The Danish Intelligence Oversight Board

Annual report 2017

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 2017 in accordance with section 19 of the Danish Defence Intelligence Service (*DDIS*) Act (Consolidated Act No. 1287 of 28 November 2017). The annual report must be submitted to the Parliamentary Intelligence Services Committee and subsequently published.

Copenhagen, May 2018

Michael Kistrup

Chairman of the Danish Intelligence Oversight Board

Foreword

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

In 2017, the Oversight Board focused especially on consolidating and strengthening its work with regard to risk and materiality assessment of the Danish Security and Intelligence Service (*DSIS*), the Danish Defence Intelligence Service (*DDIS*) and the Danish Centre for Cyber Security (*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.

As an element of these efforts, in October 2017, the Oversight Board hosted a Nordic intelligence oversight conference in cooperation with the Parliamentary Intelligence Services Committee. The theme of the conference was intelligence oversight quality assurance, including whether it was possible to identify some common oversight standards and methods for the Nordics.

Furthermore, in the autumn of 2017, a new chairman and two new members were appointed to the Oversight Board.

The aim of this annual report is to provide general information about the nature of the oversight activities performed with regard to the Danish Defence Intelligence Service (*DDIS*). The report also provides information about the aspects which the Oversight Board decided to examine more closely in 2017 and statistical data on the number of instances where the processing of personal information by the Danish Defence Intelligence Service (*DDIS*) has been found by the Oversight Board to be in violation of the legislation regarding DDIS.

Michael Kistrup

Chairman of the Danish Intelligence Oversight Board

1 About the Danish Defence Intelligence Service (DDIS)

The Danish Defence Intelligence Service (*DDIS*) is tasked with the main responsibility of being:

- Denmark's foreign and military intelligence service,
- Denmark's military security service, and
- the national IT security authority (except within the area of the Danish Ministry of Justice, where this authority lies with the Danish Security and Intelligence Service (*DSIS*).

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 gathering disciplines:

- Signals Intelligence (SIGINT), which is electronic gathering of different types of signals, including data transfers between computer networks, telecommunications, etc. The SIGINT activities are carried out at permanent intelligence gathering facilities in Denmark or facilities abroad.
- Computer Network Exploitation (CNE), which means electronic intelligence gathering 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), which is physical intelligence gathering 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), which is intelligence based on images obtained from different sensors.

- Open Source Intelligence (OSINT), which is sophisticated and systematic collection of intelligence from open sources, typically publicly available information from the internet etc.

DDIS's role as the 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 the military security service, DDIS also acts as the national security authority in the areas under the Danish Ministry of Defence.

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

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

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

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

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

2 The Danish Intelligence Oversight Board

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

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

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

The members are:

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

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

The Oversight Board is supported by a secretariat which is subject solely to the instructions from the Oversight Board in the performance of its duties. The Oversight Board recruits its own secretariat staff and also decides which educational and other qualifications the relevant candidates must have. At the end of 2017, the secretariat consisted of a legal head of secretariat, who is in charge of the day-to-day management of the secretariat, a deputy, two lawyers, an IT consultant and an administrative employee.

> 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.

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 the Danish Security and Intelligence Service (*DSIS*) and to other Danish administrative authorities, private individuals or organisations, foreign authorities, and international organisations, and
- the prohibition of processing information about natural persons resident in Denmark solely on grounds of their legal political activities.

The Oversight Board must oversee by way of compliance checks that DDIS processes information about natural and legal persons resident in Denmark in compliance with the legislation regarding DDIS, 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 the legislation regarding DDIS. The Oversight Board will verify that this is not the case and then notify the person in question (*the indirect subject access request system*). According to the legislative history of the Act, it must only be possible to infer from the Oversight Board's reply that no information is being processed about the data subject in violation of the legislation regarding DDIS. 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 the legislation regarding DDIS or whether information is being processed in compliance with the legislation regarding DDIS.

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

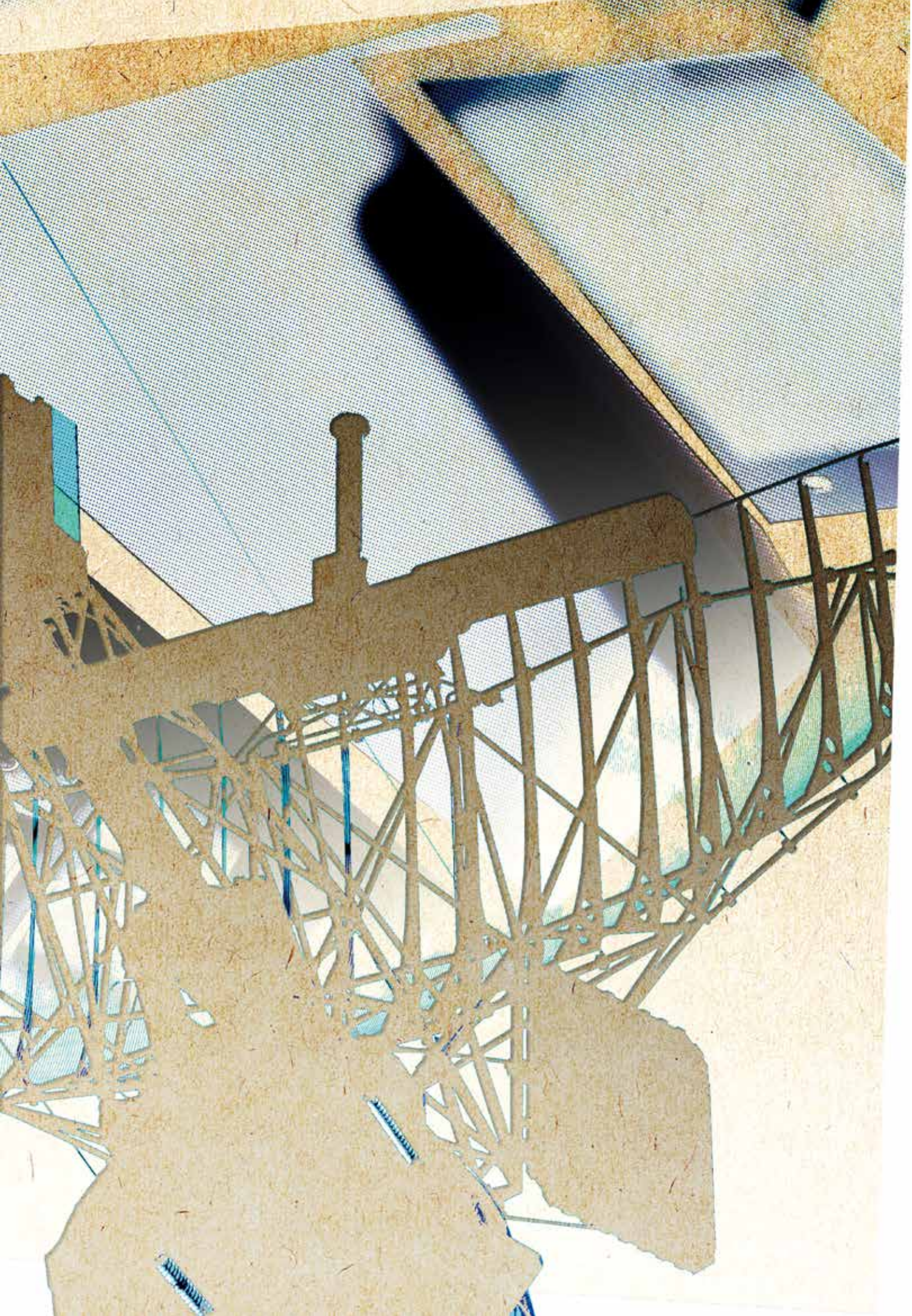
The Oversight Board generally has no authority to order DDIS to implement specific measures in relation to data processing. However, the Oversight Board may issue statements to DDIS providing its opinion on matters such as whether DDIS's complies with the rules concerning processing of information. If 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 the legislation regarding DDIS, 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 the legislation regarding DDIS.

