# Review report

## On the collection and further processing of airline passenger data by the AIVD and the MIVD

## CTIVD no. 71

[adopted on 19 August 2020]

Review Committee
on the Intelligence and
Security Services

Review Committee
on the Intelligence
and Security Services

**CTIVD no. 71**

# REVIEW REPORT

**On the collection and further processing of airline passenger data by the AIVD and the MIVD**

# Inhoudsopgave

**CTIVD no. 71**

# REVIEW REPORT

**On the collection and further processing of airline passenger data by the AIVD and the MIVD**

## Summary

This review report concerns the collection and further processing of Advance Passenger Information (API data) by the AIVD and the MIVD. API data is data on passengers of a flight and information about that flight that is stored by the airlines such as name, date of birth, nationality, airport of departure and of arrival. This data is collected routinely and by automated means. The vast majority of this data concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be. For that reason, this is actually the collection and further processing of a bulk data set.

### Scope and investigative question

In this review report, the CTIVD investigates the question whether the AIVD and the MIVD collected and further processed API data lawfully in the period from 1 January 2019 to 1 September 2019. The scope of the investigation is limited to API data. That means that this investigation does not include the collection and processing of other passenger data, such as *Passenger Name Records* (PNR details). Nor does this report investigate other possible bulk data sets that are received from informants, using the investigatory power to request information from organizations or individuals (hereinafter: the investigatory power to use informants).

### Policy for bulk data sets

The vast majority of the API data concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be. For that reason, this is actually the collection and further processing of a bulk data set. On 1 May 2018, both services published the policy document 'AIVD and MIVD policy on the acquisition and processing of bulk data sets' (hereinafter: policy on bulk data sets) on their respective websites. This policy was drafted by the services following the recommendation in the CTIVD's review report no. 55 (2018) on the acquisition, by means of the investigatory power to use informants, of bulk data sets offered on the internet by third parties. The collection and further processing of bulk data sets is a severe infringement of the fundamental rights of those involved. The services' policy for bulk data sets constitutes a more specific interpretation of the general requirements for data processing under the Intelligence and Security Services Act (ISS Act 2017) (Sections 18-24 of the ISS Act 2017). Furthermore, the policy sets the additional safeguards that require the head of service or the relevant minister to authorize the collection (as a further implementation of Section 26 of the ISS Act 2017) and that require data to be minimized. The policy must be applied when it is a bulk data set that is being collected and processed further.

### Procedure for collecting and further processing API data

API data is stored by the airlines and they must provide this information to the Royal Netherlands Marechaussee (KMar) under the EU Directive 2004/82/EC (API directive). The KMar processes the data

for its own tasks – border control. The AIVD collects the API data from the KMar based on a general investigatory power, in this case the power to use informants (Section 39 of the ISS Act 2017).

The AIVD is given the API data by the KMar routinely and by automated means. In the investigation period the AIVD database contained the data of millions of people. The MIVD uses the API data collected by the AIVD but does not collect it directly from the KMar. API data is frequently processed by the AIVD and the MIVD. The information is processed in the context of investigations into organizations and people who are a threat to national security. The information is also used in security screenings.

### Main conclusions of this report

The CTIVD established that the power to use informants that was exercised to collect API data, was *lawful*. The API data is also processed for objectives that fall within the services' tasks (purpose limitation) and it is necessary to process this data to achieve those objectives. The CTIVD does however question whether this interpretation of the power to use informants is sufficiently foreseeable for citizens. This topic deserves consideration, at the least, in the context of the evaluation of the ISS Act 2017.

The services did not, however, classify API data as bulk data sets, in conformity with the AIVD and MIVD's own policy. The specific safeguards listed in the policy for bulk data sets were not or hardly observed in practice. That includes safeguards such as requesting authorization in advance from the head of service or the minister, a strict authorization policy to access the bulk data set and a periodic check if the data sets are still necessary to achieve the objective for which they were collected. This is *unlawful*. That conclusion applies to both the collection of the data and to the further processing of that data. It is the CTIVD's recommendation that these safeguards are also applied to the collection and processing of API data.

Moreover, the CTIVD established unlawful conduct during the data analysis conducted on a large set of API data. This unlawful conduct was mainly caused by shortcomings in recording during the processing of data. Lastly, the CTIVD established unlawful conduct relating to a number of specific data processing activities by the joint Security Screenings Department of the AIVD and the MIVD. These data processing activities were found to be unlawful because they do not fit in with the department's tasks.

### In closing

This review report examines the collection of API data as bulk data set based on a general investigatory power. In addition to this specific data set, other bulk data sets may be collected based on this general investigatory power. The parliamentary debate on the implementation of the PNR Directive notes that the services may gain access to PNR details based on the power to use informants. PNR details are passenger data of flights from within the EU or the Schengen area. Besides API data they also include information about the booking, contact details, payment details and luggage information. Briefly put, the services are able to collect large amounts of data using a general investigatory power such as the power to use informants. The vast majority of this data concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be. For that reason it is vital that both services have a work procedure set up in such a way that there are solid grounds on which to lawfully collect and process information from bulk data sets, whereby the special nature of a bulk data set is taken into account.

Furthermore, regardless of how the bulk data sets are collected, that collection and their further processing must always be adequately enshrined in law. Citizens must be able to foresee that bulk data sets can be collected and further processed by the services, even with a general investigatory power such as the power to use informants. Foreseeability also stretches to the safeguards that are applied. Bulk data sets demand an appropriate set of safeguards as a counterweight to the specific privacy infringements that are inherent to bulk data. The ISS Act 2017 does not lay down any specific rule for

processing bulk data sets based on a general investigatory power, in contrast to the collection and further processing of bulk data sets from investigation-related interception. The investigation shows that legislation does insufficient justice to the protection of the fundamental rights of people who are not the subject of investigation by the services, nor ever will be. This topic deserves consideration, at the least, in the context of the evaluation of the legislation.

**CTIVD no. 71**

# REVIEW REPORT

**On the collection and further processing of airline passenger data by the AIVD and the MIVD**

## 1. Introduction

This review report concerns the collection and further processing of Advance Passenger Information (API data) from airlines by the General Intelligence and Security Service (hereinafter: AIVD) and the Military Intelligence and Security Service (hereinafter: MIVD). The vast majority of this data concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be. For that reason, this is actually the collection and further processing of a bulk data set.

