing of information about persons resident in Denmark.

! **Comments by the Oversight Board**

A check of specific work stations verified all staff members' compliance with the DDIS Act in their processing of information about persons resident in Denmark and their general awareness that such information must be processed in compliance with the DDIS Act and DDIS's internal guidelines, including that information must be erased when it is no longer relevant to process such information there.

However, the check showed that in two cases staff were processing information about persons resident in Denmark in violation of DDIS's internal guidelines as the staff members in question held information which was no longer relevant to process there.

In addition, in connection with its check, the Oversight Board provided DDIS with general recommendations concerning certain issues which DDIS should focus on in particular in relation to securing that information about persons resident in Denmark is processed in compliance with the DDIS Act and DDIS's internal guidelines.

1.2.12 Checks of DDIS's information security

In 2018, the Oversight Board has made an extensive analysis of DDIS's implementation of the ISO 27001 standard. In that connection, the Oversight Board examined documentation that had been provided and interviewed key employees.

On the basis of the analysis, the Oversight Board has made a number of recommendations to DDIS and requested DDIS for half-yearly status meetings in relation to the implementation of the ISO 27001 standard in 2019.

! **Comments by the Oversight Board**

The Oversight Board's analysis of DDIS's implementation of the ISO 27001 standard showed that a realistic timetable has been set for DDIS's implementation project, that sufficient full-time resources have been allocated to driving DDIS's implementation and subsequent management of ISO 27001 and that DDIS allocates the required resources to the project.

Furthermore, the analysis showed that DDIS is on a par with comparable organisations within the majority of the areas in the ISO 27001 standard. The Oversight Board finds it important, however,

that DDIS follows the Oversight Board's recommendations in order to ensure full implementation of the ISO 27001 standard.

1.2.13 Checks of DDIS's internal controls

In the course of its oversight of DDIS in 2018, the Oversight Board performed a check of DDIS's internal controls. The check comprised all internal controls carried out by DDIS in 2018 and DDIS's planning of the same for 2019, and was carried out by reviewing documentation provided and engaging in discussions with DDIS

DDIS has regularly updated the Oversight Board on its internal controls of specific intelligence obtaining systems. Moreover, DDIS has provided a detailed description of how its internal controls are organised, including by submitting a risk analysis concerning compliance with statutory requirements.

! **Comments by the Oversight Board**
The Oversight Board's check of DDIS's internal controls showed that at the general level DDIS's organisation and performance of the internal controls were satisfactory.

1.3 Follow-up on the Oversight Board's checks of DDIS in 2017

Each year, the Oversight Board checks that DDIS has initiated the measures which DDIS has stated that it would on the basis of the Oversight Board's checks in the preceding year.

In the Oversight Board's annual report on its activities concerning DDIS for 2017 (section 3.1.2), the Oversight Board noted that DDIS should have erased information about five persons resident in Denmark, and DDIS agreed.

The Oversight Board checked the personal information in question again with a view to determining whether the information had subsequently been erased. The check showed that in one case DDIS had not erased as provided by section 6a(1) and (2) of the DDIS Act, cf. section 4. DDIS subsequently erased the information.

The check showed that in one case DDIS had not erased as provided by section 6a(1) and (2) of the DDIS Act, cf. section 4. DDIS subsequently erased the information.

In relation to the Oversight Board's other checks as described in the Oversight Board's annual report on its activities concerning DDIS for 2017 (section 3.1), the checks performed in 2018 verified that DDIS had taken the necessary measures which were recommended by the Oversight Board or which DDIS had informed the Oversight Board that it would implement.

1.4 DDIS's briefing of the Oversight Board

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

- DDIS's 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 section 6(1) and (2),
- all important issues concerning DDIS's 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.

The Oversight Board was kept up to date on DDIS's use of the provisions. On the basis of the updates provided by DDIS, the Oversight Board initiated further discussions with DDIS about the scope of the duty of information pursuant to section 6(3) of the DDIS Act.

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

1.5.1 Processing of requests by the Oversight Board

When a natural or legal person resident in Denmark requests the Oversight Board to check if DDIS is processing personal information about them in violation of DDIS legislation, the Oversight Board will examine the matter at DDIS's premises where the Oversight Board has access to any information and all material of importance to the Oversight Board'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 the Oversight Board will endeavour to identify all information which DDIS is processing about a data subject who has submitted an indirect subject access request. With a view to providing the greatest possible assurance that all information about the data subject has been identified, the Oversight Board will subsequently ask DDIS to check if it is processing further information about the data subject.