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 the legislation regarding DDIS, including the number of instances where the Oversight Board has ordered DDIS to erase information under the indirect subject access request system.

The Oversight Board issued its most recent annual report on its activities to the Minister of Defence in May 2017. The annual report was submitted to the Parliamentary Intelligence Services Committee and then published in July 2017.



2.4 The Oversight Board's work and focus areas in 2017

In 2017, the Oversight Board carried out an in-depth and intensive compliance check with regard to DDIS's processing of information about natural and legal persons resident in Denmark. As in previous years, the Oversight Board gave priority to checks focusing on DDIS's compliance with the rules concerning procurement of information, time limits for erasure and disclosure of information. In this connection, the Oversight Board also checked that DDIS did not process information in violation of the provision on legal political activity.

In addition, the Oversight Board gave priority to checks of DDIS's compliance with the rules on security measures (information security) in connection with the processing of personal information. In this connection, the Oversight Board retained an external consultancy firm to provide assistance. The Oversight Board furthermore initiated a process to map out and verify the DDIS system landscape. The work involved in checking information security and mapping out and verifying the DDIS system landscape was not completed in 2017 and will therefore continue in 2018.

The Oversight Board organised its check such that its secretariat spent an average of three days per week at DDIS where the secretariat performed checks and met with DDIS staff to clarify issues etc. The results of the checks were presented to the Oversight Board at monthly meetings where it was decided, among other things, whether specific information etc. had given rise to additional questions to DDIS. In the course of the year, the Oversight Board furthermore participated in various meetings with DDIS for discussion of topics of a specific nature prompted by the checks performed and of a more general nature.

The Oversight Board's choice of focus areas is based on a risk and materiality assessment of which aspects in particular could be expected to be problematic and, similarly, the choice of method was adjusted to reflect the individual focus areas. In 2017, the Oversight Board had particular focus on consolidating and strengthening its materiality and risk assessment work with regard to the Danish Security and Intelligence Service (*DSIS*), the Danish Defence Intelligence Service (*DDIS*) and the Danish Centre for Cyber Security (*CFCS*) and 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.

> In cooperation with the Parliamentary Intelligence Services Committed, the Oversight Board also hosted a Nordic intelligence oversight conference. The theme of the conference was quality assurance of intelligence oversight, including whether it was possible to identify some common oversight standards and methods for the Nordics.

In 2017, the Oversight Board retained a consultancy firm, which has assisted in providing increased insight into the compliance checks with the rules on security measures in connection with processing of personal information and implementation and management of the ISO 27001 standard. It is a requirement under the Danish Government's National Strategy for Cyber and Information Security from 2014 that government authorities must implement the international security standard.

Also in 2017, the Oversight Board further developed its relationship with foreign oversight bodies which in different ways oversee their own national intelligence services in order to gain experience at an international level. In this context, the Oversight Board was in a dialogue with its counterparts in Belgium, the Netherlands, Norway, Switzerland and Sweden about general issues of relevance to its own activities.

In cooperation with the Parliamentary Intelligence Services Committed, the Oversight Board also hosted a Nordic intelligence oversight conference. The theme of the conference was quality assurance of intelligence oversight, including whether it was possible to identify some common oversight standards and methods for the Nordics.

3 The Oversight Board's oversight of DDIS in 2017

Every year, the Oversight Board prepares a risk assessment concerning processes and systems at DDIS which is used in relation to DDIS's procurement, internal processing and disclosure of information about persons resident in Denmark, for the purpose of assessing the risk of non-compliance. The risk assessment is intended to ensure that the Oversight Board's oversight activities cover all aspects of DDIS's processing of such information. 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 risk analysis further forms the basis of the Oversight Board's choice of check method in relation to the individual focus area, including whether to perform a full check, a random check, a targeted check or an interview-based check.

Before any checks are performed on an area where no check has been performed before, the Oversight Board's secretariat will hold a meeting with DDIS in order to ensure an adequate professional and technical understanding of the area from an intelligence perspective to allow the check to be appropriately adjusted and performed.

The Oversight Board's direct accesses to DDIS's systems ensure the unpredictability of the DDIS checks performed as the individual checks may be performed without prior notice. DDIS may be notified in advance of the timing and method of a check, if so deemed appropriate by the Oversight Board in relation to the purpose of the check.

On that basis, the Oversight Board's secretariat will perform the checks of the individual areas, and DDIS will be requested to provide additional information if this is found to be relevant on the basis of the checks performed.

The result of the checks will then be submitted 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.