The passenger data is collected to enable the services to carry out their tasks and it gives them a picture of people's travel movements. For example, the services can learn from passenger data that a member of a terrorist organization is taking a flight to the Netherlands. Passenger data, just like any bulk data set, can also be used to identify and recognize targets in the services' focus areas.[1]

### Background to the investigation

The Review Committee on the Intelligence and Security Services (hereinafter: CTIVD) established in report 55 on the acquisition of bulk data sets offered on the internet (2018) that a large amount of data can be and is collected using the general investigatory power to request information from administrative authorities, public sector workers and other people or organizations (hereinafter: the investigatory power to use informants).[2] At the time, the CTIVD announced in this report that it would conduct further investigation into the power to use informants as exercised by the services.

The AIVD and MIVD's core activity is the processing, and therefore also the collection, of data to carry out their tasks to protect national security.[3] Collecting bulk data sets by investigation-related interception was the subject of much political and public debate on the new Intelligence and Security Services Act (hereinafter: ISS Act 2017). However, the possibility that bulk data sets could be collected using a general investigatory power was neglected. A general investigatory power, such as the power to use informants, can be deployed to collect large amounts of data. Processing that data can lead to a serious infringement of the fundamental rights (such as the right to privacy) of those involved. The evaluation of the ISS Act commenced in May 2020 and the findings from this current investigation are intended to contribute to the evaluation of this piece of legislation.

1 See www.aivd.nl/onderwerpen/werken-met-grote-datasets.
2 Review report of the CTIVD no. 55 on the acquisition of bulk data sets offered on the internet by third parties by the AIVD and the MIVD, accessible on www.ctivd.nl.
3 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 17.

### Scope of the investigation and investigative question

This investigation focuses on the lawfulness of the collection and further processing of airline passenger data that is collected routinely and by automated means on the grounds of a general investigatory power. The Advance Passenger Information (API data) is collected by the services in this way. The investigative question is as follows:

*Did the AIVD and the MIVD collect and further process API data from airlines lawfully in the period from 1 January 2019 to 1 September 2019?*

This investigation focuses on the collection and further processing of API data. That means that it does not include the collection and processing of other passenger data, such as *Passenger Name Records* (PNR details). Nor does this report investigate other possible bulk data sets that are collected using general investigatory powers, such as the power to use informants.

Nonetheless, the recommendations in this investigation could have an impact on the collection and further processing of data from other bulk data sets that have been collected using a general investigatory power.

### Assessment of practice and procedure

Appendix I to this report contains the assessment framework for collecting and further processing airline passenger data. This assessment framework forms the basis on which to assess the lawfulness of the practice. An 'unlawful' assessment always means that the conduct conflicts with legislation and regulations. Legislation and regulations in this case refers to the ISS Act 2017, case law and the CTIVD's recommendations which were adopted by ministers, based on previous CTIVD review reports.

### Policy for bulk data sets

Both services have published their policy on acquiring (collecting) and processing bulk data sets.[4] In its report 55 (2018), the CTIVD made the recommendation to the services to publish what was then their internal policy on the acquisition of bulk data sets acquired on the internet. The ministers adopted the recommendations from that report. The services interpreted these recommendations into what the CTIVD refers to as 'the policy for bulk data sets'. This policy sets out the general provisions relating to data processing (Sections 18-24 of the ISS Act 2017) more specifically. The services did not, however, classify API data as bulk data sets, which means that the services do not apply their bulk data set policy when collecting and further processing API data.

### Procedure

For its review on the lawfulness of the collected and processed API data, the CTIVD conducted interviews with staff from various teams of both services. Furthermore the CTIVD investigated the logging activities of the application used to process API data. The realization of access to logging data and the analysis of this data was conducted in cooperation with staff from the CTIVD's IT unit. This technical investigation gave direction to the interviews which the CTIVD conducted with staff from the AIVD and MIVD departments who use API data. It also led to specific investigatory activities in the cases where the CTIVD established deviations in the use of the application. This investigatory method is more technical in nature and proved very useful. The investigation method used is described in Appendix II to this report.

### Classified appendix

This report has a classified appendix. This appendix does not contain any reports of unlawful conduct that have not been described in the public review report. The classified appendix contains information

4 The 'AIVD and MIVD policy on the acquisition and processing of bulk data sets' was published on 1 May 2018 on www.AIVD.nl and www.defensie.nl. See also footnote 1.

that can expose the AIVD and the MIVD's modus operandi and their current level of knowledge and was therefore qualified as 'classified'.

### Structure of the report

The report has the following structure. Section 2 sketches the background of the AIVD and the MIVD's use of airline passenger data. Section 3 assesses the lawfulness of the collection of passenger data by the services. Whether the AIVD and the MIVD processed that data further in a lawful manner is examined in Section 4. Lastly, Section 5 of the report describes the conclusions and recommendations.

# 2. Background to API data

Section 2.1 looks at what API data is and on the basis of which legislation and for which purposes the API data should be stored by the airlines. Section 2.2 expands on what was said in the parliamentary debate on the passenger data from airlines used by the AIVD and MIVD to protect national security. Section 2 concludes with final observations on API data and a brief reflection on the foreseeability of the legal grounds to process API data.

## 2.1 API data

API data is information about the passengers and crew of airlines.[5] This data must be stored by the carrier in question under EU Directive 2004/82/EC (API directive). The purpose of storing this data is to improve border control by the competent authorities of EU member states and to prevent illegal immigration.

On 9 July 2007, the Netherlands implemented the API Directive in its Aliens Act, Aliens Decree and its Aliens Regulations.[6] The Netherlands opted to restrict the term 'carrier' to airlines and to appoint the KMar as the competent authority. The API data must be submitted to the KMar before the end of the boarding check (in advance). That allows the authority sufficient time to conduct part of its investigation into the passengers while the trip is underway. In specific terms this means that passenger and flight data on flights to Dutch airports from outside the EU or outside the Schengen area is given to the KMar by the airlines.

Based on the directive and implementation legislation, airlines must store the following passenger data and provide it to the KMar:

- number and nature of the travel document used;
- nationality;
- full name;
- date of birth;
- sex;
- the state issuing the travel document;
- expiry date of the travel document;
- flight number;
- time of departure and arrival of the means of transport;
- the total number of passengers transported by that means of transport;
- border crossing point of arrival;
- first boarding point;
- other itinerary information;
- Passenger Name Record file location.[7]

5 Article 2 of the Directive describes the term 'carrier' as follows: any natural or legal person whose occupation it is to provide passenger transport by air.
6 Bulletin of Acts and Decrees 2007, 252.
7 See Article 3 of Directive 2004/82/EC of 29 April 2004 and the Dutch implementation of that directive in Section 2.2.a of the Act of 9 July 2007 bringing the Aliens Act 2000 into line with Directive 2004/82/EC of the Council of the European Union of 29 April 2004 regarding the obligation for carriers to provide passenger data (Bulletin of Acts and Decrees 2007, 283. Most recently modified in Bulletin of Acts and Decrees 2012, 688). The geographical restriction is due to the responsibilities of the authorities tasked with border control. When a Dutch airport serves as a stopover for a booked flight, data on flights from a Dutch airport is also stored.