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

If special circumstances weigh in favour of doing so, the Oversight Board 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 personal information about them. Where the Oversight Board receives a subject access request, the Oversight Board will find out which personal information, if any, DDIS is processing about the data subject and will also obtain DDIS's comments before the Oversight Board makes a decision under the relevant provision. For indirect subject access requests, the Oversight Board will check of its own motion whether special circumstances weigh in favour of ordering DDIS to grant full or partial access to the personal information in question.

1.5.2 Number of requests and processing time

In 2018, the Oversight Board received subject access requests from 125 natural or legal persons, asking the Oversight Board to check if DDIS was processing personal information about them in violation of DDIS legislation. In five cases, the Oversight Board found this to be the case. The Oversight Board did not find that special circumstances weighed in favour of ordering DDIS to grant the data subjects in question full or partial access to the personal information as mentioned in section 9(1) of the DDIS Act.

The average processing time for the processed requests was 107 days, 22 days of which were DDIS's processing time. Compared with 2017, the average processing time increased by 66 days.

The Oversight Board will endeavour to answer subject access requests as quickly as possible, but, as already mentioned, this may be a quite resource-intensive and complicated process and the Oversight Board must present the results to DDIS before making a decision in the matter at a monthly meeting. Given the extraordinary increase in 2018 in the number of requests compared to previous years, the processing time is not expected to increase in 2019.

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

2 Practice concerning DSIS's requests to DDIS for raw data searches

The activities of the Danish Security and Intelligence Service (*DSIS*) and DDIS have different objectives, but in some cases the interest areas of DSIS and DDIS may overlap, for instance when persons resident in Denmark engage in activities abroad which make them a potential national security threat. It is thus a requirement of DSIS and DDIS legislation that the two intelligence services work closely together and that DDIS provides technical assistance to DSIS, where necessary to satisfy a special need.

DDIS has at its disposal intelligence obtaining systems that may capture specific information flows from which DDIS can obtain very large amounts of information (several hundred million communications per year), also referred to as raw data. As DDIS's intelligence-related activities are directed at conditions abroad, the dominant part of the obtained raw data concerns foreign matters, but such data may also contain information about persons resident in Denmark.

In its role as national intelligence service, DSIS may wish to access information about persons resident in Denmark obtained by DDIS as raw data in connection with DDIS's intelligence activities directed at conditions abroad. DDIS will not be aware of the contents of the relevant raw data as such contents will not become known to DDIS until the data are processed.

When DSIS requests DDIS to procure information, such request will be based on DSIS legislation. In all cases, DSIS will obtain a court order when requesting DDIS for assistance for future intelligence obtaining, e.g. tapping of communication abroad.

However, it has been an established practice between the two intelligence services that DSIS could request DDIS to perform a raw data search without a court order having been obtained as, in the assessment of DSIS, searches in raw data already obtained did not require a court order.

2.1 About the Oversight Board's powers in respect of the intelligence services' interception of communications

According to section 6 of the DSIS Act, the provisions of the Danish Administration of Justice Act (*retsplejeloven*) apply when DSIS obtains information by intrusive measures such as interception of communications. Thus, like the other parts of the police, DSIS must as a general rule obtain a court order beforehand.

DDIS's activities, in contrast, are not governed by the Administration of Justice Act, including the provisions on court orders. This is because DDIS's activities are directed at conditions abroad and therefore must not, as a general rule, be directed at persons resident in Denmark. An exception to this rule is section 3(3) of the DDIS Act, which provides that in special cases DDIS may intercept communications in respect of persons resident in Denmark and where at the same time DDIS is subject to a requirement to obtain a court order.

It is not the Oversight Board's role to check DSIS's use of intrusive measures as section 6 of the DSIS Act does not fall within the scope of the Oversight Board's oversight activities, see section 18 of the DSIS Act.

In relation to DDIS, the Oversight Board checks all intelligence obtained which is not directed at persons resident in Denmark as DDIS must not, as a general rule, perform targeted intelligence obtaining directed at persons resident in Denmark, unless a special basis exists therefor. By way of example, such special basis may be a court order obtained by DDIS on the basis of section 3(3) of the DDIS Act or a request from DSIS.

2.2 About the basis for the Oversight Board's check

Since its setting up in 2014, the Oversight Board has regularly discussed the framework for the cooperation between DDIS and DSIS with the two intelligence services. The Oversight Board was thus informed about the practice where DSIS would only obtain a court order for tapping or prospective continuous raw data searches in the nature of tapping.

At the time, the Oversight Board did not have any reason to question the lawfulness of this practice as it was well-established between the two intelligence services and had existed prior to the adoption of the DSIS Act and the DDIS Act.

With the passing of Act No. 1571 of 15 December 2015 (Strengthening the effort to combat activities abroad which may involve a terrorist threat against Denmark and Danish interests), DDIS was authorised under section 3(3) of the DDIS Act in special cases to intercept communications in respect of persons resident in Denmark on the basis of a court order.