3.1 Own motion checks

For the purpose of overseeing DDIS's compliance with the provisions of the DDIS Act regarding processing of information about natural and legal persons resident in Denmark, the Oversight Board carried out the following checks in 2017 of DDIS's:

- electronic obtaining of raw data (SIGINT) (3.1.1),
- targeted electronic intelligence obtaining (SIGINT), including under section 3(3) of the DDIS Act (3.1.2),
- raw data search, including under section 3(3) of the DDIS Act (3.1.3),
- collection of open source intelligence (OSINT) (3.1.4),
- computer network exploitation (CNE) (3.1.5),
- physical gathering of intelligence (HUMINT) (3.1.6),
- processing of information in electronic analysis and documentation systems as well as other systems (3.1.7),
- disclosure of information to the Danish Security and Intelligence Service (*DSIS*) and foreign partners (3.1.8),
- work stations (3.1.9), and
- DDIS's internal controls (3.1.10).

In addition, the Oversight Board has given priority to checking DDIS's compliance with the rules on security measures in connection with the processing of personal information (information security) and initiated a process to map out and verify the DDIS system landscape. The work involved has not been completed in 2017 and will therefore continue in 2018.

Summary of the Oversight Board's checks in 2017

The Oversight Board's checks concerning DDIS's procurement of information about persons resident in Denmark verified DDIS's general compliance with the provisions of the legislation on procurement of information, including the fact that DDIS adopts a general criterion of legitimacy for electronic procurement of information.

However, the checks showed that in four instances DDIS engaged in unlawful targeted procurement of information about persons resident in Denmark for a total of 20 days in 2014, eight months in 2014-2015, four days in 2016 and 17 months in 2016-2017. The checks further showed that in 20 percent of the samples drawn DDIS made unlawful searches in raw data. In the Oversight Board's opinion, the unlawful instances of procurement, including searches in raw data, were in the nature of negligent actions in all cases. Similarly, the Oversight Board notes that since the publication of the Oversight Board's annual report for 2016 DDIS has taken a number of measures to reduce the number of errors. For one thing, DDIS has intensified its internal controls in the area and strengthened and targeted its staff training.

The Oversight Board's checks of DDIS's internal processing and disclosure of information about persons resident in Denmark and the provision on legal political activity, see sections 3.1.2 and 3.1.7-3.1.9 verified DDIS's general compliance with the provisions of the legislation in this regard.

However, the checks showed that in some instances, DDIS should have erased information about five persons resident in Denmark, see section 3.1.2. In addition, the check of DDIS's processing of information in its electronic analysis and documentation systems and other systems, see section 3.1.7, and the check of a sample of work stations, see section 3.1.9, showed that in a total of two instances DDIS held information about persons resident in Denmark in violation of DDIS' internal guidelines.

Furthermore, the checks showed, see section 3.1.8, that in a few instances DDIS was not in possession of documentation of the reason underlying the legal approval of a disclosure of information about persons resident in Denmark and that DDIS did not carry out logging of a system sampled for disclosure of information.

The check concerning DDIS's internal checks, see section 3.1.10, showed that DDIS has generally organised and carried out its internal controls in a satisfactory manner.

3.1.1 Checks concerning electronic obtaining of raw data (SIGINT)

In its electronic intelligence gathering – also called *Signal Intelligence* (SIGINT) – DDIS gathers very large amounts of non-processed data, also known as raw data, which are characterised by the fact that until they are exposed to processing, it is not possible to determine what information may be retrieved from these data.

DDIS's compliance with the legislation concerning gathering of intelligence means in relation to electronic obtaining of raw data that such obtaining must be for legitimate reasons as regards DDIS's intelligence related activities directed at conditions abroad and that any intelligence which concerns persons resident in Denmark is received by DDIS only by chance. For the purpose of its compliance check among other things, in 2017 the secretariat of the Oversight Board carried out inspections at DDIS's premises where specified electronic intelligence gathering systems were inspected.

At the inspections, DDIS answered questions from the secretariat concerning the technical set-up of the systems and DDIS's information handling procedures concerning information about persons resident in Denmark. The secretariat prepared summaries and requested DDIS's comments to ensure that the secretariat had understood the workings of the systems etc. correctly. In that connection, the secretariat also requested further information about logging of the individual systems.

On that basis, the results of the inspections were submitted to the Oversight Board for its decision as to whether sufficient information had been obtained or whether further details or discussions with DDIS were required.

! **Comments by the Oversight Board**

The checks concerning electronic obtaining of raw data and the subsequent discussion thereof with DDIS verified that DDIS applies a general criterion of legitimacy in its electronic obtaining of raw data and that information concerning persons resident in Denmark is generally received by DDIS only by chance.

3.1.2 Checks concerning targeted electronic intelligence obtaining (SIGINT), including under section 3(3) of the DDIS Act

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

DDIS's compliance with the legislation regarding obtaining of intelligence means in relation to electronic obtaining of intelligence targeted at a person resident in Denmark that such obtaining must be based on a court order obtained by DDIS, see section 3(3) of the DDIS Act, or at the request of the Danish Security and Intelligence Service (*DSIS*) based on a court order obtained by DSIS.

Under section 3(3) of the DDIS Act, DDIS is authorised to collect information about a Danish resident when such person is abroad and there are specific reasons to believe that such person participates in activities that may involve or increase a threat of terrorism against Denmark and Danish interests. If the collection of information results in an interception of communications occurring, DDIS must obtain a court order, as mentioned above.

For the purpose of its compliance check in this regard, in 2017 the Oversight Board's secretariat carried out regular random checks concerning Danish related selectors tasked in DDIS's systems for electronic obtaining and selectors belonging to all persons in respect of whom DDIS had obtained a court order for interception of communications under section 3(3) of the DDIS Act. The secretariat checked logs for the selectors sampled and, based on a specific assessment, requested DDIS's clarifying comments. On that basis, the results of the checks were submitted to the Oversight Board for its decision as to whether sufficient information had been obtained or whether further details or discussions with DDIS were required.

! **Comments by the Oversight Board**

The regular random checks concerning DDIS's targeted electronic obtaining of intelligence, including under section 3(3) of the DDIS Act, showed that on four occasions, DDIS had gathered intelligence about persons resident in Denmark in violation of the legislation for a total of 20 days in 2014, eight months in 2014-2015, four days in 2016 and 17 months in 2016-2017. In the Oversight Board's opinion, the unlawful instances of procurement were in the nature of negligent actions in all cases.

Similarly, the checks showed that in some instances, DDIS should have erased information about persons resident in Denmark, and DDIS agreed.

