Danish Intelligence Oversight Board

Annual report 2019

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 2019 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.

Copenhagen, October 2020

Michael Kistrup

Chair of the Danish Intelligence Oversight Board

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

The report includes information about the aspects which the Oversight Board has decided to examine more closely as well as the number of instances where DDIS's processing of personal information has been found by the Oversight Board to be in violation of DDIS legislation. For 2019, the following central and fundamentally important parts of the report are emphasised:

! **In November 2019**, as already announced in the Oversight Board's press release of 24 August 2020, the Oversight Board came into possession, through the agency of one or more whistleblowers, of a significant amount of material concerning DDIS, which had not been known or available to the Oversight Board previously. The nature of the material was such that the Oversight Board decided to focus its checks of DDIS in order to make an in-depth examination of the circumstances at hand.

On 21 August 2020, based on the examination, the Oversight Board submitted an analysis to the Danish Minister of Defence setting out the Oversight Board's findings and recommendations.

Based on the examination, the Oversight Board found, among other things, that on several occasions since the Oversight Board's establishment in 2014 and until the summer of 2020, DDIS withheld central and crucial information from the Oversight Board – in connection with, among other things, the Oversight Board's specific checks and meetings with the Head of DDIS – and misinformed the Oversight Board about matters concerning DDIS's obtaining and disclosure of information.

In the Oversight Board's view, the statutory duty to inform is crucially necessary for a functional oversight body and it is based on the legislature's trust in DDIS to comply with the duty in all respects. The result of those repeated breaches of the statutory duty to inform is that the legality check which the Oversight Board is required to carry out under the DDIS Act and which contributes to legitimising DDIS's activities does not work as intended.

The Oversight Board further found that central parts of DDIS's intelligence gathering capabilities involve a risk that information about Danish citizens is obtained in violation of DDIS legislation.

Based on the special examination of DDIS, the Oversight Board's findings will form part, to the necessary extent, of the Oversight Board's annual risk assessment concerning DDIS's processes and systems.

The Oversight Board's special examination of DDIS, including other findings and recommendations, is described in section 2.

! **The Oversight Board's** completed checks of DDIS's electronic obtaining of raw data verified, see section 1.2.1, that DDIS applied a general requirement of legitimacy in its organisation thereof and that, as a general rule, information which concerns persons resident in Denmark is received by DDIS only by chance.

As regards one of the systems which formed part of the Oversight Board's check, the check was not completed in 2019. The reason was, see section 2, that in November 2019, the Oversight Board decided to focus its oversight activities of DDIS as a result of material submitted by one or more whistleblowers.

- **However**, the Oversight Board's oversight activities concerning DDIS's targeted electronic intelligence obtaining, including the Oversight Board's targeted check of DDIS's obtaining of intelligence on behalf of the Danish Security and Intelligence Service (DSIS) showed, see sections 1.2.2 - 1.2.3, that in 14 instances DDIS had engaged in obtaining of intelligence about persons resident in Denmark in violation of DDIS legislation for periods of between one day and 142 days.

- **The Oversight Board's** checks concerning DDIS's raw data searches showed, see section 1.2.4, that in 14 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. Also, the Oversight Board found in its targeted check of DDIS's procurement of intelligence on behalf of the Danish Security and Intelligence Service (DSIS), see section 1.2.3, that, in connection with the cooperation with the Danish Security and Intelligence Service (DSIS), DDIS had made raw data searches in violation of DDIS legislation in 75 instances over a period of 124 days.

- **Finally**, in 2019, the Oversight Board processed requests from 86 natural or legal persons to check if DDIS was processing information about them in violation of DDIS legislation. In this connection, the Oversight Board found that DDIS complied with the provisions of legislation in most of the cases, but that DDIS had processed information about the data subjects in violation of DDIS legislation as far as five of the processed requests were concerned, see section 1.5.2.

  Please note that the above references only represent a minor cross-section of the Oversight Board's checks of DDIS in 2019 where the Oversight Board had special remarks or remarks of general importance. For a full picture of the Oversight Board's checks of DDIS, the report should be read in its entirety.

Foreword

The Danish Intelligence Oversight Board is a special independent monitoring body, which among other things oversees that the Danish Defence Intelligence Service (DDIS) processes personal information 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 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 DDIS. The report also provides information about the aspects which the Oversight Board has decided to examine more closely in 2019 as well as the number of instances where DDIS's processing of personal information has been found by the Oversight Board to be in violation of DDIS legislation.

Like in the preceding years, the Oversight Board has also in 2019 had particular focus on consolidating and strengthening the basis underlying its checks of the Danish Security and Intelligence Service (DSIS), DDIS 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 2019, 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 2019, the Oversight Board carried out in-depth and intensive compliance checks with regard to DDIS's processing of information about natural and legal persons. Like in the preceding years, the Oversight Board has given priority to checks with special focus on DDIS's compliance with legislation on procurement of information, on internal processing of information, including erasure, on legal political activity, and on disclosure of information.

Of particular importance to the Oversight Board's oversight activities regarding DDIS in 2019, as already announced in the Oversight Board's press release of 24 August 2020, has been the fact that, in November 2019, the Oversight Board came into possession, through the agency of one or more whistleblowers, of a significant amount of material concerning DDIS which had not been known or available to the Oversight Board previously. The nature of the material was such that the Oversight Board decided to focus its checks of DDIS with a view to making an in-depth examination of the circumstances at hand. On 21 August 2020, based on the investigation, the Oversight Board submitted a major analysis to the Danish Minister of Defence setting out the Oversight Board's findings and recommendations. The Oversight Board's special investigation of DDIS is described in section 2.

By Act No. 1706 of 27 December 2018 on the collection, use and storage of airline passenger name records (the PNR Act) (lov om indsamling, anvendelse og opbevaring af oplysninger om flypassagerer (PNR-loven)) which entered into force on 1 January 2019, the Oversight Board was charged with the task of overseeing the processing by the PNR Unit under the Danish police of airline passenger name records on behalf of DSIS and DDIS. In 2019, however, the Oversight Board was unable to carry out the oversight activities envisaged in the PNR Act because the legal framework for the Oversight Board's oversight activities under the PNR Act had not yet been clarified, including whether the Danish police's processing of airline passenger name records on behalf of DSIS and DDIS falls within the scope of the indirect subject access request system under section 13 of the DSIS Act and section 10 of the DDIS Act. See also section 3 below.