As, with the adoption of section 3(3) of the DDIS Act, DDIS became subject to a duty to obtain a court order, this raised the question in the Oversight Board's view whether the new legislation had a bearing on the existing interpretation of DSIS and DDIS legislation as the amendment could indicate that raw data searches also constitute interception of communications requiring a court order.

As the Oversight Board does not, as mentioned above, have competence to check DSIS's use of intrusive measures under section 6 of the DSIS Act, it was necessary to consider whether the Oversight Board was competent to give an opinion on whether DSIS was under an obligation to obtain a court order prior to DDIS's raw data searches on behalf of DSIS.

The Oversight Board had initial discussions with DSIS and DDIS during the course of 2017, after which, in February 2018, the Oversight Board undertook a written consultation of DSIS for the purpose of final confirmation that the Oversight Board's understanding of the practice was correct.

The Oversight Board then decided to present its assessment of the practice in question to the two intelligence services for their comments, after which the Oversight Board would inform the Danish Ministry of Justice and the Danish Ministry of Defence in order for the ministries to decide whether the practice in question was legal.

The Oversight Board's assessment was sent to DSIS and DDIS on 28 June 2018.

2.3 The Oversight Board's assessment of the intelligence services' practice

As described above, it is established in section 6 of the DSIS Act that DSIS's use of intrusive measures is subject to the provisions of the Administration of Justice Act. Raw data searches are an activity that is only performed by DDIS and, as a result, raw data searches are only discussed in the legislative history of the DDIS Act. Whether raw data searches constitute interception of communications requiring a court order should therefore, in the Oversight Board's opinion, be answered by an interpretation of the DDIS Act.

As DDIS's activities, as mentioned, are not governed by the Administration of Justice Act, the DDIS Act does not specifically address the issue of whether raw data searches constitute interception of communications.

By Act No. 1571 of 15 December 2015 (Strengthening the effort to combat activities abroad which may involve a terrorist threat against Denmark and Danish interests), DDIS was with the new section 3(3) of the DDIS Act granted special authority to perform targeted intelligence obtaining directed at persons resident in Denmark, provided that such persons are not physically located in Denmark and there are specific reasons to believe that the persons in question are engaging in activities that may involve or increase a threat of terrorism against Denmark and Danish interests. According to the second sentence of section 3(3) of the DDIS Act, DDIS must obtain a court order if the intelligence obtaining activities involve interception of communications.

It follows from section 7 of the commented public consultation list for the Bill to Act No. 1571 that the Danish Ministry of Defence has noted that DDIS, *after having obtained a court order*, may perform raw data searches, provided that the conditions in section 3(3) of the DDIS Act are satisfied.

Furthermore, it can be seen from the committee review of the Bill that the Defence Committee asked the following question to the Minister of Defence:

> "*Will DDIS be entitled under the Bill to perform targeted searches for information in raw data about a natural person resident in Denmark if the conditions in section 3(3) are satisfied without this constituting interception of communications and thus not requiring a court order?*"

The Minister of Defence replied as follows:

> "*As stated in section 7 of the commented consultation list, DDIS may, after having obtained a court order, perform targeted raw data searches concerning a specific person in order to find any information about the person in question in such data, provided that the conditions in section 3(3) are satisfied*."

The Oversight Board understands the comments of the Danish Ministry of Defence and the reply of the Minister of Defence to the committee question to mean that DDIS's raw data searches constitute interception of communications requiring a court order, see section 3(3) of the DDIS Act.

If the comments of the Danish Ministry of Defence and the reply of the Minister of Defence to the committee question is not to be understood as meaning that DDIS's raw data searches constitute interception of communications requiring a court order, see section 3(3) of the DDIS Act, the Oversight Board is of the opinion that the considerations underlying the requirement to obtain a court order in connection with raw data searches under section 3(3) of the DDIS Act would also apply to DSIS making a similar raw data search.

In the overall opinion of the Oversight Board, the practice established by the two intelligence services falls outside the scope of the framework provided by statute as the obtaining of information at the request of DSIS is based on DSIS legislation, and as DSIS, if it were itself to make a corresponding raw data search, would only be able to do so on the basis of a court order pursuant to the provisions of the Administration of Justice Act, see section 6 of the DSIS Act.

2.4 DSIS and DDIS's response to the Oversight Board's assessment

On 28 June 2018, the Oversight Board informed DSIS and DDIS that in the opinion of the Oversight Board, the practice in question falls outside the scope of the DSIS Act and the DDIS Act.