3.1.3 Checks concerning raw data search, including under section 3(3) of the DDIS Act

It follows from the principle in section 3 of the DDIS Act on procurement of intelligence that DDIS is not allowed to search raw data of its own motion if the result may be expected to be mainly information about identifiable persons resident in Denmark, unless the search is based on a court order obtained by DDIS, see subsection (3) of the provision, or if so requested by the Danish Security and Intelligence Service (*DSIS*).

For the purpose of its compliance check in this regard, in 2017 the Oversight Board's secretariat carried out regular random checks concerning DDIS's raw data searches, including searches on selectors used for targeted electronic gathering of intelligence under section 3(3) of the DDIS Act. Based on logs from specific systems, the secretariat drew random samples from among Danish related selectors used by DDIS in its raw data searches and, based on a specific assessment, requested DDIS's clarifying comments. On that basis, the results of the checks were submitted to the Oversight Board for its decision as to whether sufficient information had been obtained or whether further details or discussions with DDIS were required.

! **Comments by the Oversight Board**

The Oversight Board's regular random checks concerning raw data searches and the subsequent discussion thereof with DDIS showed that in 20 percent of the samples DDIS had performed raw data searches in violation of the legislation regarding DDIS 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, the above-mentioned unlawful searches in raw data were in the nature of negligent actions in all cases.

Similarly, the Oversight Board notes that since the publication of the Oversight Board's annual report for 2016 DDIS has taken a number of measures to reduce the number of errors. For one thing, DDIS has intensified its internal controls in the area and strengthened and targeted its staff training.

3.1.4 Checks concerning collection of open source intelligence (OSINT)

DDIS's collection of intelligence via open sources, also known as *Open Source Intelligence* (OSINT), includes sophisticated and systematic collection of information from the internet and various other sources, e.g. communication in open internet forums, and print media, etc.

DDIS's compliance with the legislation concerning open source intelligence only requires that the information may be of significance to DDIS's intelligence related activities directed at conditions abroad and that the information must be publicly available. Thus, collection differs from electronic gathering, among other things by the fact that DDIS is allowed to perform targeted intelligence gathering directed at persons resident in Denmark on its own initiative, provided that the requirements mentioned are satisfied, see section 3.1.2.

For the purpose of its compliance check of the legislation concerning gathering of open source intelligence, in 2017 the Oversight Board's secretariat drew a random sample from among all selectors relating to persons resident in Denmark about whom DDIS had collected information via open sources. Based on a specific assessment, the secretariat requested DDIS's clarifying comments and on that basis, the results of the checks were submitted to the Oversight Board for its decision as to whether sufficient information had been obtained or whether further details or discussions with DDIS were required.

! **Comments by the Oversight Board**

The check regarding DDIS's collection of open source intelligence verified DDIS's compliance with the legislation regarding DDIS concerning procurement of information.

3.1.5 Checks concerning computer network exploitation (CNE)

Computer network exploitation means DDIS's electronic gathering of intelligence from computer networks which typically require that the data subject obtains access to closed internet forums, IT systems and computers, and that the data subject thus has considerable IT insight.

DDIS's compliance with the legislation concerning intelligence gathering requires in relation to computer network exploitation that intelligence concerning persons resident in Denmark may be received by DDIS only by chance, unless the information is collected based on a court order obtained by DDIS, see section 3(3) of the DDIS Act, or if so requested by the Danish Security and Intelligence Service (*DSIS*) based on a court order obtained by DSIS.

For the purpose of its compliance check in this regard, in 2017 the Oversight Board's secretariat carried out checks of selected computer network exploitation operations. Based on a specific evaluation, the secretariat requested DDIS's clarifying comments and, on that basis, the results of the check were submitted to the Oversight Board for its decision as to whether sufficient information had been obtained or whether further details or discussions with DDIS were required.

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

3.1.6 Checks concerning physical gathering (HUMINT)

DDIS engages in physical gathering of 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 the legislation concerning intelligence gathering 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 if the human intelligence is gathered at the request of the Danish Security and Intelligence Service (*DSIS*).

For the purpose of checking this aspect, in 2017 the Oversight Board's secretariat carried out a check of a sample of human intelligence concerning persons resident in Denmark. Based on a specific assessment, the secretariat requested DDIS's clarifying comments and, on that basis, the results of the check were submitted to the Oversight Board for its decision as to whether sufficient information had been obtained or whether further details or discussions with DDIS were required
.

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

3.1.7 Checks concerning processing of information in electronic analysis and documentation systems and other systems

DDIS processes, including holds, information about natural and legal persons resident in Denmark in various IT systems.

In 2017, the Oversight Board's secretariat regularly drew random samples from DDIS's electronic analysis and documentation systems and other systems concerning information on persons resident in Denmark. The samples were essentially randomly drawn from within all areas covered by DDIS. In connection with the random checks, the secretariat procured and reviewed specific searchable information about the persons sampled and, based on a specific assessment, requested DDIS's clarifying comments. In relation to some of the persons sampled, the secretariat had questions to and/or discussions with DDIS, including concerning the basis for obtaining the information on the persons in question.

On that basis, the results of the random checks were submitted to the Oversight Board for its decision as to whether sufficient information had been obtained or whether further details or discussions with DDIS were required.

! **Comments by the Oversight Board**

The regular random checks in DDIS's electronic analysis and documentation systems verified DDIS's compliance with the provisions of the legislation on procurement, internal processing and disclosure of information and on legal political activity.

However, the checks also showed that in one case DDIS had retained information about persons resident in Denmark in violation of the DDIS guidelines.