As was the case in 2018, the Oversight Board saw an increased interest in the indirect subject access request system in 2019. Thus, in 2019, the Oversight Board received requests from 86 natural or legal persons to check if DDIS was processing information about them in violation of DDIS legislation. The Oversight Board welcomes the increased interest in the system and is working to reduce the processing time with regard to responding to the 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 2019, the Oversight Board continued 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). Another body, the British Investigatory Powers Commissioner's Office (IPCO), joined the cooperation in 2019. The focus of this cooperation is to share experience with respect to oversight methods and to discuss legal subjects of mutual relevance. One result of the cooperation was the conference held by the Oversight Board in June 2019 in Copenhagen for the discussion of common intelligence oversight standards.

In November 2019, the Oversight Board further participated in a Nordic meeting in Oslo with oversight and review bodies from Norway, Sweden and Finland. In addition to the Oversight Board's close cooperation with specific oversight and review bodies, in December 2019 the Oversight Board participated in a joint European conference for oversight and review bodies in The Hague, which was attended by 18 European countries.

A new member also joined the Oversight Board in the autumn of 2019.

Michael Kistrup

Chair 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 work of the Oversight Board.

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 Oversight Board's 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, completely random or stratified samples, 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 start-up meetings 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 completed a development project for the purpose of securing more efficient system support for the Oversight Board's checks in 2019. Based on the special risk assessment and analysis for 2019, the Oversight Board has decided to include another four systems in its checks in 2020. For two of the four systems, however, it is not sufficiently possible to carry out an effective check of the information held by DDIS in the systems, which means that, at present, no investigation is made of those systems in connection with indirect subject access requests. Therefore, the Oversight Board has opened a dialogue with DDIS for the purpose of enabling effective checks of the systems in question. In addition, the Oversight Board has identified a number of systems where it will carry out an investigation if there is a presumption, based on its investigation of other systems, that DDIS processes information about the citizen in question in violation of DDIS legislation.

1.2 Oversight of DDIS in 2019

For the purpose of overseeing DDIS's compliance with the provisions of the DDIS Act when processing information about natural and legal persons, the Oversight Board has carried out checks in 2019 of DDIS's:

- electronic obtaining of raw data (SIGINT) (1.2.1),
- targeted electronic intelligence obtaining (SIGINT) (1.2.2),

- obtaining of intelligence at the request of DSIS (1.2.3),
- raw data searches (1.2.4),
- obtaining of human intelligence (HUMINT) (1.2.5),
- processing of open source intelligence (OSINT) (1.2.6),
- processing of material classified as COSMIC TOP SECRET (1.2.7),
- other information processing (1.2.8),
- disclosure of information to partners (1.2.9),
- workstations (1.2.10), and
- information security (1.2.11).

The Oversight Board's oversight activities concerning DDIS's internal checks in 2019 will be carried out as part of its oversight activities concerning DDIS in 2020.

In November 2019, the Oversight Board came into possession, through the agency of one or more whistleblowers, of a significant amount of material concerning DDIS which had not been known or available to the Oversight Board previously. The nature of the material was such that the Oversight Board decided to focus its checks of DDIS with a view to making an in-depth examination of the circumstances at hand.

The Oversight Board's special examination is described in section 2.

Summary of the Oversight Board's checks in 2019

The Oversight Board's completed checks of DDIS's electronic obtaining of raw data (SIGINT) verified, see section 1.2.1, that DDIS applied a general requirement of legitimacy in its organisation thereof and that, as a general rule, information which concerns persons resident in Denmark is received by DDIS only by chance. As regards one of the DDIS systems which is used for electronic obtaining of raw data, the check was not completed in 2019. The reason was, see section 2, that in November 2019, the Oversight Board decided to focus its oversight activities of DDIS as a result of material submitted by one or more whistleblowers.

However, the Oversight Board's checks of DDIS's targeted electronic intelligence obtaining (SIGINT) showed, see section 1.2.2, that in three instances DDIS had performed obtaining of intelligence about persons resident in Denmark in violation of DDIS legislation. Furthermore, the Oversight Board's checks showed, see section 1.2.3, that in 11 instances DDIS had engaged in obtaining of intelligence about persons resident in Denmark in violation of DDIS legislation at the request of DSIS.

The Oversight Board's checks of DDIS's raw data searches also showed, see section 1.2.4, that in 14 percent of the instances sampled DDIS had performed raw data searches in violation of DDIS legislation. Also, the Oversight Board found in its targeted check of DDIS's procurement of intelligence on behalf of DSIS, see section 1.2.3, that in connection with the cooperation with DSIS, DDIS had made raw data searches in violation of DDIS legislation in 75 instances over a period of 124 days.

As regards one of the DDIS systems which is used for raw data searches, the Oversight Board had to cancel its scheduled check as it was impossible for the Oversight Board to set up logging in the system before the end of 2019.

The Oversight Board's checks of DDIS's obtaining of human intelligence (HUMINT) verified, see section 1.2.5, DDIS's compliance with the provisions of legislation concerning procurement of information.

The Oversight Board's checks of DDIS's processing of open source intelligence (OSINT) showed, see section 1.2.6, that DDIS should have erased information concerning two persons resident in Denmark under section 6a(1) of the DDIS Act and also that, in one instance, DDIS had engaged in collection of intelligence about a person resident in Denmark in violation of DDIS legislation.

The Oversight Board's checks of DDIS's other processing of information verified, see section 1.2.8, DDIS's compliance with the provisions of legislation concerning processing of information.

The Oversight Board's checks of four systems which are used by DDIS in relation to disclosure of information to partners verified, see section 1.2.9, DDIS's compliance with the provisions of legislation concerning disclosure of information in relation to the systems being checked.

Furthermore, the Oversight Board's check of workstations verified, see section 1.2.10, that the DDIS staff members processed information about persons resident in Denmark in compliance with legislation and that the staff members were generally aware of the rules governing processing of information about persons resident in Denmark.

The Oversight Board's checks of information security verified, see section 1.2.11, that DDIS's implementation of the ISO 27001 standard essentially took place as planned by DDIS as DDIS generally implemented an information security management system (ISMS) in 2019 as contemplated by the ISO 27001 standard. However, in 2020, DDIS will continue to work with operationalisation and expansion of the implemented ISMS. The Oversight Board also noted that DDIS has implemented most of the recommendations given by the Oversight Board on the basis of the analysis of DDIS's implementation of the ISO 27001 standard in 2018. In a few areas, however, the fulfilment of the Oversight Board's recommendations has not been either documented to the Oversight Board or fully implemented in 2019.

The Oversight Board's check of DDIS's processing of material classified COSMIC TOP SECRET has not been completed, see section 1.2.7, as DDIS has not yet submitted a response to the Oversight Board's consultation questions. The results of the checks will be discussed in the Oversight Board's annual report for 2020.