Based on the Oversight Board's assessment, DSIS and DDIS decided on 4 July 2018 to suspend the practice in question until the legal situation had been fully clarified.

On 22 January 2019, the Oversight Board received comments from DSIS and DDIS concerning the two intelligence services' assessment of the existing practice.

DSIS stated in that connection that it had so far been of the view that a request for searches in raw data already obtained did not require a court order. However, in light of the Oversight Board's comments, DSIS will in future obtain a court order pursuant to the provisions of the Administration of Justice Act before requesting DDIS to perform a raw data search concerning persons resident in Denmark as DSIS does not wish for a situation where it could be called into question whether DSIS has the authority required for its activities.

DDIS noted in this connection that any assistance provided in the obtaining of information at the request of DSIS is based on DSIS legislation, and that DSIS had been of the view that a request for searches in raw data already obtained did not require a court order. DDIS further noted that the Oversight Board has been aware of the practice in question since 2014.

In connection with its checks in 2018 of DDIS's raw data searches directed at persons resident in Denmark, the Oversight Board has noted that in 23 percent of the cases sampled searches have been performed on the basis of a request from DSIS without, according to the information provided in the request, a court order having been obtained.

In the Oversight Board's opinion, DSIS and DDIS have not subsequent to the decision of the two intelligence services of 4 July 2018 performed raw data searches against persons resident in Denmark without a court order.

As subsequent to the Oversight Board's notice of 28 June 2018 DSIS and DDIS have arranged their practice in accordance with the Oversight Board's interpretation of the DSIS Act and the DDIS Act, there has been no need in the opinion of the Oversight Board to involve the Danish Ministry of Justice and the Danish Ministry of Defence.

Going forward, the Oversight Board will check that the cooperation between DSIS and DDIS about raw data searches is in compliance with the framework which the two intelligence services on the basis of the Oversight Board's assessment have accepted to comply with.

3 Publicity in 2018

DDIS's activities and the framework for such activities set by the Danish Parliament and Government, including the Oversight Board's oversight, have been the subject of regular comment by the Danish media.

The Oversight Board would like to contribute as much as possible to the press and thus the public getting the best possible insight into the Oversight Board's oversight of DDIS, without compromising the need for secrecy following from DDIS's special function.

The Oversight Board makes sure that it is updated on the public debate about its oversight of DDIS in order to assess whether it can contribute to a better understanding of its role, oversight options as well as the results of its oversight.

Early 2018, the Oversight Board's checks of DDIS work stations were mentioned in a newspaper article as, according to the Oversight Board's annual report on its activities concerning DDIS for 2016, a majority of the staff that had been subjected to checking had informed the Oversight Board that they had erased information from their work stations before the check. In order to contribute to the proper public understanding of the results of the check, the Chairman of the Oversight Board expressed his view in the article, explaining that, in the Oversight Board's opinion, it was not wrong for information to be erased from the work stations as one of the purposes of the check in question had been to check the effectiveness of DDIS's information to its staff about applicable personal data processing rules.

The Oversight Board's annual report on its activities concerning DDIS for 2017, which was published in June 2018, also gave rise to media coverage. The coverage focused in particular on the results of the Oversight Board's checks of DDIS's raw data searches. DDIS responded to the coverage and published, among other things, information about its internal controls where the error rate differed from the results of the Oversight Board's checks. The Oversight Board finds it positive that DDIS provides the greatest possible degree of transparency with respect to its internal controls as well as the other security measures put in place by DDIS in relation to the citizens.

1. About the 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's 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's 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 information collection. 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's 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 Danish Ministry of Defence.

The legal framework for DDIS's activities is essentially laid down in the Danish Defence Intelligence Service (*DDIS*) (*lov om Forsvarets Efterretningstjeneste (FE)*) (the "DDIS Act"). The DDIS Act governs, among other things, DDIS's responsibilities and the procurement, internal processing and disclosure of personal information.

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

DDIS's 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 (*lov om Center for Cybersikkerhed*) (the "CFCS Act"), which entered into force on 1 July 2014. Under this Act, the Oversight Board must also oversee that the processing of the Centre for Cyber Security (the "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.

> In the context of DDIS's 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.

2. The Danish Intelligence Oversight Board

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

The Oversight Board 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.

The Oversight Board is composed of five members who are appointed by the Minister of Justice following consultation with the Minister of Defence. The chairman, 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.