3.1.8 Checks concerning disclosure of information to DSIS and foreign partners

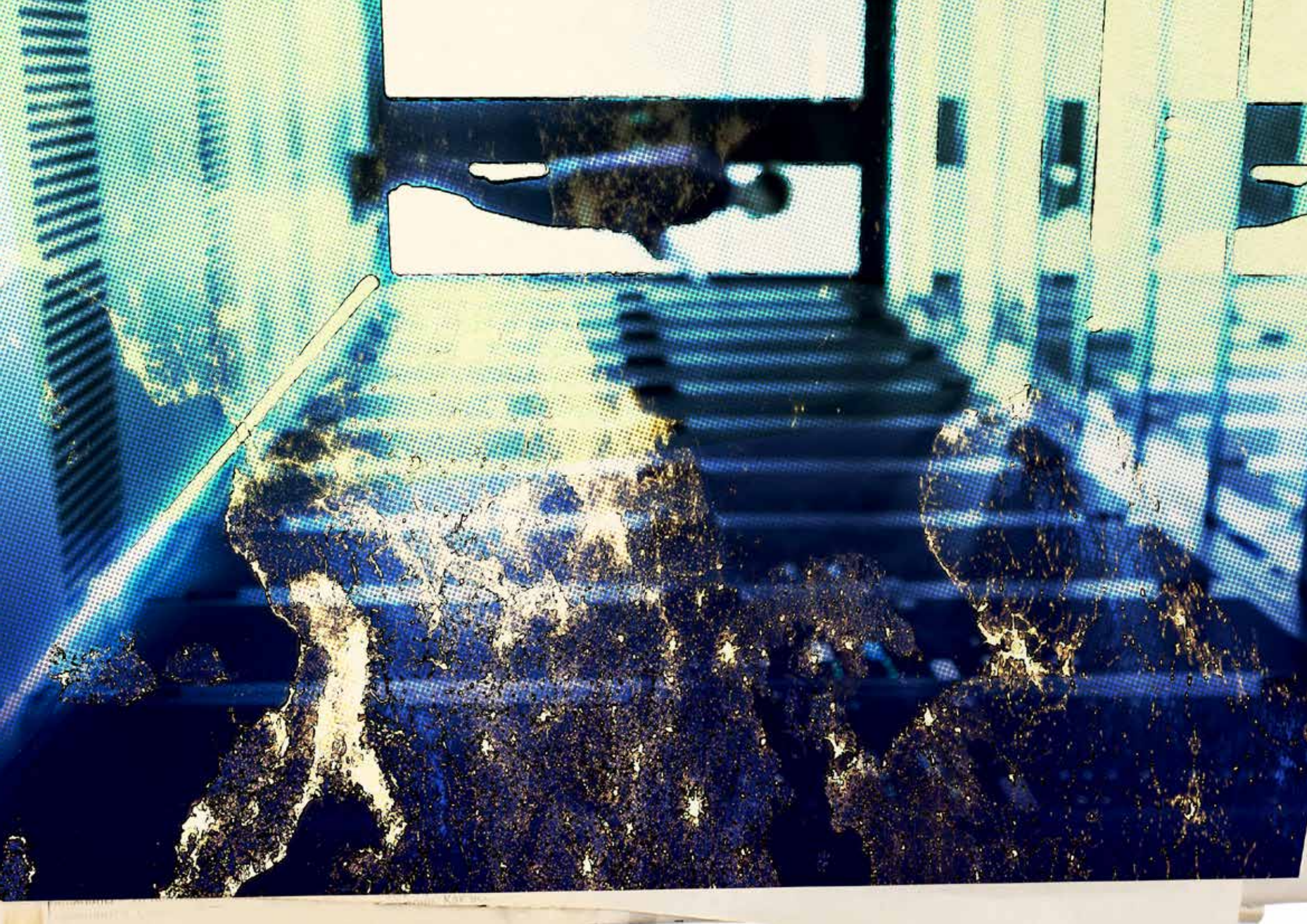
In 2017, the Oversight Board performed regular random checks of DDIS's disclosure of information about persons resident in Denmark to DSIS and foreign partners and checks of selected systems in support thereof.

Based on a specific assessment, including whether a disclosure was deemed to be sound, the Oversight Board's secretariat requested DDIS's clarifying comments, and the comments were then submitted to the Oversight Board for its decision as to whether sufficient information had been obtained about the individual disclosure and systems in support thereof or whether further details or discussions with DDIS were required.

! **Comments by the Oversight Board**

The Oversight Board's regular checks concerning DDIS's disclosure of information to DSIS and foreign partners, including systems in support thereof, verified DDIS's compliance with the provisions of the legislation on disclosure of information.

However, the checks showed that in a few instances DDIS was not in possession of documentation of the reason underlying the legal approval of a disclosure of information about persons resident in Denmark. The Oversight Board encouraged DDIS to ensure that documentation is obtained in all cases. Furthermore, the check showed that DDIS did not carry out logging of a system sampled for disclosure of information. The Oversight Board encouraged DDIS to implement system logging, which was soon implemented by DDIS.



3.1.9 Check of work stations

In 2017, the Oversight Board performed a check of a number of staff work stations, focusing on the staff's processing of information about persons resident in Denmark, including their knowledge of the rules in this area.

Within two DDIS departments, the Oversight Board's secretariat checked a number of randomly chosen work stations, including their drives, Outlook folders, external storage devices and documents in hard copy. In connection with the check performed of the information held on each of the work stations, the secretariat asked questions to the individual staff members in question about their knowledge of the rules on processing, including erasure, of information about persons resident in Denmark. When asked, a majority of the staff informed the secretariat that they had erased information from their work stations before the check.

The secretariat discussed the results of the checks with DDIS and requested DDIS's clarifying comments on the results of the checks, and the results of the checks were then submitted to the Oversight Board for its decision as to whether sufficient information had been obtained or whether further details or discussions with DDIS were required.

! **Comments by the Oversight Board**

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

However, the check also showed that in one case a staff member processed information about persons resident in Denmark in violation of DDIS's internal guidelines as the staff member in question retained information which he or she believed was no longer relevant to process there.

3.1.10 Check concerning DDIS's internal controls

In the course of its oversight of DDIS in 2017, the Oversight Board also performed a check of DDIS's internal controls. The check comprised all DDIS internal controls in 2017 as well as DDIS's planning of the same for 2018, and was carried out by reviewing documentation provided and engaging in discussions with DSIS.

In its review of DDIS's internal controls, the Oversight Board based itself, among other things, on a report submitted by an audit and consultancy firm concerning internal controls and the Oversight Board's scope for verification, which is based on international standards and guidelines for good auditing practice and test of internal controls (International Standards on Auditing) and on the "Good public sector auditing practice" issued by the Danish National Audit Office (*Rigsrevisionen*).

DDIS has kept the Oversight Board informed of its internal checks of selected systems which are used to obtain information. In addition, DDIS has provide written details of its organisation

of internal controls, including by forwarding DDIS's risks analysis concerning compliance with statutory requirements and the status in this area has been discussed at a meeting between DDIS and the Oversight Board.

! **Comments by the Oversight Board**
The check verified that DDIS has generally organised and carried out its internal controls in a satisfactory manner.