1.2.1 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 purposes of its check thereof, in 2019 the Oversight Board performed a check of four systems which are used by DDIS in relation to DDIS's electronic obtaining of raw data.

The checks were performed by discussions with the responsible DDIS staff members and with the legal department of DDIS as well as by inspections and demonstrations of the systems being subject to checking. As regards one of the systems in question, the Oversight Board's check was not completed in 2019. The reason was that in November 2019, the Oversight Board came into possession of a significant amount of material concerning DDIS the nature of which was such that the Oversight Board decided to focus its oversight activities in relation to DDIS with a view to making an in-depth examination of the circumstances at hand, see section 2. In 2020, the Oversight Board will follow up on the check of the system concerned.

! **Comments by the Oversight Board**
The checks of DDIS's electronic obtaining of raw data completed by the Oversight Board verified that DDIS applied a general requirement of legitimacy in its organisation thereof and that, as a general rule, information which concerns persons resident in Denmark is received by DDIS only by chance.

1.2.2 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 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 2019 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 sample checks of DDIS's targeted electronic intelligence obtaining, including pursuant to section 3(3) of the DDIS Act, showed that, in three instances, DDIS had performed obtaining of intelligence about persons resident in Denmark in violation of DDIS legislation over 142 days in 2016, 58 days in the period 2017 to 2018 as well as one day in 2018.

The above instances only concern the situations where DDIS engaged in targeted obtaining of intelligence of its own motion. Instances where DDIS's targeted obtaining was performed at the request of DSIS are discussed separately in section 1.2.3.

1.2.3 Checks of DDIS's obtaining of intelligence at the request of DSIS

It is a requirement under 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. Thus, DSIS may submit a request to DDIS for targeted electronic obtaining of information directed at persons resident in Denmark which DDIS is not allowed to performed of its own motion under the provisions of the DDIS Act.

The obtaining of intelligence is performed on the basis of DSIS legislation and assumes that DSIS has obtained a court order for the intervention measure. Errors or miscommunication between DDIS and DSIS may cause DDIS to engage in or continue the obtaining of information directed at persons resident in Denmark without DDIS being covered by a court order obtained by DSIS. By way of example, this may occur due to errors in the request from DSIS or errors in DDIS's reading of the request, and if DDIS is not informed of the termination of a court order or if DDIS is unable to stop the obtaining by the time-limit issued by DSIS.

In connection with its other checks of DDIS's targeted electronic obtaining, see section 1.2.2, the Oversight Board performs regular checks of intelligence obtaining activities which have been initiated at the request of DSIS. In addition, in 2019, the Oversight Board has performed a targeted check of DDIS's obtaining at the request of DSIS, focusing on whether DDIS's intelligence obtaining activities fall within the framework of the court order obtained by DSIS, including that the intervention measure ceases no later than when the court order terminates.

! **Comments by the Oversight Board**

The Oversight Board's checks of DDIS's obtaining of intelligence at the request of DSIS showed that, in 11 instances, DDIS had engaged in obtaining of information about persons resident in Denmark over eight days in 2018 (in one instance), one day in 2018 (in two instances), 89 days in the period 2018 to 2019 (in two instances), 24 days in 2019 (in one instance) and in 34 days in 2019 (in five instances).

Also, the Oversight Board noted that in connection with the cooperation with DSIS, DDIS had performed raw data searches in violation of DDIS legislation in 75 instances over a period of 12 days in 2018 to 2019, although the result may be expected to be mainly information about persons resident in Denmark.

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 section 3(3) of the DDIS Act. In addition, DDIS is allowed to make such searches at the request of DSIS, where such requests are submitted on the basis of DSIS legislation.

If DDIS performs raw data searches the result of which must be expected to be mainly information about persons resident in Denmark without DDIS having a legal basis for the search, the search in question will be in violation of DDIS legislation. The reason for raw data searches being performed in violation of DDIS legislation may be a failure to time limit searches according to court orders, a 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.

For the purpose of its compliance check, in 2019 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 did not continue its raw data searches for information about persons resident in Denmark when the court order against the relevant persons 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 2019.

! **Comments by the Oversight Board**

The Oversight Board's regular checks concerning DDIS's raw data searches showed that, in 14 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 opinion, DDIS still has a challenge when performing raw data searches in relation to its compliance with legislation on procurement of information about persons resident in Denmark. The Oversight Board notes that the error rate has not been reduced in relation to the result of the check in 2018, but that DDIS still has a considerable focus on reducing the number of errors, including by carrying out an intensive internal control in the area as well as training of DDIS staff.

As regards one of the DDIS systems which is used for raw data searches, the Oversight Board had to cancel its scheduled check as no logging is performed of DDIS's raw data searches via the system and as it was impossible for the Oversight Board to set up such logging before the end of 2019. In 2020, the Oversight Board will follow up to ensure that system logging is set up.

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 DSIS.

For the purpose of checking this aspect, in 2019 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 legislation regarding procurement of information.