The members are:

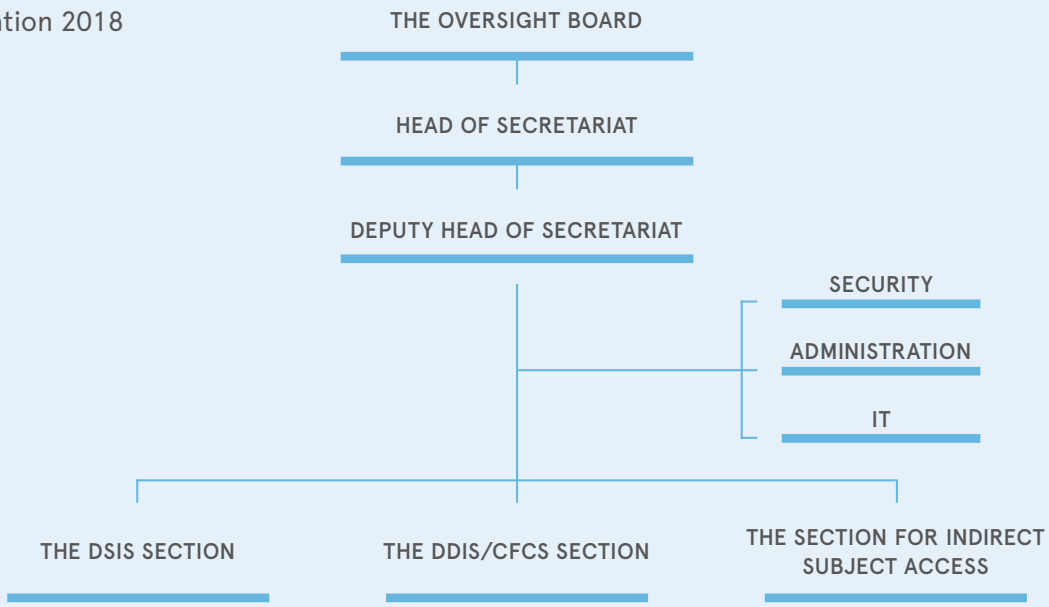
- Michael Kistrup, High Court Judge, the Danish Eastern High Court (chairman)
- Professor Jørgen Grønnegård Christensen, Aarhus University
- Erik Jacobsen, Chairman of the Board of Directors, Roskilde University
- Pernille Christensen, Legal Chief, Local Government Denmark
- Professor Henrik Udsen, Copenhagen University

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 the Oversight Board was set up in October 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.

The Oversight Board is supported by a secretariat which is subject solely to the instructions from the Oversight Board in the performance of its duties. The Oversight Board recruits its own secretariat staff and also decides which educational and other qualifications the relevant candidates must have. At the end of 2018, the secretariat consisted of a head of secretariat, who is in charge of the day-to-day management of the secretariat, a deputy, three lawyers, an IT consultant and an administrative employee.

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

Organisation 2018



2.1 The Oversight Board's duties in relation to DDIS

The DDIS Act provides that upon receipt of a complaint or of its own motion, the Oversight Board must oversee 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. The Oversight Board must oversee DDIS's compliance with the provisions of the Act concerning:

- procurement of information, including collection and obtaining of information,
- internal processing of information, including time limits for erasure of information,
- disclosure of information, including to 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 Oversight Board must oversee by way of compliance checks that DDIS processes information about natural and legal persons resident in Denmark in compliance with DDIS legislation, and the Oversight Board thus has no mandate to oversee whether DDIS carries out its activities in an appropriate manner, including how DDIS's resources are prioritised, as these aspects are to be determined by DDIS itself based on an intelligence assessment.

The Oversight Board itself decides the intensity of oversight, including whether to perform full oversight or random checks, which aspects of the activities are to be given special priority and

the extent to which the Oversight Board wishes to raise a matter of its own motion. No specific guidelines have been provided for the Oversight Board's performance of its oversight functions, except that – according to the legislative history of the Act – the Oversight Board 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, the Oversight Board will also investigate whether DDIS is processing information about the data subject in violation of DDIS legislation. The Oversight Board will verify that this is not the case and then notify the person in question (*the indirect subject access request system*). According to the legislative history of the Act, it must only be possible to infer from the Oversight Board'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 The Oversight Board's access to information held by DDIS

The Oversight Board may require DDIS to provide any information and all material of importance to the Oversight Board's activities, and the Oversight Board is entitled at any time to access any premises where the information being processed may be accessed or where technical facilities are being used. The Oversight Board may furthermore require DDIS to provide written statements on factual and legal matters of importance to the Oversight Board'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 the Oversight Board for the Oversight Board to make its own searches in DDIS's IT systems.

The Oversight Board may require DDIS to provide any information and all material of importance to the Oversight Board's activities, and the Oversight Board is entitled at any time to access any premises where the information being processed may be accessed or where technical facilities are being used.