### Creation of the API directive

The API Directive was drafted in 2003 at the initiative of Spain, with the aim of preventing illegal immigration and facilitating external border controls.[8] After the terrorist attacks in Madrid in 2004, the proposal for the directive was fast-tracked. On 25 March 2004, the Council of the European Union drafted a declaration on the fight against terrorism. One of the action points in the declaration was strengthening the border control. The directive initiated by Spain was referred to as a measure that should become effective immediately.[9] Shortly afterwards, on 29 April 2004, the directive 2004/82/EC (API directive) was adopted. The original text of the directive was amended in the adopted version of the directive, allowing for the possibility to use API data for purposes other than in the fight against illegal immigration. Consideration 2 of the directive establishes a direct link between fighting terrorism by including a reference to the declaration by the European Council of 25 March 2004. In the Netherlands, as indicated above, airlines are obligated to provide data to the KMar.

### Use by KMar

The KMar may store the data for no more than 24 hours. That retention period may be extended to a maximum of 4 days, in the case of passengers from a category of aliens with an increased risk of illegal immigration. After these 4 days, the API data is anonymized.[10] The anonymized data is used for analyses.

If a border control leads to further investigation, for example into illegal immigration, the data is transferred from the regime of the Illegal Aliens Act to the regime of the Police Data Act. One effect is that API data relating to a specific investigation may then be stored for 5 years.[11]

## 2.2 The use of passenger data for the purpose of national security in the Netherlands

Since the 9/11 attacks in 2001 the external border controls in the Schengen area were referenced as a tool to combat terrorism.[12] The idea is that by strengthening the checks on the external borders, potential terrorists could be identified and stopped at an early stage. The AIVD and the MIVD are also involved in counterterrorism – to protect national security. To that end they process data, including passenger data from airlines. The AIVD and the MIVD process the data under the legal regime of the ISS Act 2017. That means that the safeguards from the API directive and implementing Act, such as legal retention periods, do not apply.

### Use of API data

The parliamentary debate in 2006 on the API legislation referred several times to using passenger data for the purpose of national security whereas the processing of API data by the AIVD and MIVD was hardly debated at all in the House of Representatives. Only on 16 May 2007 in the House of Representatives did the then Minister of Justice point in general terms to 'the access by the AIVD based on the ISS Act'.[13] The use of API data by the AIVD is also referred to in a letter dated 9 March 2012 by

8 Initiative by the Kingdom of Spain with a view to adopting a Council Directive on the obligation of carriers to communicate passenger data (2003/C82/08) of 5 April 2003.
9 Council of the European Union, Draft declaration on combating terrorism, 25 March 2004, 7764/04, p. 8.
10 Government Gazette, 2016, no. 16221, p. 33.
11 Police Data Act, Section 14.
12 *Parliamentary Documents II* 2001/02, 27925, no. 10 and Framework document Border control, appendix to *Parliamentary documents II* 2008/09, 30315, no. 8
13 Proceedings II 2006/07, no. 69, p. 3745. See in similar terms *Parliamentary documents II* 2010/11, no. 3536.

the Minister for Immigration, Integration and Asylum.[14] This letter informs both Houses on the use of passenger data.[15]

The letter of 9 March 2012 outlines that if the relevant government services, including the AIVD, had access to passenger travel data and travel documents before any actual border crossing, they would be able to work in a more effective, more efficient and better coordinated way.[16] The evaluation report drafted by the ministry of Security and Justice in 2013 refers to the use of API data by the intelligence and security services.[17] That report explains that the use of the data by the AIVD and the MIVD is permitted by law based on the investigatory power to use informants (Section 17 of the ISS Act 2002, currently Section 39 in the ISS Act 2017). The report also says that the AIVD considers the use of API data to perform their tasks as having added value and a positive impact on their effectiveness.[18]

## 2.3 Concluding observations

API data is information about the passengers and crew of airlines. The data is stored to improve border controls and combat illegal immigration. That includes the fight against terrorism. API data includes information listed on passports and travel information. In the Netherlands, airlines are obligated to provide this data to the KMar in support of their work, namely to exercise border control. The obligation applies to flights made from countries outside the EU or the Schengen Area to a Dutch airport.

In the parliamentary debate on API data the AIVD and MIVD's use of that data was hardly discussed. The response to parliamentary questions on this topic is generally to refer to the scope provided by the directive to use the data for other purposes, including national security. The AIVD and the MIVD process the data under the provisions of the Intelligence and Security Services Act 2017. Safeguards from the API directive and implementing Act, such as legal retention periods, do not apply to the collection and further processing of the data by the AIVD and the MIVD. It would have been appropriate if the legal grounds and resulting conditions in the Intelligence and Security Services Act had been given more weight in the parliamentary debate on collecting and further processing passenger data by the intelligence and security services.

The severe infringement of fundamental rights involved when bulk data sets are collected and further processed, as in the case of API data, demand foreseeable legislation and sufficient safeguards to protect those involved. The investigatory power to use informants arising from the ISS Act 2017 in itself offers insufficient safeguards for this. Collecting and processing bulk data sets, regardless of how they are collected, must always be adequately enshrined in law. Citizens must be able to foresee that bulk data sets can be collected and further processed by the services, even with a general investigatory power such as the power to use informants. Foreseeability also stretches to the safeguards that are applied. Bulk data sets demand an appropriate set of safeguards as a counterweight to the specific infringements of people's fundamental rights that are inherent to bulk data.

The ISS Act 2017 does not lay down any specific rule for processing bulk data sets based on a general investigatory power, in contrast to the collection and further processing of bulk data sets from investigation-related interception. This topic deserves consideration, at the least, in the context of the evaluation of the legislation.

14 Parliamentary Documents II 2011/12, 32 317, no. 111. The letter was sent on behalf of the Minister for Immigration, Integration and Asylum, the Minister of Internal Affairs and Kingdom Relations, the Minister and State Secretary for Security and Justice, the Minister of Defence, the State Secretary of Finance and the Minister and State Secretary of Infrastructure and the Environment.
15 *Parliamentary Documents II* 2011/12, 32 317, no. 111.
16 *Parliamentary Documents II* 2011/12, 32 317, no. 111, p. 2.
17 Appendix to *Parliamentary Documents II* 2013/14, 32 317, no. 247.
18 Appendix to *Parliamentary Documents II* 2013/14, 32317, no. 247, p. 25.