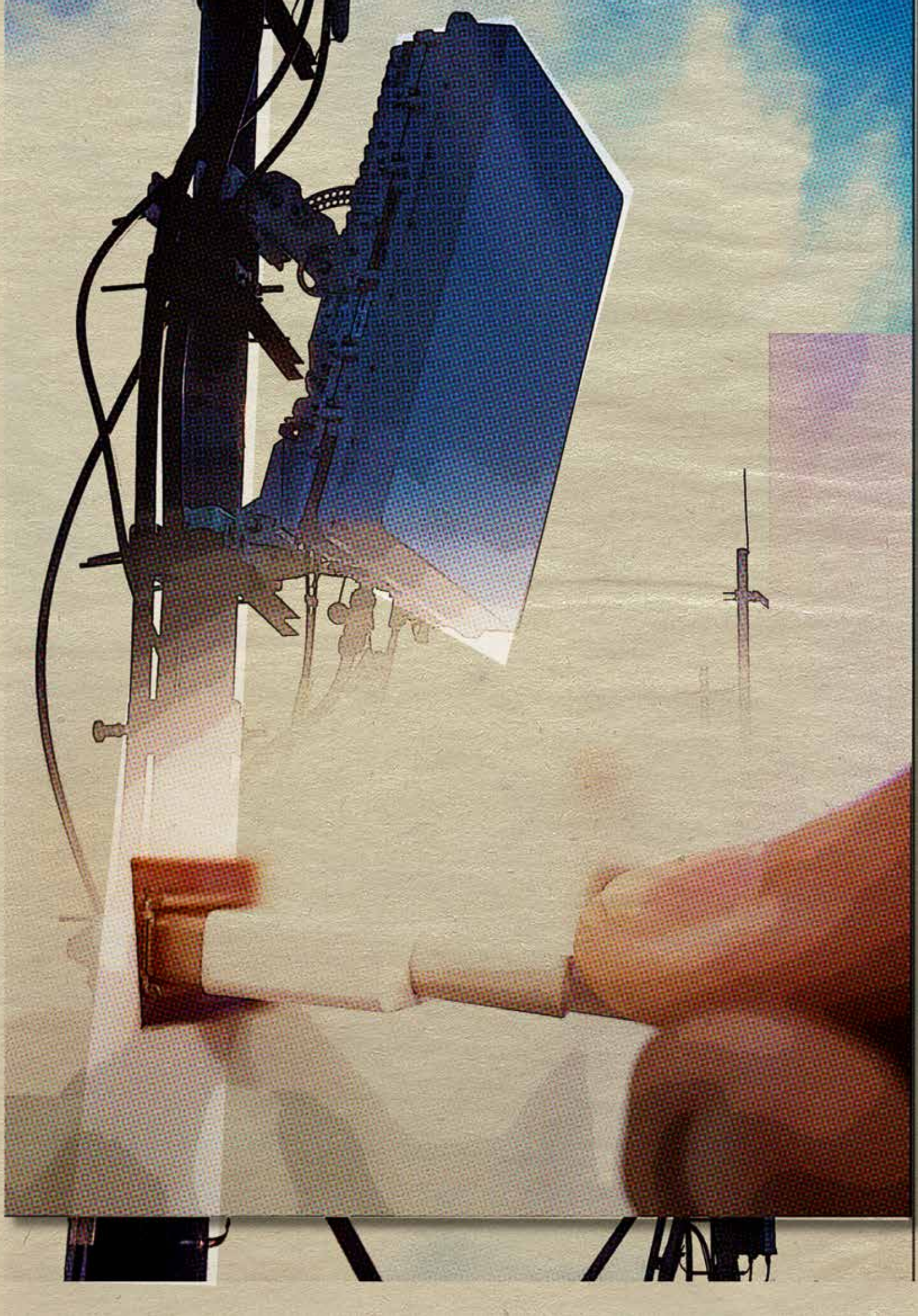
1.2.6 Checks of DDIS's processing of open source intelligence (OSINT)

DDIS's collection of open source intelligence (OSINT) includes sophisticated and systematic collection of information from sources such as the internet, e.g. communication in open network forums, as well as print media, television, etc.

DDIS's compliance with the rules on collection of open source intelligence only involves requirements to the effect that the information may be of significance to DDIS's intelligence-related activities directed at conditions abroad and that the information is publicly available. Collection thus differs from electronic obtaining in that DDIS is allowed, of its own motion, to engage in targeted collection of information against persons resident in Denmark, provided that the above requirements are met.

When, in connection with its activities, DDIS becomes aware that cases or documents etc. no longer meet the conditions of processing in sections 4 and 5 of the DDIS Act, they must be erased, see section 6a(1) of the DDIS Act.

In 2019, the Oversight Board performed a targeted check of whether DDIS still processed information about a number of persons resident in Denmark in a system which is used by DDIS in relation to the collection of open source intelligence notwithstanding that the Oversight Board's check of DDIS in 2017 showed that DDIS should erase information about the persons in question. At the same time, the Oversight Board checked that DDIS had not subsequently collected new information about the persons in question.



! **Comments by the Oversight Board**
The Oversight Board's checks showed that DDIS should have erased information concerning two persons resident in Denmark under section 6a(1) of the DDIS Act. The checks also showed that in one instance DDIS engaged in obtaining of intelligence about a person resident in Denmark in violation of DDIS legislation.

1.2.7 Checks of DDIS's processing of material classified as COSMIC TOP SECRET

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

In 2019, the Oversight Board performed a check of DDIS's processing of material classified as COSMIC TOP SECRET which concerns persons resident in Denmark. The check was performed by way of discussions with DDIS as well as a review of DDIS's documentation concerning material classified as COSMIC TOP SECRET.

! **Comments by the Oversight Board**
The check gave rise to a consultation of DDIS on its processing of material classified as COSMIC TOP SECRET. As at the date of this report, no consultation response has been received. The results of the check will be discussed in the Oversight Board's annual report for 2020.

1.2.8 Checks of DDIS's other processing of information

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

In 2019, the Oversight Board drew one random sample from one of DDIS's electronic analysis and documentation systems where DDIS processes information about persons resident in Denmark.

The Oversight Board also performed a check of two systems which are used by DDIS in relation to DDIS's processing of information. The check was performed by discussions with the responsible DDIS staff members and with the legal department of DDIS as well as for one of the systems concerned, by a demonstration of the system.

! **Comments by the Oversight Board**
The Oversight Board's checks of DDIS's other processing of information verified DDIS's compliance with the requirements of legislation concerning processing of information.

1.2.9 Checks of DDIS's disclosure of information to partners

DDIS is involved in bilateral and multilateral partnerships with foreign intelligence services for the

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

DDIS also discloses information to national partners, e.g. DSIS and other authorities under the Danish Ministry of Defence.

In 2019, the Oversight Board performed a check of four systems which are used by DDIS in relation to DDIS's disclosure of information to its partners. The check was performed by discussions with the DDIS staff members who were responsible therefor and with the legal department of DDIS as well as for three of the systems concerned, by a demonstration of the systems.

! **Comments by the Oversight Board**

The Oversight Board's checks of DDIS's disclosure of information to its partners verified DDIS's compliance with the provisions of legislation concerning disclosure of information in relation to the systems being checked.

1.2.10 Checks of DDIS workstations

In 2019, the Oversight Board performed a check of a number of staff workstations, focusing on the staff's processing of information about persons resident in Denmark, including their knowledge of the rules in this area.

The Oversight Board performed a check of a random sample of the workstations in one of the DDIS sections, including of staff members' drives, email system folders, external storage devices and documents in hard copy, and the Oversight Board also performed a supplementary check of central internal shared drives and mail boxes. In connection with the random checks performed of the information held on the workstations, the Oversight Board asked questions to the individual staff members in question about their knowledge of legislation on processing of information about persons resident in Denmark.

! **Comments by the Oversight Board**

The check of the sampled workstations 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.

1.2.11 Checks of DDIS's information security

In 2018, the Oversight Board prepared an extensive analysis of DDIS's implementation of the ISO 27001 standard and, based on the analysis, issued a number of recommendations to DDIS.