3.2 DDIS's briefing of the Oversight Board

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

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

The Oversight Board was kept informed of important issues concerning DDIS's processing of information about natural and legal persons resident in Denmark and concerning updating of administrative guidelines.

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

3.3.1 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 the legislation regarding DDIS, the secretariat 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 secretariat will endeavour to identify all information which DDIS is processing about a data subject who has submitted an indirect request. With a view to providing the greatest possible assurance that all information about the data subject has been identified, the secretariat will subsequently ask DDIS to check if it is processing further information about the data subject.

When the process has been completed, the Oversight Board will assess whether, in the Oversight Board's view, DDIS is processing information about the data subject in violation of the legislation regarding DDIS. If the Oversight Board concludes that this is the case, the Oversight Board will

order DDIS to erase such information. When the Oversight Board has verified that DDIS is no longer processing any personal information about the data subject in violation of the legislation regarding DDIS, 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 in this regard, the secretariat 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.

3.3.2 Number of requests and processing time

In 2017, the Oversight Board received subject access requests from five natural or legal persons, asking the Oversight Board to check if DDIS was processing personal information about them in violation of the legislation regarding DDIS. The Oversight Board did not in any of the cases find this to be the case. Nor did the Oversight Board 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 five processed requests was 41 days, 13 days of which were DDIS's processing time. Compared with 2016, the average processing time was reduced by one day.

The Oversight Board will endeavour to answer subject access requests as quickly as possible, but since this may be a quite resource-intensive and complicated process, as already mentioned, since the Oversight Board must present the results to DDIS before making a decision in the matter at a monthly meeting, and since in early 2018 the Oversight Board received a substantial number of enquiries compared with previous years, it will hardly be possible to further reduce the processing time in 2018.

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

Appendix

LEGAL FRAMEWORK

1) The Danish Defence Intelligence Service (*DDIS*) Act (Consolidated Act No. 1287 of 28 November 2017) (the "DDIS Act"), and
2) The Danish Act on processing of personal data (Act No. 429 of 31 May 2000, as amended by Act No. 639 of 12 June 2013) (the "Data Protection Act"), sections 3, 5, 11(1), 14, 41(1)-(4) and 42.

1. Procurement of information

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

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

The most important purpose of this provision is to emphasise that in its intelligence related activities directed at conditions abroad DDIS is entitled to collect and obtain data, including raw data (see the appendix, section 2.1), among other things through electronic and physical intelligence 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 obtaining of raw data 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 obtaining is subject to a request from the Danish Security and Intelligence Service (*DSIS*), unless the conditions in section 3(3) of the Act are satisfied (see section 1.2). Information which is obtained at the request of DSIS will not be obtained by DDIS by chance, regardless of the obtaining method used.

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 intelligence 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.

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

1.2 About obtaining of information under section 3(3) of the DDIS Act

Act No. 1571 of 15 December 2015 (Strengthening the effort to combat activities abroad which may involve a terrorist threat against Denmark and Danish interests) amended the DDIS Act, strengthening DDIS's scope for gathering information about Danish extremists abroad, particularly foreign fighters, in the early phases of intelligence gathering.

In section 3(3), the new Act authorises DDIS to initiate targeted gathering 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. 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 DDIS Bill, the amendment will not change the fundamental allocation of responsibilities and mode of cooperation between the Danish Security and Intelligence Service (*DSIS*) and DDIS. Consequently, the two intelligence services will still work closely together and the information obtained under the new provisions will thus be shared with DSIS and the latter will also still be allowed to disclose information to DDIS about foreign fighters and the like. Nor will the amendment change the current state of the law which allows DDIS to obtain information about natural and legal persons resident in Denmark at the request of DSIS, if necessary, by court order. If a court order is available based on the provisions of the Danish Administration of Justice Act (*retsplejeloven*), those provisions will continue to form the basis of DDIS's targeted obtaining of information about persons resident in Denmark. The scope of the provision is the early phase of intelligence obtaining when the conditions for obtaining a court order for interception of communications under the provisions of the Danish Administration of Justice Act are not satisfied. Information about natural persons resident in Denmark which is obtained under this provision will fall within the scope of the Oversight Board's oversight of DDIS, and DDIS's processing of information obtained under the provision thus forms part of the Oversight Board's annual report on its activities concerning DDIS.

The explanatory notes to the DDIS Bill concerning its individual provisions specify with regard to section 3(3) that the provision may be applied only if there is a presumption that the person in question is not physically located in Denmark. The activities that may be authorised under the provision include the situations where a person abroad through their activities or through support to others engages in activities that may involve or increase a threat of terrorism against Denmark and Danish interests.

2. Internal processing of information

2.1 About internal processing of information under sections 4 and 5 of the DDIS Act

Under the provisions of sections 4(1) and 5(1) of the DDIS Act, a number of the provisions of the Data Protection Act apply to DDIS's processing of information collected, obtained and received about natural and legal persons resident in Denmark. According to the explanatory notes to the DDIS Bill concerning the provisions, the same general data protection principles etc. will generally apply to the determination of which fundamental conditions must be satisfied by DDIS when processing the said personal information as those applying to other Danish authorities when processing personal information. In this regard, DDIS is subject to section 5 of the Data Protection Act, which among other things lays down the requirements of legitimacy and proportionality of processing, including the requirement that a processing operation must not be incompatible with the purposes for which the information was collected and that personal information which has been collected and obtained must not be held in identifiable form longer than necessary. Also, sections 41(1)-(4) and 42 of the Data Protection Act on security of processing apply to DDIS's processing of information about persons resident in Denmark.

Under sections 4(2) and 5(2) of the Act, DDIS is allowed to process any information about natural and legal persons resident in Denmark if:

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

Under sections 4(2)(ii) and 5(2)(ii) of the Act, DDIS is thus authorised to process any information about natural and legal persons resident in Denmark if processing *may be assumed to be of importance* to the performance of DDIS's activities as intelligence service etc. The condition that the information may be assumed to be of importance to DDIS's performance of those activities reflects the requirement of a somewhat substantive presumption that the information DDIS wishes to process will be of importance to DDIS's performance of those activities.

Under sections 4(2)(iii) and 5(2)(iii) of the Act, DDIS is authorised to process any information about natural and legal persons resident in Denmark if processing *is necessary* for the performance of DDIS's activities as military security service. The condition that the information must be necessary for DDIS's performance of those activities reflects the requirement that, based on an assessment in each individual case, DDIS may be assumed to have a genuine need to process the information in question in order to perform its activities as military security service.