# 3. Findings regarding the collection of API data

The collection of API data by the AIVD and the MIVD is reviewed in this section against the data processing requirements in the ISS Act 2017 and the AIVD and MIVD's policy for bulk data sets. It concerns the following requirements:

- The use of an investigatory power is required to collect API data. This is the power to use informants (Section 39 of the ISS Act 2017) or the KMar's duty of disclosure (Section 94 of the ISS Act 2017).
- An assessment of necessity as well as the proportionality and subsidiarity principles are required to use a general investigatory power (Section 26 of the ISS Act 2017). Records must be kept of the use that is made of the investigatory power to use informants (Section 31 of the ISS Act 2017).
- The bulk data set policy is a further specification of the general requirements to use investigatory powers in Section 26 of the ISS Act 2017 with the requirement of a written assessment of necessity, proportionality and subsidiarity. That written assessment contains the following elements: (1) specifying the purpose, (2) describing the necessity and (3) weighing the interests. It should be noted that it is not permitted to store more data than necessary for the purpose specified. Data minimization is used as a practical application of the necessity principle.
- The bulk data set policy adds to the legal requirements that authorization is required from the head of service or the relevant minister to collect the data set, depending on the nature of the data.
- The AIVD and the MIVD have the duty to cooperate. That cooperation can take the form of exchanging passenger data from airlines between the AIVD and the MIVD (Section 86(2) of the ISS Act 2017).[19]

This section examines to what extent the API data are collected lawfully. Section 3.1 assesses the lawfulness of the collection of API data by the AIVD. Section 3.2 assesses the lawfulness of providing that data to the MIVD. The findings of Section 3 are summarized in the interim conclusion in Section 3.3.

## 3.1 Findings regarding the collection of data by the AIVD

During the investigation period from 1 January 2019 to 1 September 2019 and in the preceding period, the KMar provided data to the AIVD routinely by automated means. The AIVD does not have direct automated access to the data at the KMar on a 'hit/no-hit' basis. Instead, the data is stored at the AIVD.

In other words, there is no 'direct automated access' as described in Sections 39 and 94 of the ISS Act 2017 and in the 'Decree on measures for direct automated access by the intelligence and security services'. Or to put it in more formal legal terms, this is 'the provision of an automated data file' by the KMar to the AIVD based on the power to use informants.[20] It is important to establish this because direct automated access works on the basis of a hit/no-hit format, meaning that the AIVD would only receive data on specific people the service is investigating. In the current situation, however, the result is that the AIVD collects and stores the data in bulk, the vast majority of which concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be (collecting a bulk data set). In the investigation period the AIVD database contained the data of millions of people.

19 See Section 2 of the assessment framework (Appendix I).
20 See also Section 2.3 of the Assessment Framework (Appendix I).

The AIVD made a deliberate choice at the time for this method of access because of the security advantages, such as having control over the data in a secure environment and preventing the risk that unauthorized people could learn which individuals the AIVD is interested in. This procedure has the added advantage that the services are able to retain the data for longer, in light of the retention period to which the KMar is bound.

### Power to use informants

The API data are provided by the KMar to the AIVD based on the investigatory power to use informants.[21] The investigatory power to use informants allows for the collection of API data routinely and by automated means (current Section 39 of the ISS Act 2017).[22] How the data is collected by the AIVD is therefore in line with the legal framework of Section 39 of the ISS Act 2017.[23] The exercise of the investigatory power to use informants to collect API data is, as such, lawful. The legal text of the investigatory power to use informants and the legislative history do not however provide further details on the term and way of providing a 'automated data file'.

### Policy for bulk data sets

The general requirements of necessity, proportionality and subsidiarity apply to the use of any investigatory power to collect data by the AIVD and the MIVD, therefore also for general investigatory powers such as the power to use informants.[24]

The policy for bulk data further details the general requirements for the use of investigatory powers, because a written substantiation for collecting data is required which includes (1) specifying the purpose, (2) describing the necessity and (3) weighing the interests. It should be noted that it is not permitted to store more data than necessary for the purpose (data minimization).

The CTIVD established that prior to and during the investigation period from 1 January 2019 to 1 September 2019, the AIVD failed to classify API data as bulk data set, although it should have done so, based on CTIVD report no. 55 (2018) and the policy published by the services themselves. Consequently, the safeguards from this policy were not applied to the collection of API data. Thus the assessment of the general principles of necessity, proportionality and subsidiarity (Section 26 of the ISS Act 2017) did not take place. This is *unlawful*.

The above finding raises the question whether other bulk data sets are being collected based on the investigatory power to use informants and whether these are classified as bulk data sets. The CTIVD instructs the AIVD and the MIVD to determine whether there are other bulk data files present and if so, to apply the policy for bulk data sets on those files (*recommendation 1)*.

Furthermore, the CTIVD recommends that the AIVD conducts a written assessment on the necessity, proportionality and subsidiarity to collect API data in accordance with the policy for bulk data sets (*recommendation 2*). This assessment must comply with the conditions of the bulk data set policy and must be repeated periodically (annually) given the ongoing collection of passenger data.

21 See also the Appendix to *Parliamentary Documents II* 2013/14, 32 317, no. 247 (evaluation report on the use of API data).
22 See Section 2 of the assessment framework (Appendix I).
23 Section 94 does not offer the possibility to provide data using an automated data file.
24 Sections 18(1) and 26(1) and (2) of the ISS Act 2017. During the current investigation, the requirement 'as targeted as possible' only applies to the use of investigatory powers (Section 5 Policy Rules of the ISS Act 2017). The Bill amending the ISS Act 2017 proposes to have the requirement 'as targeted as possible' apply to all investigatory powers.

## 3.2 Findings regarding the provision of data to the MIVD

The MIVD does not collect API data through the KMar. The MIVD has access to passenger data of airlines stored by the AIVD. MIVD staff generally consult this data using an application at the AIVD. The AIVD and the MIVD have jointly agreed that – following authorization by an AIVD officer – certain MIVD staff members may use the AIVD's IT infrastructure and programs to carry out their tasks.

The AIVD provides the data to the MIVD in the context of the best possible cooperation, as the AIVD and the MIVD have the legal duty to cooperate as much as possible.[25] This cooperation may, according to Section 86(2) of the ISS Act 2017, consist of providing data for the performance of the services' tasks.

The MIVD is authorized to consult API data on the AIVD's systems based on the cooperation provision of Section 86 of the ISS Act 2017. This is *lawful*. However that does not release the MIVD of its obligation to observe the general requirements of data processing.[26] The CTIVD reviews these provisions in Section 4.

## 3.3 Interim conclusion

In this section, the CTIVD establishes that passenger data from airlines is collected routinely and by automated means by the AIVD through the investigatory power to use informants. It concerns large collections of data, the vast majority of which concerns organizations or people who are not the subject of investigation by the services, nor ever will be. For that reason, that constitutes a 'bulk data set'.