In 2019, the Oversight Board held half-yearly status meetings with DDIS in relation to the implementation of the ISO 27001 standard in 2019 and reviewed the material prepared by DDIS in connection with the implementation.

! **Comments by the Oversight Board**

In the Oversight Board's assessment, DDIS's implementation of the ISO 27001 standard essentially has taken place as planned by DDIS as DDIS generally implemented an information security management system (ISMS) in 2019 as contemplated by the ISO 27001 standard.

However, in 2020, DDIS will need to continue to work with operationalisation and expansion of the implemented ISMS.

The Oversight Board also noted that DDIS has implemented most of the recommendations given by the Oversight Board on the basis of the analysis of DDIS's implementation of the ISO 27001 standard in 2018. In a few areas, however, the fulfilment of the Oversight Board's recommendations has been neither documented to the Oversight Board nor fully implemented in 2019.

1.3 Follow-up on the Oversight Board's checks of DDIS in 2018

Each year, the Oversight Board checks whether 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 for 2018, section 1.2.9, the Oversight Board wrote that DDIS had indicated that it would erase specific information about a number of persons resident in Denmark as the information was no longer relevant to process for the performance of DDIS's activities as a military security service.

Therefore, among other things, the Oversight Board checked the personal information in question again with a view to determining whether the information had subsequently been erased.

! **Comments by the Oversight Board**

The Oversight Board's follow-up on the check of DDIS in 2018 verified DDIS's erasure of the information which DDIS had indicated in connection with the Oversight Board's check in 2018 that it would erase.

However, the check also showed that, in one instance, DDIS had not implemented the necessary actions which it had indicated in connection with the Oversight Board's check in 2017 that it would take. As DDIS had stated in connection with the Oversight Board's follow-up on the check in 2017 that the actions in question would be implemented by the end of 2018, DDIS's failure to follow up was not mentioned in the Oversight Board's annual report on DDIS for 2018, section 1.3.

In relation to the Oversight Board's other checks as described in the Oversight Board's annual report on its activities concerning DDIS for 2018 (section 1.2), the checks performed 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 subsections (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.

DDIS has kept the Oversight Board informed of its use of the provisions.

In 2019, based on a briefing by DDIS on a decision under section 6(3) of the DDIS Act not to erase information which has reached the time limit for erasure of 15 years, the Oversight Board had regular discussions with DDIS in 2019 concerning practical measures in relation to matters such as identification of such information.

Based on the Oversight Board's special examination of DDIS, see section 2, the Oversight Board found that, on several occasions since the Oversight Board's establishment in 2014 and until the summer of 2020, DDIS withheld central and crucial information from the Oversight Board and misinformed the Oversight Board about matters concerning DDIS's obtaining and disclosure of information.

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.

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

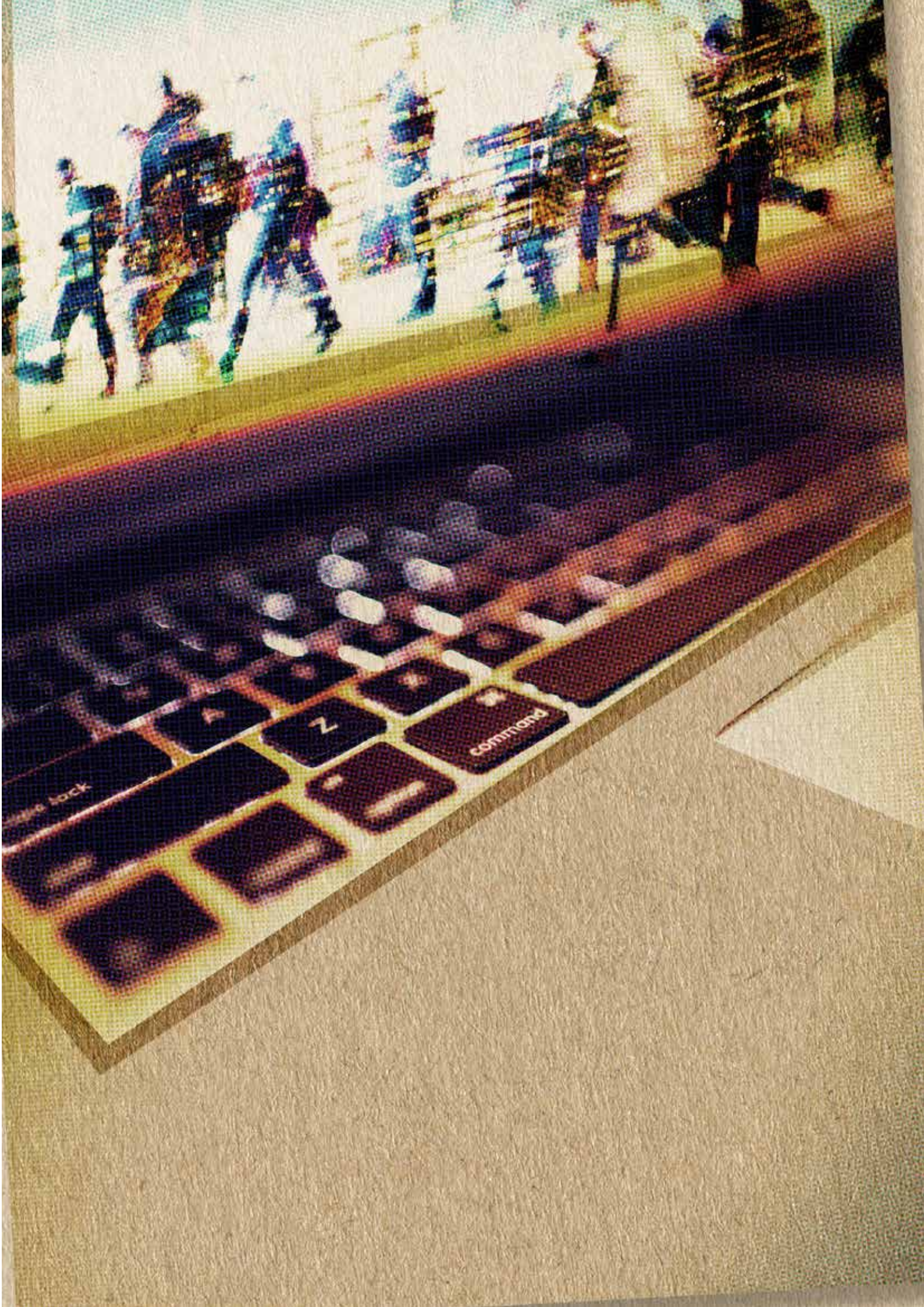
In 2019, the Oversight Board received subject access requests from 86 natural or legal persons, asking the Oversight Board to check if DDIS was processing personal information about them in violation of DDIS legislation. In relation to most of the instances where the Oversight Board completed its check, DDIS's compliance with the provisions of legislation was verified. In five of the instances where the Oversight Board completed its check, the Oversight Board found that DDIS had processed information about the candidates in violation of DDIS legislation. 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 126 days, 7 days of which were DDIS's processing time. Compared with 2018, the average processing time increased by 19 days, which was due, among other reasons, to increased interest in the indirect subject access request system.