2.3 Responses available to the Oversight Board

The Oversight Board generally has no authority to order DDIS to implement specific measures in relation to data processing. However, the Oversight Board may issue statements to DDIS providing its opinion on matters such as whether DDIS's complies with the rules concerning processing of information. If DDIS decides not to comply with a recommendation issued by the Oversight Board in exceptional cases, DDIS must notify the Oversight Board 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 the Oversight Board in exceptional cases, the Government must notify the Parliamentary Intelligence Services Committee.

The Oversight Board must inform the Minister of Defence of any matters which the Minister ought to know in the opinion of the Oversight Board.

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

Each year, the Oversight Board 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 the Oversight Board has decided to examine more closely. Similarly, the Oversight Board 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 the Oversight Board has ordered DDIS to erase information under the indirect subject access request system.

The Oversight Board issued its most recent annual report on its activities to the Minister of Defence in May 2018. The annual report was submitted to the Parliamentary Intelligence Services Committee and then published in June 2018.

3. Legal Framework

1) The Danish Defence Intelligence Service (*DDIS*) Act (Consolidated Act No. 1287 of 28 November 2017, as amended 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).

The DDIS Act was amended by Act No. 1706 of 27 December 2018 as a consequence of the passing of the Act on the collection, use and storage of airline passenger records (the PNR Act).

With the PNR Act, a national PNR unit was established under the Danish police, which on behalf of DDIS, among others, may obtain and process PNR data for the purpose of disclosure to DDIS.

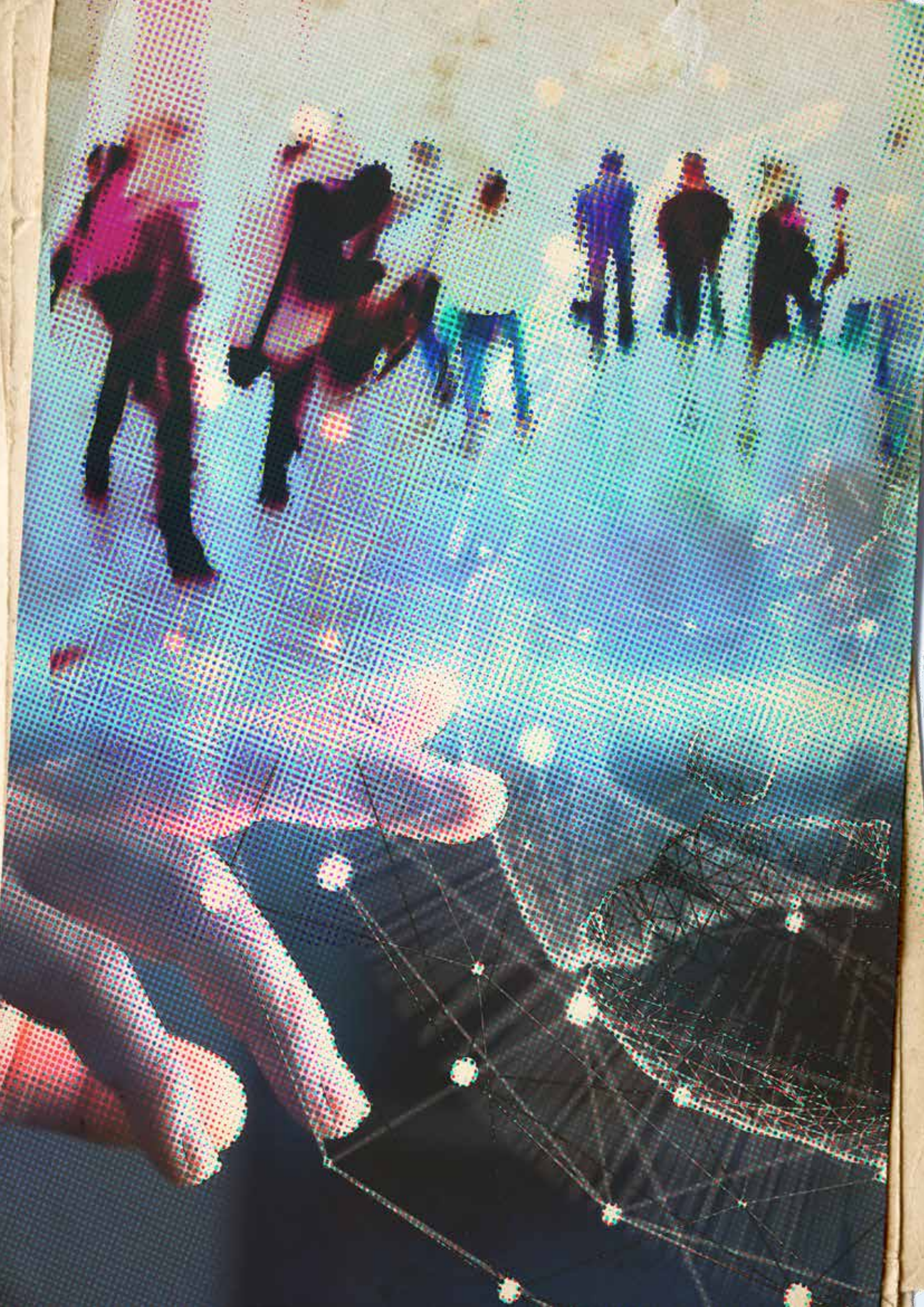
The Danish Intelligence Oversight Board is charged with the task of overseeing the PNR unit's processing of information about persons resident in Denmark on behalf of DDIS. As the Act did not enter into force until on 1 January 2019, it will not be discussed further in this annual report.