In its electronic intelligence gathering, DDIS gathers 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 they are exposed to processing, 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 Data Protection Act 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 obtaining of raw data in section 5(2) of the Data Protection Act, a general requirement of legitimacy must be applied with regard to the obtaining of raw data, as such obtaining must be for legitimate reasons. In addition, the principles also mean 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.

2.2 About erasure of information, see section 6-6a of the DDIS Act

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

It follows from the provision in section 6a(1) that when DDIS becomes aware in connection with its activities that cases or documents, etc. no longer meet the conditions of processing in sections 4(2) and 5(2), they must be erased, regardless of whether the time limit for erasure of information in section 6(1) has expired, but that DDIS is not required beyond that to review its cases and documents, etc. of its own motion in order to assess if the above conditions of processing are still met.

In the notes to the individual provisions of the Bill, it is specified with regard to section 6a(1) that the term "activities" is to be understood in the broad sense as encompassing all the tasks that DDIS is engaged in. Thus, by way of example, in addition to operational activities, the term also includes DDIS's tasks in connection with indirect subject access requests, see section 10 of the Act, and random checks performed by the Oversight Board.

It follows from the provision in section 6a(2) that notwithstanding the provisions of 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(2) and 5(2) 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(2) and 5(2) 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 case 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 the legislation regarding DDIS, 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.

2.3 About security of processing (information security), see sections 41(1)-(4) and 42 of the Data Protection Act

As already mentioned, as a result of sections 4 and 5 of the DDIS Act, sections 41(1)-(4) and 42 of the Data Protection Act on security of processing also apply to DDIS's processing of information that is collected, obtained and received about natural and legal persons resident in Denmark.

Under section 41(1) of the Data Protection Act, individuals, companies, etc. performing work for the data controller or data processor and having access to information may process this information only on instructions from the data controller, 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 the controller authorises an employee or others to access particular information. The requirement that the person etc. in question may only process information in accordance with the controller's instructions means, among other things, that the person etc. may not process information for other purposes than those laid down by the controller – including for own purposes – and that the person etc. in question may not process information on instructions from other parties than the controller.

The controller must implement appropriate technical and organisational security measures to protect the information against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in violation of the provisions laid down in the Act, and the same applies to processors, see section 41(3) of the Act. For information which is being processed for the public administration 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 41(4) of the Act.

Executive Order No. 528 of 15 June 2000 on security measures to protect personal information being processed on behalf of the public administration (the Executive Order on Security Measures) provides more detailed rules on the security measures referred to in section 41(3) of the Danish Data Protection Act. Notwithstanding that the Executive Order does not apply to DDIS's processing of personal information, in its assessment of the requirements to security measures the Oversight Board has also taken into account the provisions of the Executive Order, including sections 5 and 19.

Section 5 of the Executive Order on Security Measures provides, among other things, that the data controlling public authority must adopt a set of guidelines for its monitoring of compliance with the security measures laid down by the authority, see the fourth sentence of sub-section (1). In addition, subsection (2) of the same section provides that the internal regulations must be revisited at least once a year in order to ensure that they are adequate and reflect the actual circumstances prevailing in the authority.

Section 19 of the Executive Order on Security Measures provides that all uses of personal information must be subject to machine registration (logging). The log must at least provide information about the time, user, type of use and identification of data subject or the search criterion used. The log must be kept for six months, and then be erased. Public authorities with a specific need therefor may keep the log for up to five years. The provision in subsection (1) does not apply to personal information which forms part of word processing documents and the like which are not in their final form, and the same is true of such documents in their final form if erasure is effected within a relatively short period of time specified by the data controlling public authority, see section 19(2).

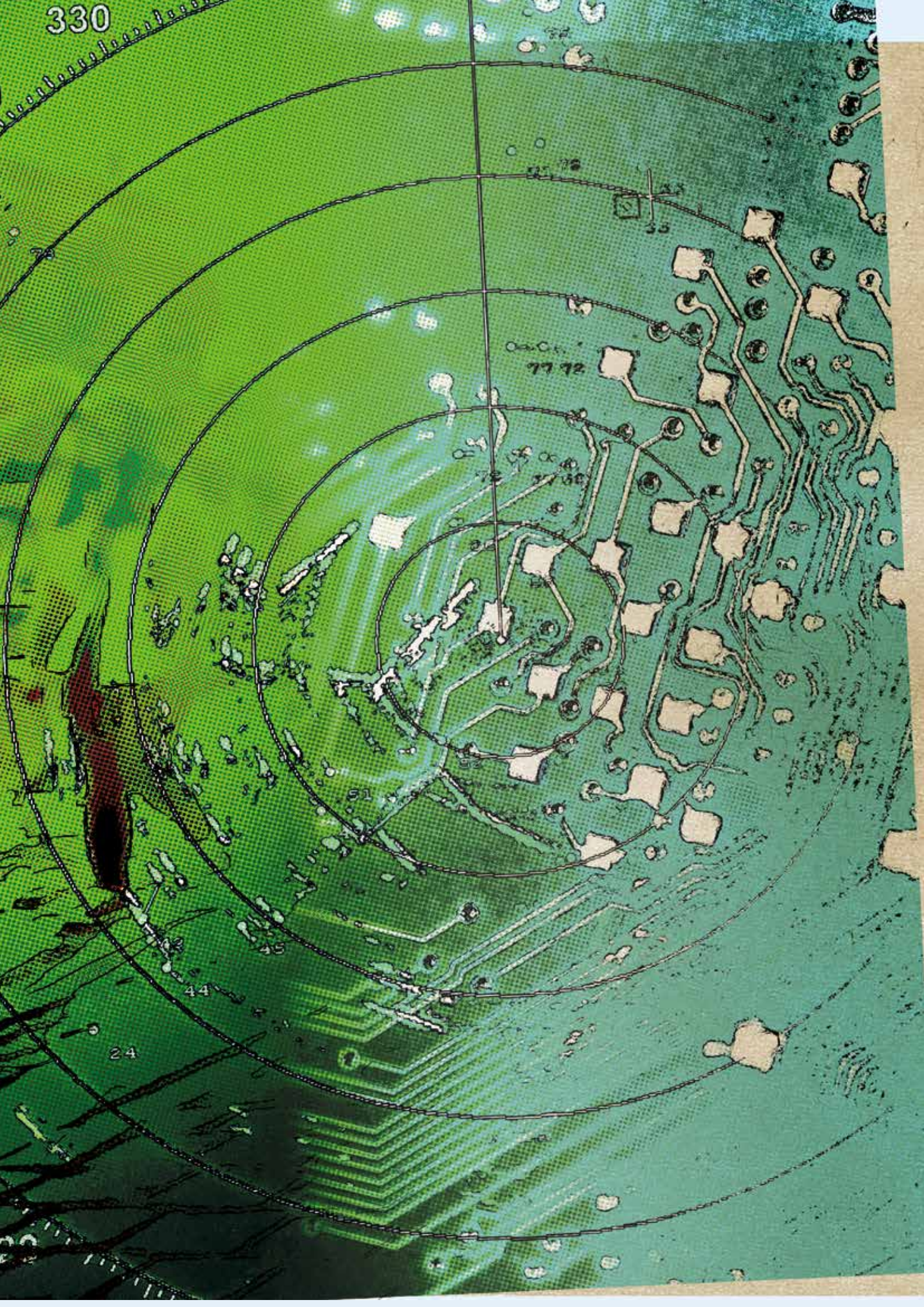
When a controller makes information available for processing by a processor, the controller must ensure that the processor is able to implement the technical and organisational security measures mentioned in section 41(3)-(4) of the Act, and must oversee that this is done, see section 42(1) of the Act. If a controller makes information available for processing by a processor, the parties must conclude a written agreement, see section 42(2) of the Act.