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

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.

In 2019, the Oversight Board opened a dialogue with DDIS in order to enable effective control of DDIS's processing of information in specified DDIS systems as this is currently not possible. Thus, at present, the Oversight Board is unable to perform effective checks of these systems in connection with indirect subject access requests.


Z
command

2

The Oversight Board's special examination of DDIS

On 24 August 2020, the Oversight Board issued the following press release:

The Danish Intelligence Oversight Board ends special examination of DDIS based on material provided by one or more whistleblowers

In November 2019, the Danish Intelligence Oversight Board came into possession, through the agency of one or more whistleblowers, of a significant amount of material concerning DDIS which had not been known or available to the Oversight Board previously. The nature of the material is such that the Oversight Board decided to focus its oversight activities in relation to DDIS with a view to making an in-depth examination of the circumstances at hand. With this announcement, the Oversight Board publishes the unclassified results of the examination.

On 21 August 2020, based on the Oversight Board's examination of the material provided, the Oversight Board submitted an analysis in four binders to the Danish Minister of Defence setting out the Oversight Board's findings and recommendations.

Throughout the process of the special examination of DDIS, the Oversight Board has kept the Danish Minister of Defence informed. The Minister of Defence has regularly expressed her support for the in-depth examination of the material.

The Oversight Board's assessments and recommendations concern matters which are deemed, in whole or in part, to fall within the Oversight Board's legality check under the DDIS Act and rules issued thereunder, as well as matters which the Minister should have known in the Oversight Board's opinion, see section 16(2) of the DDIS Act.

Based on a source critical approach to the examination of the material received, the Oversight Board takes the following view:

- That, on several occasions since the Oversight Board's establishment in 2014 and until the summer of 2020 – in connection with, among other things, the Oversight Board's specific checks and meetings with the Head of DDIS – DDIS withheld central and crucial information from the Oversight Board and misinformed the Oversight Board about matters concerning DDIS's obtaining and disclosure of information.

In the Oversight Board's view, the statutory duty to inform is crucially necessary for a functional oversight body and it rests on the legislature's trust in DDIS to comply with the duty in all respects. The result of those repeated breaches of the statutory duty to inform is that the legality check which the Oversight Board is required to carry out under the DDIS Act and which contributes to legitimising DDIS's activities does not work as intended.

- That there is a risk with regard to central parts of DDIS's intelligence gathering capabilities that information about Danish citizens may be obtained in violation of DDIS legislation.

- That the material received indicates that DDIS management has omitted to follow up on or look into indications of espionage in areas under the Ministry of Defence.

- That, in DDIS management and parts of DDIS, an inappropriate legality culture exists where DDIS seeks to shelve any unauthorised DDIS activities or inappropriate matters, including by omitting to inform the Oversight Board about matters of relevance to its oversight activities.

- That the material received indicates that, before the establishment of the Oversight Board in 2014, DDIS has initiated operative activities in violation of Danish law, including by obtaining and disclosure of a significant amount of information about Danish citizens.

- That DDIS has processed information about an Oversight Board employee in violation of DDIS legislation.

On that basis, the Oversight Board recommends that the following issues be politically addressed:

- Whether to initiate a probe into whether DDIS has performed and is performing its duties as the national security authority under the Danish Ministry of Defence in accordance with section 1(2) of the DDIS Act.

- The need for determining whether DDIS has sufficiently and adequately informed political decision-makers of all relevant matters concerning central parts of DDIS's intelligence gathering capabilities.

With the control and response options currently available to the Oversight Board under the DDIS Act, the Oversight Board is unable to look further into specific concerns emerging from the material received. The Oversight Board would therefore in general recommend as follows:

- That an evaluation of the DDIS Act should be performed soon for the purpose of deciding if the Oversight Board has been granted sufficient powers and resources to perform an effective legality check of DDIS, including in particular whether the Oversight Board needs powers to examine DDIS staff members as witnesses under oath.

- That, based on the circumstances surrounding the Oversight Board's receipt of the material received, an external whistleblowing scheme should be set up for DDIS, ideally under the management of the Oversight Board.

The purpose of such a scheme should be to improve current and former DDIS staff members' possibilities of reporting wrongdoing in DDIS without being concerned about reprisals, including employment or criminal consequences. Furthermore, such a scheme would allow classified information to be disclosed in a secure environment. The scheme should also ensure that the external whistleblowing body has the necessary resources and measures to protect the persons reporting their concerns.

The Oversight Board has engaged in careful consideration with regard to the publication of findings and recommendations based on the check performed. It is of crucial importance to the Oversight Board that the public is given as full insight in this as at all possible. Having regard to the high sensitivity surrounding the submission of material to the Oversight Board and the classified content of the material, however, the Oversight Board is unable to provide further information to the public.

Based on the special examination of DDIS, the Oversight Board's findings will form part, to the necessary extent, of the Oversight Board's annual risk assessment concerning DDIS's processes and systems. As already discussed in section 1.1, the purpose of this annual 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.

3

The Oversight Board's oversight activities under the PNR Act

By Act No. 1706 of 27 December 2018 on the collection, use and storage of airline passenger name records (the PNR Act) which entered into force on 1 January 2019, the Oversight Board was charged with the task of overseeing the processing by the PNR Unit under the Danish police of airline passenger name records on behalf of DSIS and DDIS. The statutory authority formerly granted to the Danish Customs Agency with regard to receiving and passing on PNR information to DSIS and DDIS under the DSIS Act, the DDIS Act and the Danish Customs Act, respectively, was repealed when the PNR Act entered into force.

In 2019, however, the Oversight Board was unable to carry out the oversight activities envisaged in the PNR Act because the legal framework for the Oversight Board's oversight activities under the PNR Act had not yet been clarified, including whether the Danish police's processing of airline passenger name records on behalf of DSIS and DDIS falls within the scope of the indirect subject access request system under section 13 of the DSIS Act and section 10 of the DDIS Act.