Collecting API data from the KMar by the AIVD through the investigatory power to use informants is *lawful*. Furthermore, the MIVD is authorized to consult API data on the AIVD's systems based on the cooperation provision in the ISS Act 2017. However, the AIVD failed to classify API data collected as a bulk data set. Based on CTIVD report no. 55 (2018) and the policy published by the services themselves, it should have done so. Consequently, the safeguards in this policy were not applied to the collection of API data and compliance with the general requirements to use investigatory powers was thus insufficient. This is *unlawful*.

**Recommendations**

The AIVD and the MIVD failed to classify the API data as bulk data sets. That should be rectified as soon as possible. The CTIVD instructs the AIVD and the MIVD to determine whether there are other bulk data files present and if so, to apply the internal policy on those files (*recommendation 1)*.

Furthermore, the AIVD should conduct a written assessment on the necessity, proportionality and subsidiarity to collect API data in accordance with the policy for bulk data sets (*recommendation 2*). This assessment must be repeated periodically (annually) given the ongoing collection of passenger data.

25 Section 86(1) of the ISS Act 2017.
26 *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 156. See also Section 2.3 in the Assessment framework (Appendix I).

# 4. Findings regarding the further processing of API data

The further processing (the use) of API data by the AIVD and the MIVD is reviewed in this section against the data processing requirements in the ISS Act 2017 and the AIVD and MIVD's policy for bulk data sets. The requirements are as follows:

- The data may be processed for the purpose of the AIVD and the MIVD's task performance (Sections 8 and 10 of the ISS Act 2017).
- The data processing must be connected to a specific purpose and be necessary to the services' task performance (Section 18 of the ISS Act 2017).
- The policy for bulk data sets specifies the obligation of careful data processing with the safeguard that requires authorization for staff who need access to the data (Sections 18 and 24 of the ISS Act 2017).
- The data processing itself must be recorded in such a way to enable appropriate internal control and effective external review (Sections 18 and 24 of the ISS Act 2017).
- Data that is not significant must be removed and destroyed unless legal rules regarding storage preclude this (Section 20 of the ISS Act 2017). The policy for bulk data sets stipulates that the services must check periodically whether a previously acquired data set is still necessary to achieve the purpose for which it was obtained.
- The duty of care means that the services have the policy, process descriptions and work instructions that are an interpretation of the legal requirements in practice. The entire processing procedure must be set up in such a way that internal control and effective external review is possible (Section 24 of the ISS Act 2017).[27]

This section lists the findings of the lawfulness assessment conducted of the further processing of API data. The section has the following structure. Section 4.1 contains the investigation findings regarding the purpose and necessity of processing the data. Section 4.2 looks at compliance with the provisions for authorizations from the bulk data set policy. Section 4.3 lists the investigation findings on how the data-processing activities are recorded. Section 4.4 looks at the periodic check on the significance of the data. Section 4.5 contains the investigation findings regarding compliance with the AIVD and MIVD's duty of care when processing data. Section 4 ends with an interim conclusion about the lawfulness of the further processing of API data.

## 4.1 Findings regarding purpose limitation and necessity

Data should only be processed by the AIVD and the MIVD for a certain purpose and only in as far as necessary for the services to properly perform their tasks.[28] Processing data is the services' core activity.[29]

The investigation showed in assessing purpose limitation and the necessity requirement that API data are mostly processed for investigations into organizations and people who are a threat to national security. In general, those investigations focus on terrorism and identifying espionage and unwanted foreign interference. These investigations ensue from the Integrated Intelligence and Security

27 See Section 3 of the assessment framework (Appendix I).
28 Section 18 of the ISS Act 2017.
29 *Parliamentary Documents II* 2016/17, 34 588, no. 17.

Services Order (hereinafter: Integrated Order).[30] API data are also processed in the context of security screenings. Processing API data is part of the AIVD and the MIVD's tasks described in Sections 8 and 10 of the ISS Act 2017.

### Investigations into organizations and people posing a threat

The CTIVD established that for the majority API data are consulted in investigations into targets, or people who are the focus of the services. That can include consulting API data following a notification that someone may be a jihadist. In that case API data are one of the sources used to evaluate the notification. API data can help to map past flight movements, for example. Based on information such as API data, the service is then able to estimate whether further investigation is necessary. API data are also processed to find more information on known targets. In that case, API data may prompt a new direction of the investigation. Lastly API data may also be used to identify and recognize targets in the services' focus areas.

The CTIVD established that in one case a large amount of API data were copied and used for further data analysis. That analysis failed to use 'profiling' or any predictive data-analysis techniques.

The purpose and necessity of that data processing emerged in the interviews held by the CTIVD and were sufficiently explained. As regards the requirement of purpose limitation and the necessity criterion, the processing activities were found to be *lawful*.

### Conducting security screenings

Security screenings are conducted when someone will fill a position involving confidentiality. The Security Screenings Department of the AIVD and the MIVD follow the same procedure to process API data.

AIVD and MIVD staff from the joint Security Screenings Department process API data under certain circumstances as part of their tasks. API data may be consulted when investigating the individual for who the security screening was requested. That could mean that information about individuals other than the person in question will be consulted if necessary, for example family members. The results of the enquiry may be significant to confirm or refute a certain assumption of the security screening. The CTIVD established on the basis of the interviews it held that the data processed during the investigation period was necessary and *lawful*.[31]

The CTIVD established by its investigation into application logging that staff from the Security Screenings Department also processed data that was not necessary for the performance of their tasks. The CTIVD enquired about this with the AIVD given the fact that this type of data processing does not fit in with the department's activities. The AIVD was unable to give a conclusive explanation for the data processing. After conducting its own investigation, the AIVD concluded that part of that processing activities could be explained by the fact that the relevant staff had changed jobs and the processing activities were carried out in the context of their former work. The CTIVD finds this data processing to be *unlawful*. It was not necessary to process that data nor does it fit in with the job and tasks of the staff members in question. The AIVD has now taken measures to ensure this kind of data

30 The Integrated Order is an instruction by the Council for the Security and Intelligence Services, a sub-council of the cabinet. The investigations conducted by AIVD and the MIVD are guided by that order. The Integrated Order is adopted once every four years. The responsible ministers from the ministries who most frequently use AIVD and MIVD data define the investigative priorities. The Integrated Order is drawn up in consultation between the ministries and the AIVD and the MIVD. The investigative themes and priorities are included in the appendix to the Integrated Order, which is a state secret.