3. Disclosure of information

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 the Danish Security and Intelligence Service (*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 section 4 of the DDIS Act. Disclosure of sensitive personal information as mentioned in sections 7(1) and 8(1) of the Data Protection Act is also subject to the conditions in section 8(2) of the Data Protection Act. This means that information concerning racial or


330
77 72
44
24

ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or personal information concerning health or sex life, criminal offences, serious social problems and other purely private matters 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 section 5 of the Act must be satisfied.

Having regard to the serious implications which, depending on the circumstances, disclosure may involve for the data subjects, the conditions of disclosure in section 7(2) and (3) are supplemented by a condition in subsection (4) to the effect that DDIS will be allowed to disclose information under subsections (2) and (3) only if the disclosure is deemed to be sound based on a specific assessment in each individual case.

According to the explanatory notes to the DDIS Bill concerning section 7(4), this decision must be based on a test where all factors in each individual case are balanced against each other. In particular, this balancing of factors must include the specific contents of the information, the purpose of disclosure and an assessment of any adverse effects that disclosure may be deemed to involve for the data subject. The outcome of the soundness test may differ, depending on whether the disclosure is to another Danish administrative authority, a private individual or organisation, a foreign authority or an international organisation. For disclosure to foreign authorities, it may be taken into account in the test whether the disclosure of personal information is to be made with a view to preventing and investigating serious international crime which Denmark, too, has a material interest in combating. The conditions prevailing in the country of the recipient may also be taken into account in the test. The provision on disclosure is assumed to be supplemented by rules of a procedural nature issued administratively, which – like the provisions of DDIS's former internal guidelines on cooperation with foreign intelligence services and the like – must include clear provisions on the conditions for disclosure of identifiable personal information to foreign partners. The Oversight Board will be given an opportunity to oversee DDIS's compliance with such rules.

4. Legal political activity

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

Section 8 of the DDIS Act on legal political activity provides in subsection (1) that the participation by a natural person resident in Denmark in legal political activity does not in itself warrant processing of information about that person by DDIS. Subsection (2) provides, however, that the provision in subsection (1) does not preclude DDIS from processing information about a person's political activity with a view to determining if the activity is legal. According to subsection (3), subsection (1) also does not preclude DDIS from including information about the leadership of

political associations and organisations when processing information about such associations and organisations.

With regard to political activity, the explanatory notes to the DDIS Bill concerning section 8 state that this generally means any activity which concerns government and influence of existing societies and social conditions and that political activity not only covers statements but also includes political manifestations in other forms such as participation in political demonstrations.

The prohibition of processing information about legal political activity is not absolute. This will be seen from the expression "not in itself". Thus, DDIS is allowed to process information about a person's legal political activity if there are other factors which mean that a person has attracted DDIS's interest. If the person in question has already become the focus of DDIS in connection with the performance of its activities, DDIS is also allowed to process information about the person's legal political activity if such information is relevant to the inquiries. By way of example, this could be a person who engages in political activity as a pretext for planning, preparing or engaging in espionage, terrorism or violent extremist activity directed at the Danish military. In each individual case, DDIS must thus assess whether processing of information about legal political activity is warranted by other grounds than the very performance of such activity, and such an assessment is inherently discretionary.

Under subsection (2), DDIS is allowed in the course of its investigations to process personal information about a person's political activity with a view to determining if the activity is legal or illegal. If the investigations show that the activity is legal, the personal information must be erased. The Oversight Board may verify that the provision of subsection (2) is not abused to circumvent the prohibition in subsection (1) and thus that DDIS's investigations of whether a given political activity is legal is made in a sound and reasonable manner with due respect of the purpose underlying the prohibition.

Subsection (3) of the provision provides that in cases involving political associations and organisations DDIS is allowed to include information about the leadership of the association or organisation. The prohibition in subsection (1) against processing of information about legal political activity does not include processing of information about legal persons. However, the general rules of the Act on processing of information about legal persons apply to such processing of information.

Information about the leadership only covers identification information about the leaders in question, which in relation to a political association could be members of the general council or executive committee, ministers, members of Parliament and of the European Parliament and members of regional and local councils. Those who do not belong to this category would be ordinary members of a political party, persons supporting others' candidature for political office, delegates as well as participants in seminars, deputations and election meetings.

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

5. Rules on subject access requests etc.

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 the legislation regarding DDIS. 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 the legislation regarding DDIS. 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 the legislation regarding DDIS. The Oversight Board will verify that DDIS is not processing information about the data subject in violation of the legislation regarding DDIS 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 the legislation regarding DDIS. 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 the legislation regarding DDIS or whether information is being processed in compliance with the legislation regarding DDIS.

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.

Annual report 2017
Danish Defence Intelligence Service
Published by the Danish Intelligence Oversight Board, May 2018

Layout + illustrations: Eckardt ApS
Portrait photographs: Lars Engelgaar

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

Members of the Danish Intelligence Oversight Board

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

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