On that basis, the Oversight Board has had an ongoing dialogue with the Danish Ministry of Justice since January 2019 concerning the Oversight Board's oversight activities under the PNR Act, including its powers under legislation in relation to the Danish police, DSIS and DDIS, respectively. On 19 December 2019, the Oversight Board received a response from the Ministry of Justice concerning clarification of the legal framework for the Oversight Board's oversight activities.

On that basis, the Oversight Board will begin its oversight activities under the PNR Act in 2020.

4 Publicity in 2019

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 very 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 and oversight options as well as the results of its oversight.

The Oversight Board's annual report for 2018, which was published in July 2019, gave rise to media coverage, among other things because of the Oversight Board's finding that, for one of its intelligence gathering systems, DDIS had not complied with its duty to keep the Oversight Board informed of all material questions concerning DDIS's processing of information about persons resident in Denmark.

Moreover, in late summer of 2019, a number of media focused on the former practices of DSIS concerning requests to DDIS for raw data searches which, in the Oversight Board's view, did not fall within the framework established by legislation. In this connection, the Chair of the Oversight Board gave an interview in the Danish newspaper Berlingske, which was published on 30 August 2019. The media coverage spawned increased interest in the indirect subject access request system, which has meant that the Oversight Board received a large number of requests from citizens concerning the indirect subject access request system in 2019, as described in section 1.5 of the report.

Finally, in November 2019, the think tank "Stiftung Neue Verantworden" published a report entitled "Data-driven Intelligence Oversight – Recommendations for a System Update" in which the Oversight Board's work methods are emphasised. The report suggests seven tools to reform intelligence oversight across Europe, highlighting in this connection the Oversight Board's risk-based work as an example of how to handle challenges with effective allocation of sparse intelligence oversight resources.

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*) Act (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, as amended (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 (CFCS) of personal information is in compliance with DDIS legislation, and submit an annual report in this regard to the Minister of Defence.

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

2. Danish Intelligence Oversight Board

The Oversight Board is a special independent monitoring body charged with overseeing that DSIS, DDIS and CFCS process personal information in compliance with DSIS, DDIS and CFCS 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 Chair, who must be a High Court judge, is appointed on the recommendation of the Presidents of the Danish Eastern and Western High Courts, while the remaining four members are appointed following consultation with the Parliamentary Intelligence Services Committee.

The Oversight Board had the following members as at the end of 2019:

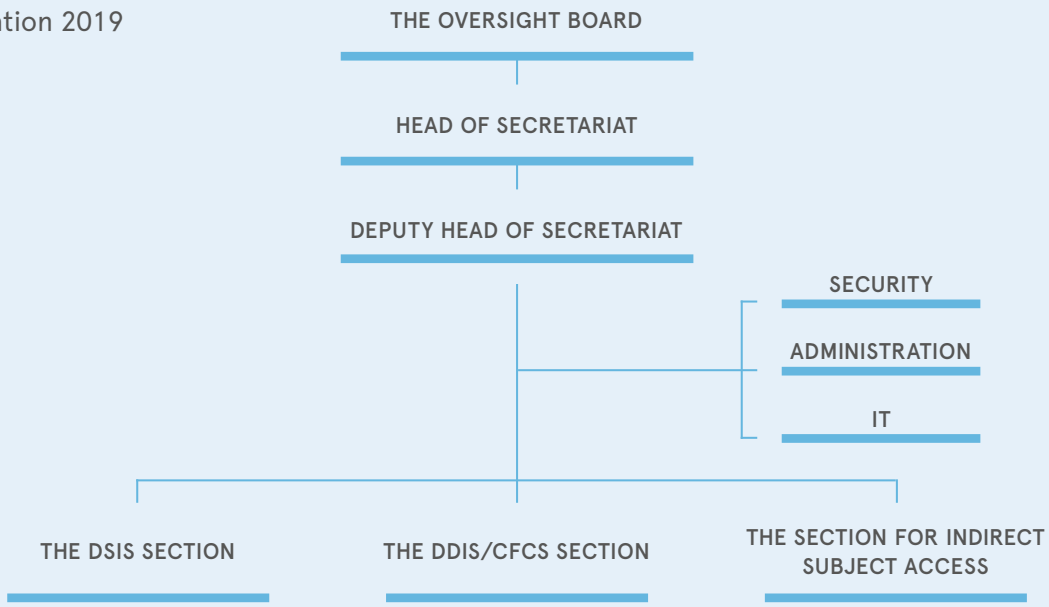
- Michael Kistrup, High Court Judge, the Danish Eastern High Court (Chair)
- Erik Jacobsen, Chair of the Board of Directors, Roskilde University
- Pernille Christensen, Legal Chief, Local Government Denmark
- Professor Henrik Udsen, Copenhagen University
- Professor Rebecca Adler-Nissen, Copenhagen University

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 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 2019, 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, two IT consultants 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 2019



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 data subject (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 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.

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 June 2019. The annual report was submitted to the Parliamentary Intelligence Services Committee and then published in July 2019.

3. Legal framework

1) The Danish Defence Intelligence Service (DDIS) Act (Consolidated Act No. 1287 of 28 November 2017, as amended (most recently by Act No. 1706 of 27 December 2018) (the DDIS Act)

2) Executive Order on security measures to protect personal information being processed by the Danish Defence Intelligence Service (DDIS) (Executive Order No. 1028 of 11 July 2018) (the DDIS Executive Order on Security Measures)

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

4) Executive Order on the PNR Unit's processing of PNR information in a transitional period (Executive Order No. 1757 of 27 December 2018)

3.1 Procurement of information

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

Under section 3(1) of the DDIS Act, DDIS is authorised to collect and obtain information which may be of importance to the performance of its intelligence-related activities and DDIS is entitled in those activities directed at conditions abroad to include information on natural and legal persons resident in Denmark and persons currently staying in Denmark. As far as its other activities are concerned, DDIS may collect and obtain information which is necessary for the performance of its activities, see section 3(4) of the Act.

The most important purpose of this provision is to emphasise that in its intelligence-related activities directed at conditions abroad DDIS is entitled to collect and obtain data, including raw data, among other things through electronic and physical obtaining, so long as those data are deemed at the time of collection and obtaining to be of potential importance to DDIS'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 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 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.

3.2 Internal processing of information

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

Under section 3e(1)-(7) of the DDIS Act, a number of general data protection principles apply to DDIS'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).