31 By implementing the safeguards from the bulk data set policy when processing bulk data, the current authorization regime needs to be amended (see Section 4.2). As a result, access to the API data may become more restricted for some departments given the nature of the information in a bulk data set.

processing is no longer possible. The measures were mainly set down in work instructions, but are not enforced in a technical sense.

### Automated data analysis

In all cases where an application is used to process API data, automated data analysis takes place (Section 60 of the ISS Act 2017). In an application a search is carried out for a certain characteristic (for example, a name). That query is compared and combined with the data stored by the AIVD by automated means. For that reason, this constitutes automated data analysis. Conducting automated data analyses is a core activity of both the AIVD and the MIVD. In the processing of API data during the investigation period from 1 January 2019 to 1 September 2019, no measures were promoted or taken solely on the basis of the results of an automated data analysis without human intervention.

## 4.2 Findings regarding authorizations

API data can be searched by using an application developed and managed by the AIVD. Only authorized staff may use the application. The CTIVD established that the authorization regime has not been set up as described in the policy for bulk data sets.

### Obtaining access

The AIVD has specified per job role which applications are necessary for staff members to carry out their tasks. One general request is sufficient to gain access to all necessary applications. A superior authorizes that request. Thus there is no underlying written substantiation to obtain an authorization for API data. This is not in accordance with the policy for bulk data sets.

In the period investigated, MIVD staff could, on request, be authorized to consult API data using the application. There was no centralized or process-based set-up for the authorization during the investigation period. The MIVD cannot trace when and how its staff were first granted access to the API data.

### Wide authorizations

The application to process API data has one authorization profile, which means that there is no technical distinction in the application between the various job roles. All authorized staff members from both the AIVD and MIVD have the same rights in the application and they can consult all the available data and all the features of the application. An authorization regime that is as wide as this is not appropriate where it concerns bulk data sets and is not in line with the bulk data set policy.

This wide authorization regime has led in practice to a situation where staff from the Security Screenings Department were able to process data that was not appropriate to their current tasks, but instead was linked to their former job (see Section 4.1).

The CTIVD finds that the authorization process gives too little consideration to authorizations to ensure compliance with the duty of careful and proper data processing and as an important safeguard when processing data from a bulk data set. The services' own bulk data set policy stipulates that staff members must submit a separate request to gain access to the data in a bulk data set and that they must substantiate why they need that data to perform their tasks.

A strict authorization procedure where staff only have access to the data that is necessary to perform their tasks is an important safeguard to limit the infringements of privacy. The AIVD and the MIVD are currently in talks to improve the authorization process and the access by MIVD staff to AIVD applications.

The CTIVD recommends that both services examine how the authorizations to use the application to process API data can be set more stringently, taking into account the different job roles and related tasks within the AIVD and the MIVD (*recommendation 3)*.

## 4.3 Recording

Recording is part of careful data processing (Section 18 of the ISS Act 2017) and of the duty of care regarding the processing of data (Section 24 of the ISS Act 2017). The services themselves must be able to see what happens to the data, where it is stored and when it should be removed or destroyed (internal control). In addition, the CTIVD must be able to exercise effective external review of the data-processing activities by the services. It must be transparent when the data was processed and for what purposes. The recording must be accurate enough to be able to establish compliance with the provisions regarding data processing in the ISS Act 2017. Logging is one way to enable that recording.

### Recording by staff

The CTIVD concludes that the AIVD and the MIVD do not have any general policy in place for recording the use of the application. The CTIVD inferred from its interviews with service staff that there is no uniform way of recording.

The AIVD stores API data in a way that the data can be identified as such. When staff then access the data in the application it is clear that it concerns API data. It is important that staff continue to record the source of the data when processing it further. That duty to record does not mean, in the CTIVD's interpretation, that a full written report is required for every query of the application concerning an individual. The extent and manner of recording differ for each type of investigation and depend on the data processed. In practice, staff only record a result in writing. That means that consulted API data that did not yield any result is not recorded by the staff member. The Security Screenings Department does record the search result, even in the case of no result. When recording, a reference is included to the source of the data.

### Recording of further data-analyses by staff

The CTIVD established that during the investigation period relatively simple data-analyses were conducted at the AIVD and the MIVD. Recording of data-analyses conducted on data copied from the application is generally inadequate. The CTIVD considers it important that that type of data processing is recorded. Simply recording the result of the analysis is not sufficient.

The CTIVD established that in one case a large amount of API data was copied and stored outside the regular application environment for further data analysis. The purpose and necessity of that data analysis emerged in the interviews held by the CTIVD and were sufficiently explained (see also Section 4.1). However the CTIVD concludes that this analysis was not sufficiently recorded. It is important, as regards these kinds of data-processing activities, to be clear about the purpose and the necessity for which the data is to be copied, that it is copied, where it is stored and that this data is then removed in time. Those records were not kept. The CTIVD finds this to be *unlawful*.

### Recording by logging

Records can be kept by staff but can also be kept by logging the actions in the application. That means that logging should be complete and be set up to enable internal control and external review. Logging of the application during the investigation period was mainly set up for security purposes and not to ensure the lawful processing of data. Nor is logging done in a uniform way. For example, the MIVD does not log which of its departments specifically use passenger data, in contrast to the AIVD. However, it is possible to deduce which staff use the application.

The services should effect the recording of any further data processing in such a way as to enable sufficient internal control and effective external review *(recommendation 4)*.

## 4.4 Findings regarding a periodic check on significance

The ISS Act 2017 does not prescribe a retention period for data collected by general investigatory powers such as the power to use informants. That data may be stored until it has lost its significance for the task of the service.. As part of careful data processing, data that is no longer significant for the services' tasks must be removed and destroyed unless legal rules regarding storage preclude this, in particular the Public Records Act 1995 (Section 20 of the ISS Act 2017). The bulk data set policy also includes the obligation to assess periodically whether previously obtained data sets are still necessary to achieve the purpose for which they were obtained.

The CTIVD concludes that since collection started, no assessment has been made of whether the data is still significant and whether previously obtained data sets are still necessary to achieve the purpose for which they were obtained. No data was removed or destroyed except for technical reasons, such as to delete duplicates.

The CTIVD recommends that the AIVD and the MIVD periodically check whether the stored data is still significant and whether previously obtained data sets (passenger data) are still necessary for the purpose for which they were obtained (*recommendation 5*).

## 4.5 Findings regarding compliance of duty of care

To assess the duty of care, the following elements were investigated:
1. Internal control of the data processing (Section 24 of the ISS Act 2017);
2. Policy, process descriptions and work instructions relating to data processing (Sections 18(2) and 24 of the ISS Act 2017).