3.1 Procurement of information

3.1.1 About collection and obtaining of information, see section 3(1), (2), (3), (4) and (6) of the DDIS Act

Under section 3 of the 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.

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's 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 the Danish Security and Intelligence Service (*DSIS*), unless the conditions in section 3(3) of the Act are satisfied.

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.

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.

However, 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.

According to the explanatory notes to the provision, it will not change the fundamental allocation of responsibilities and mode of cooperation between the Danish Security and Intelligence Service (*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's targeted intelligence obtaining.

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 [...]

Under subsection (4) of the provision, the Danish Customs and Tax Administration (SKAT) must pass on information about aircraft passengers and crew to DDIS if DDIS believes that the information may be important for DDIS's performance of its activities in respect of matters abroad and the information concerns non-Danish nationals.

3.2 Internal processing of information

3.2.1 About internal processing of information under 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's 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.

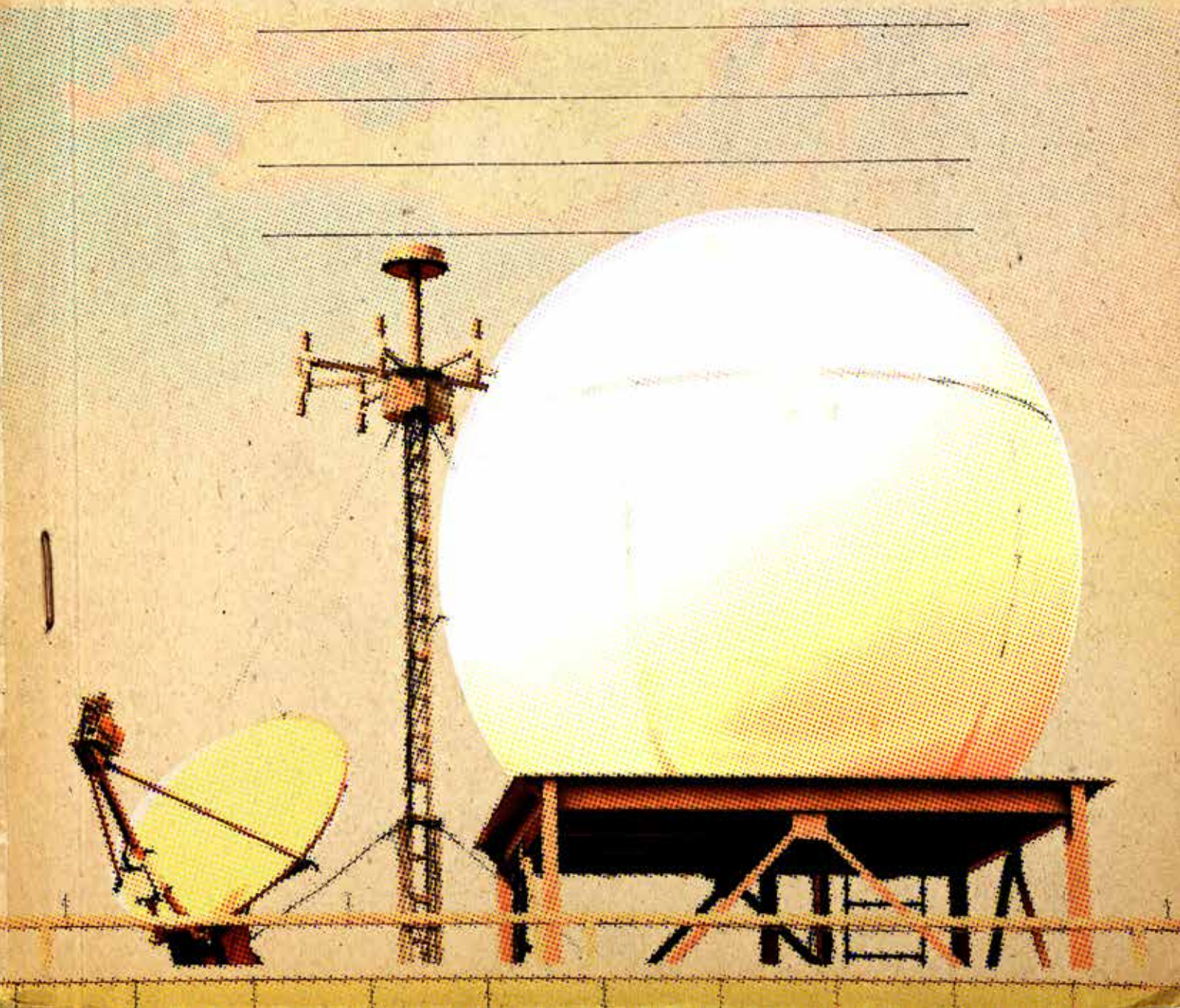
Under sections 4(1) and 5(1) of the Act, DDIS is allowed to process any information about natural and legal persons resident in Denmark if:

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

Under sections 4(1)(ii) and 5(1)(ii) of the Act, DDIS is thus authorised to process any information about natural and legal persons resident in Denmark if processing may be assumed to be of importance to the performance of DDIS's activities as intelligence service etc. The condition that the information may be assumed to be of importance to DDIS's performance of those activities reflects the requirement of a somewhat substantive presumption that the information DDIS wishes to process will be of importance to DDIS's performance of those activities.

Under sections 4(1)(iii) and 5(1)(iii) of the Act, DDIS is authorised to process any information about natural and legal persons resident in Denmark if processing is necessary for the performance of DDIS's activities as military security service. The condition that the information must be necessary for DDIS's performance of those activities reflects the requirement that, based on an assessment in each individual case, DDIS may be assumed to have a genuine need to process the information in question in order to perform its activities as military security 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's 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 and adapted (so as to no longer be raw data). In the understanding of the principles of the former Data Protection Act (*persondataloven*) on good processing practice and security of processing in relation to DDIS's 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 or legal persons resident in Denmark which has been procured in the course of DDIS's 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's 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's 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 sections 4(1) and 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. 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's tasks in connection with indirect subject access requests, see section 10 of the Act, and random checks performed by the Oversight Board.

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 the Oversight Board 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 obtained 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's obligation to erase information does not apply if otherwise prescribed by law or statutory regulation.

3.2.3 About information security, 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's 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 information security 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's 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's 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 processing in violation of the provisions laid down in the Act, and the same applies to DDIS's 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.

> 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 [...]

This means that the information may be disclosed only if (i) explicit consent has been obtained from the data subject; (ii) disclosure is made to safeguard private or public interests which clearly outweigh the interests of confidentiality, including the interests of the data subject; (iii) disclosure is necessary for the performance of a public authority's activities or required for a decision to be made by the public authority; or (iv) if disclosure is necessary for the performance of the activities of a person or business on behalf of the public authorities.

For 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 DDIS 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's 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. The Oversight Board will be given an opportunity to oversee DDIS's 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's 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. The Oversight Board may verify that the provision of subsection (2) is not abused to circumvent the prohibition in subsection (1) and thus that DDIS's 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 DDIS Bill concerning the provision in subsection (3), it will be a central responsibility for the Oversight Board 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 the Oversight Board to check if DDIS is processing information about them in violation of DDIS legislation. The Oversight Board will verify that this is not the case and then notify the data subject.

If special circumstances weigh in favour of doing so, the Oversight Board 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's processing of information about natural and legal persons resident in Denmark, the Oversight Board 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, the Oversight Board is entitled among other things to order DDIS to erase information which, in the opinion of the Oversight Board, DDIS is processing in violation of DDIS legislation. The Oversight Board 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 the Oversight Board'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 the Oversight Board 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.

Under section 10 of the DDIS Act, natural and legal persons resident in Denmark are allowed to request the Oversight Board to check if DDIS is processing information about them in violation of DDIS legislation. The Oversight Board will verify that this is not the case and then notify the data subject.

Annual report 2018
Danish Defence Intelligence Service
Published by the Danish Intelligence Oversight Board, June 2019

Layout + illustrations: Eckardt ApS
Portrait photographs: Lars Engelgaar

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

Members of the Danish Intelligence Oversight Board

Michael Kistrup, High Court Judge, the Danish Eastern High Court (chairman)
Pernille Christensen, Legal Chief, Local Government Denmark
Professor Henrik Udsen, Copenhagen University
Professor Jørgen Grønnegård Christensen, Aarhus University
Erik Jacobsen, Chairman of the Board of Directors, Roskilde University

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