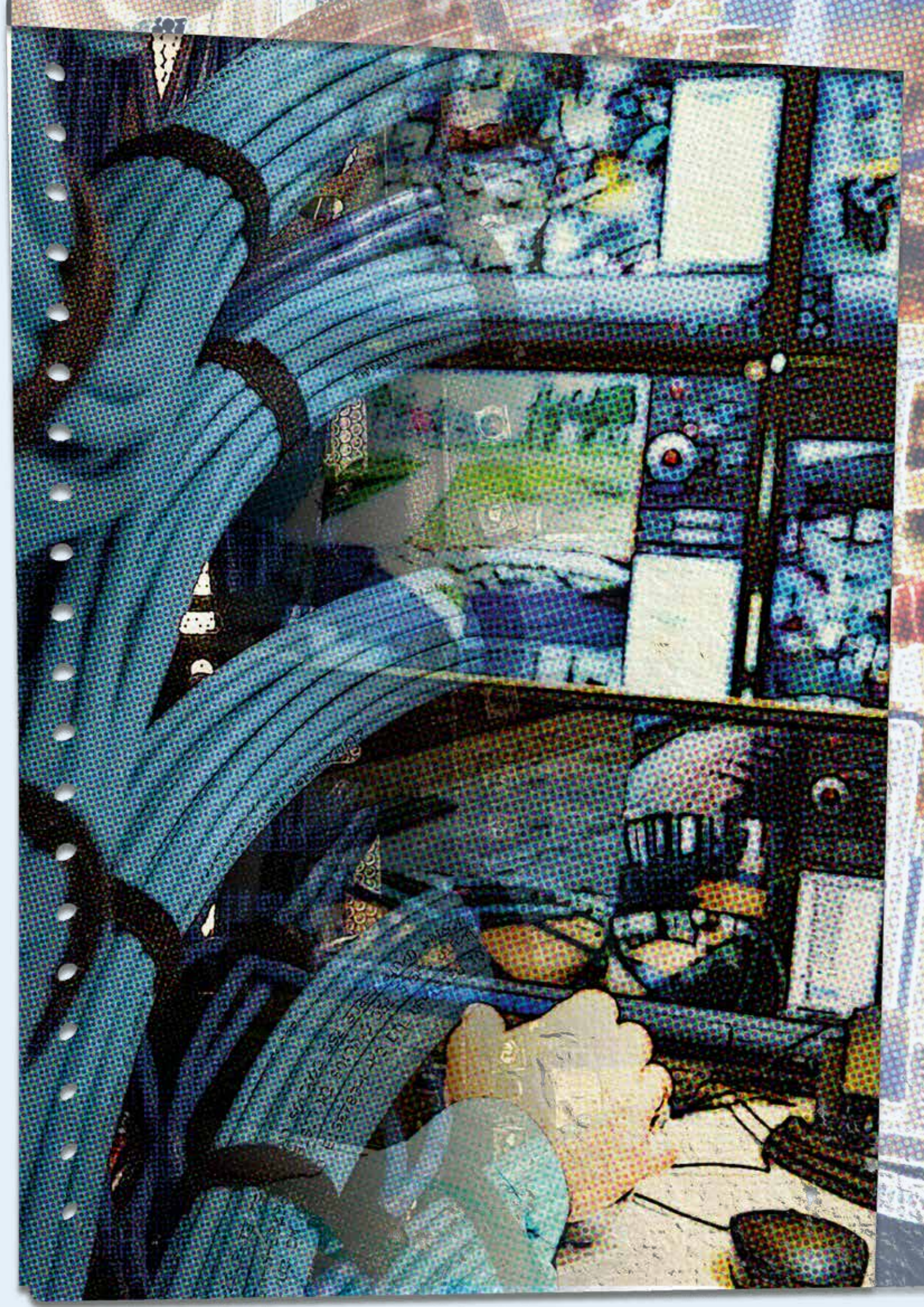
In its electronic intelligence obtaining, DDIS obtains very large amounts of information which at the time of obtaining is made up of non-processed data. Such data are known as "raw data" and are characterised by the fact that until processed, including, if necessary, decryption and translation, it is 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 and 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 section 4(1) and section 5(1), they must be erased, regardless of whether the time limit for erasure of information in section 6(1) has expired, but that DDIS is not required beyond that to review its cases and documents, etc. on a regular basis of its own motion in order to assess if the above conditions of processing are still met.



In the notes to the individual provisions of the Bill, it is specified with regard to section 6a(1) that the term "activities" is to be understood in the broad sense as encompassing all the tasks that DDIS is engaged in. Thus, by way of example, in addition to operational activities, the term also includes DDIS'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 unlawful processing contrary to the DDIS 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. 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 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 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. According to the explanatory notes to the 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.

3.6 Processing of passenger name records (PNR information) for DDIS

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

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

As a general rule, therefore, DDIS is not allowed to engage in targeted intelligence obtaining about persons resident in Denmark. However, there are a number of exceptions to the general rule, including in connection with DDIS's physical obtaining and obtaining pursuant to section 3(3) of the DDIS Act.

Under section 15(3) of the PNR Act, DDIS is only allowed to request the PNR authority to provide PNR information about natural persons resident in Denmark if the information concerns specified persons and DDIS believes that the information must be assumed to be of significance to the

performance of DDIS's activities directed at conditions abroad. The requirement to processing is thus stricter than the other provisions of the PNR Act concerning DDIS, according to which it is only a requirement that the PNR information may be of significance to DDIS's activities.

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

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

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

Further, under section 16(3)(iii) of the PNR Act, the PNR Unit may request the PNR units of other EU member states to disclose PNR information or the result of the processing of such information where DDIS believes that the information may be of significance to the performance of its activities directed at conditions abroad.

3.6.3 The PNR Unit's processing and disclosure of PNR information on behalf of DDIS, see sections 8, 10 and 15 of the PNR Act

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

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

Further, under para. (iii) of section 10 of the PNR Act, the PNR Unit is allowed to process PNR information where DDIS believes that the information may be of significance to the performance of its activities directed at conditions abroad. If the PNR information concerns natural persons resident in Denmark, DDIS is only allowed under section 15(3) of the PNR Act to request such information if the information concerns specified persons and DDIS believes that the information must be assumed to be of significance to the performance of DDIS's activities directed at conditions abroad.

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

3.6.4 Information security, see section 24 of the PNR Act

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

(i) Collection
(ii) Search
(iii) Changes
(iv) Disclosure
(v) Masking and unmasking
(vi) Erasure

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

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

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

Annual report 2019
Danish Defence Intelligence Service
Published by the Danish Intelligence Oversight Board, October 2020

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 (Chair)
Erik Jacobsen, Chair of the Board of Directors, Roskilde University
Pernille Christensen, Legal Chief, Local Government Denmark
Professor Henrik Udsen, Copenhagen University
Professor Rebecca Adler-Nissen, Copenhagen University

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