### 4.5.1 Internal control

The nature of the data set, namely a bulk data set, demands strict checks on the use of the data by the AIVD and the MIVD, given the serious infringement of privacy that the data processing involves. As discussed in Section 4.3, staff members do not record their data-processing activities fully or in a uniform way. Logging of the application during the investigation period was mainly set up for security purposes and not to ensure the lawful processing of data.

Consequently a superior, for example, does not have a clear enough picture on which to exercise effective and efficient control and assess to what extent the data contributes, or is still relevant, to the services' tasks. Checks such as these did not take place during the investigation period. The AIVD and the MIVD must take more steps to facilitate internal control of the careful processing of API data.

As regards the internal control in the context of 'ISS Act compliance', the AIVD conducted a quick scan in May 2019 of the collection and further processing of data including passenger data. That document states that in collecting and processing large amounts of API data privacy infringement occurs. The legal department was asked to indicate to what extent that procedure is within legal boundaries. However, the document does not classify the data as a bulk data set which is subject to the internal policy. Nor does the AIVD find that there is any serious infringement of citizens' privacy. The quick scan did not result in any specific measures in the investigated period.

The mechanisms for internal control of further data processing are inadequate. The follow-up of internal warnings from the quick scan as regards an incident of unlawful data processing was inadequate as well. The services should ensure internal control that is sufficient to comply with the requirements set by the duty of care in Section 24 of the ISS Act 2017 (*recommendation 6)*.

### 4.5.2 Policy, process descriptions and work instructions

Policy, process descriptions and work instructions can contribute to careful data processing because they can result in a uniform manner of processing data, for example. Some staff are given instructions about the further processing of API data as part of a training course. That course is mainly practical in nature, however, and the implementation of the legal requirements for data processing is not discussed.

The bulk data set policy is an interpretation of careful and proper data processing as referred to in Sections 18 ff. in the ISS Act 2017. A combined non-compliance with the policy and a lack of uniform process descriptions and work instructions aggravate the risk of unlawful conduct.

In fact, in a number of incidents in which API data were collected and further processed, that risk did indeed manifest itself as unlawful conduct.

Policy, process descriptions and work instructions should at least set out what the purpose and necessity is for processing API data for the various focus areas. Another suggestion is to set the contours within which data processing is permitted. Lastly it must be laid down in writing which additional safeguards should be in place for which forms of further data analysis, to limit as much as possible the infringement of the fundamental rights of the people involved. This includes considering in which circumstances and under which conditions copying data to another IT environment is permitted and how long the data may be stored for analysis.

The MIVD mainly processes API data through the AIVD systems. Use by the MIVD of the AIVD's systems, does not release the MIVD of its responsibility to comply with careful data processing.[32] The AIVD and the MIVD must therefore endeavour to discuss how they can ensure that data is processed carefully. In consultation with the MIVD, the AIVD must put further arrangements in place for the policy and the legal requirements for data processing by specifying process descriptions, work instructions and their implementation in the technical systems, taking into account the nature and amount of data and the infringement involved in collecting and further processing (*recommendation 7*).

## 4.6 Interim conclusion

AIVD and MIVD staff use API data for a variety of purposes, depending on their tasks. That data may for example contribute to interpret the reports which the AIVD or the MIVD receive. API data may help to assess the threat a particular individual poses. Passenger data, just like any bulk data set, can also be used to identify and recognize targets in the services' focus areas. Lastly, API data is used in the context of security screenings to assess whether a security clearance can be given when an individual is appointed to a position involving confidentiality. Passenger data can be consulted using an application. When consulting API data using a search query, the data is compared by automated means. That means it is automated data analysis (Section 60). In the processing of API data during the investigation period from 1 January 2019 to 1 September 2019, no measures were promoted or taken solely on the basis of the results of an automated data analysis without human intervention.

32 *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 156.

The majority of the data-processing activities investigated by the CTIVD were found by the CTIVD to be lawful. The processing activities can be linked to the services' tasks and arise from the Integrated Order. This does not apply to the data-processing activities conducted by the Security Screenings Department, which are not part of that department's job responsibilities. Moreover, the CTIVD established unlawful conduct during the data analysis conducted on a large-scale set of API data. That analysis failed to use 'profiling' or any predictive data-analysis techniques.

The CTIVD further established the following:

- The authorization regime is too wide and not in accordance with the policy for bulk data sets;
- The recording of data-processing activities does not comply sufficiently with the requirements set by the duty of care and careful data processing;
- Since data collection started, no periodical check has taken place of whether the stored data is still significant and whether previously obtained data sets (passenger data) are still necessary for the purpose for which they were obtained;
- Internal control is not properly set up and specific work instructions are lacking for the various data-processing activities of API data.

Based on the above findings, the CTIVD concludes that the specific measures referred to in the policy for processing data from bulk data sets are not or not sufficiently applied. This is *unlawful*.

### Recommendations

The CTIVD firstly recommends that both services examine how the authorizations to use the application to process API data can be set more stringently, taking into account the different job roles and related tasks within the AIVD and the MIVD (Section 4.2). Secondly, the services should effect the recording of any further data processing in such a way as to enable sufficient internal control and effective external review (Sections 4.3 and 4.5.1). Thirdly, the AIVD and the MIVD must check periodically whether the stored data is still significant and if the collection of API data is still necessary for them to perform their tasks (Section 4.4). Fourthly, the CTIVD recommends that the services arrange for internal control that is sufficient to comply with the requirements set by the duty of care in Section 24 of the ISS Act 2017 (Section 4.5.1). The fifth recommendation is that in consultation with the MIVD, the AIVD must further implement the policy and the legal requirements for data processing by specifying process descriptions, work instructions and their implementation in the technical systems, taking into account the nature and amount of data and the infringement involved in collecting and further processing that data (Section 4.5.2).

# 5. Conclusions and recommendations

Central to this report is the question whether the AIVD and the MIVD collected and further processed API data from airlines lawfully in the period from 1 January 2019 to 1 September 2019. API data is a specific set of passenger data from airlines which the AIVD collects routinely and by automated means.

The vast majority of the API data concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be. For that reason, this is actually the collection and further processing of a bulk data set. On 1 May 2018, both services published the policy document 'AIVD and MIVD policy on the acquisition and processing of bulk data sets' (the policy on bulk data sets) on their respective websites. This policy was drafted by the services following the recommendation in the CTIVD's review report no. 55 (2018) on the acquisition, by means of the investigatory power to use informants, of bulk data sets offered on the internet by third parties. The collection and further processing of bulk data sets is a severe infringement of the fundamental rights of those involved. The services' policy for bulk data sets constitutes a more specific interpretation of the general requirements for data processing under the ISS Act (Sections 18-24 of the ISS Act 2017). Furthermore, the policy sets the additional safeguards that require the head of service or the relevant minister to authorize the collection (as a further implementation of Section 26 of the ISS Act 2017) and that require data to be minimized. The policy must be applied when it is a bulk data set that is being collected and processed further.

## 5.1 Conclusions regarding the collection of passenger data

The KMar is given the passenger data from the airlines for its own tasks, i.e. border control. The AIVD collects the API data routinely and by automated means based on the investigatory power to use informants. This entails the provision of an automated data file and not 'direct automated access' using a 'hit/no-hit' system. It is important to establish this because direct automated access works on the basis of a hit/no-hit format, meaning that the AIVD would only receive data on specific people the service is investigating. This in contrast to the provision of automated data files, which has as result that the AIVD collects and stores data, the vast majority of which concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be.

The CTIVD established that applying the investigatory power to use informants (Section 39 of the ISS Act 2017) as legal grounds for this method of collecting API data is as such lawful. The AIVD makes the API data available to the MIVD by offering MIVD staff the possibility to use the AIVD application to process passenger data. The services are authorized to do this. To this point, the API data collected by the AIVD and the MIVD is *lawful* (Section 3.3).

However, API data is in fact a bulk data set, i.e. a large collection of data, the vast majority of which concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be. In the investigation period the AIVD database contained the data of millions of people.

The AIVD and the MIVD failed to classify the API data as bulk data sets as required by their own policy. In addition the services did not conduct any written assessment of necessity, proportionality and subsidiarity. This is *unlawful*.

The policy is a more specific interpretation of the general legal requirements and offers additional safeguards on some points. The additional safeguards provided by the policy – the request for authorization from the head of service or minister involved to collect API data and the check of data minimization when collecting data – were not in place.

## 5.2 Conclusions regarding the further processing of passenger data

The investigation by the CTIVD showed that passenger data from airlines, particularly the API data, was frequently processed by the AIVD and the MIVD. The data is processed in the context of investigations into espionage, unwanted foreign interference and terrorism. The data is also used to conduct security screenings. API data is used to gain insight into targets' travel behaviour. To a lesser extent API data is used to discover new targets. The CTIVD established that API data is processed for objectives that fall within the services performance of tasks (purpose limitation) and that it is necessary to process this data to achieve those objectives. This is *lawful* (Sections 4.1 and 4.2).

The AIVD developed an application to further process API data. MIVD staff also use this application after being granted authorization. The application compares the data by automated means. That makes it automated data analysis (Section 60 of the ISS Act 2017). The application does not have any technical restrictions built in to process passenger data, so that if a member of staff is authorized to use the application, they can consult all the API data stored.

The processing of API data must comply with the general requirements for data processing (Sections 18-24 of the ISS Act 2017). In addition, the bulk data set policy interprets these requirements in a specific way, such as by a strict authorization regime and periodic assessment of whether the data is still necessary for the services to perform their tasks. The CTIVD notes the following:

- The authorization regime is not in accordance with the policy for bulk data sets;
- The recording of the data-processing activities does not comply sufficiently with the requirements set by the duty of care and careful data processing;
- Since data collection started, no periodical check has taken place of whether the stored data is still significant and whether previously obtained data sets are still necessary for the purpose for which they were obtained;
- Internal control is not properly set up and specific work instructions are lacking for the various data-processing activities of API data.

Based on the above findings, the CTIVD concludes that the specific safeguards referred to in the policy for processing data from bulk data sets are not or not sufficiently applied. This is *unlawful*.

Moreover, the CTIVD established unlawful conduct during the data analysis conducted on a large-scale set of API data. This did not entail 'profiling' or any predictive data-analysis techniques. The CTIVD also established unlawful conduct relating to data processing by the Security Screenings Department, given the fact that these specific data-processing activities are not part of the tasks of that department's staff.

## 5.3 Recommendations

### Recommendations for collecting API data

1. The AIVD and the MIVD failed to classify the API data as bulk data sets. That should be rectified as soon as possible. The CTIVD recommends that the AIVD and the MIVD determine whether there are other bulk data files present and if so, that the internal policy is applied to those files (recommendation 3.1).
2. Furthermore, the AIVD and MIVD should conduct a written assessment on the necessity, proportionality and subsidiarity in order to collect API data in accordance with the policy for bulk data sets. In addition, that assessment must be repeated periodically (annually) given the ongoing collection of passenger data (Section 3.1).

**Recommendations for processing API data**

3. The CTIVD recommends that both services examine how the authorizations to use the application to further process API data can be set more stringently, taking into account the different job roles and related tasks within the AIVD and the MIVD (Section 4.2).
4. The services should effect the recording of any further data processing in such a way as to enable sufficient internal control and effective external review (Sections 4.3 and 4.5.2).
5. The CTIVD recommends that the AIVD and the MIVD periodically check whether the stored data is still significant and whether previously obtained data sets (passenger data) are still necessary for the purpose for which they were obtained (Section 4.4).
6. The services should ensure internal control that is sufficient to comply with the requirements set by the duty of care in Section 24 of the ISS Act 2017 (Section 4.5.1).
7. In consultation with the MIVD, the AIVD must further implement the policy and the legal requirements for data processing by specifying process descriptions, work instructions and their implementation in the technical systems, taking into account the nature and amount of data and the infringement involved in collecting and further processing that data (Section 4.5.2).

## 5.4 Reflection on the investigatory power to use informants and bulk data sets

The severe infringement of the fundamental rights involved when bulk data sets are collected and further processed, as in the case of API data, demands foreseeable legislation and sufficient safeguards to protect those involved. From a legal perspective, the investigatory power to use informants offers scope to collect bulk data sets, such as API data, using this power. However that does raise the question whether this is foreseeable for citizens and to what extent policy offers sufficient safeguards to collect and process that type of data.

Collecting and processing bulk data sets, regardless of how they are collected, must always be adequately enshrined in law. Citizens must be able to foresee that bulk data sets can be collected and further processed by the services, even with a general investigatory power such as the power to use informants. Foreseeability also stretches to the safeguards that are applied. Bulk data sets demand an appropriate set of safeguards as a counterweight to the specific privacy infringements that are inherent to bulk data.

The ISS Act 2017 does not lay down any specific rule for processing bulk data sets based on a general investigatory power, in contrast to the collection and further processing of bulk data sets from investigation-related interception. The investigation shows that legislation does insufficient justice to the protection of the fundamental rights of people who are not the subject of investigation by the services, nor ever will be. This topic deserves consideration, at the least, in the context of the evaluation of the legislation.

Oranjestraat 15, 2514 JB The Hague
P.O.Box 85556, 2508 CG The Hague

**T** 070 315 58 20
**E** info@ctivd.nl | www.ctivd.nl