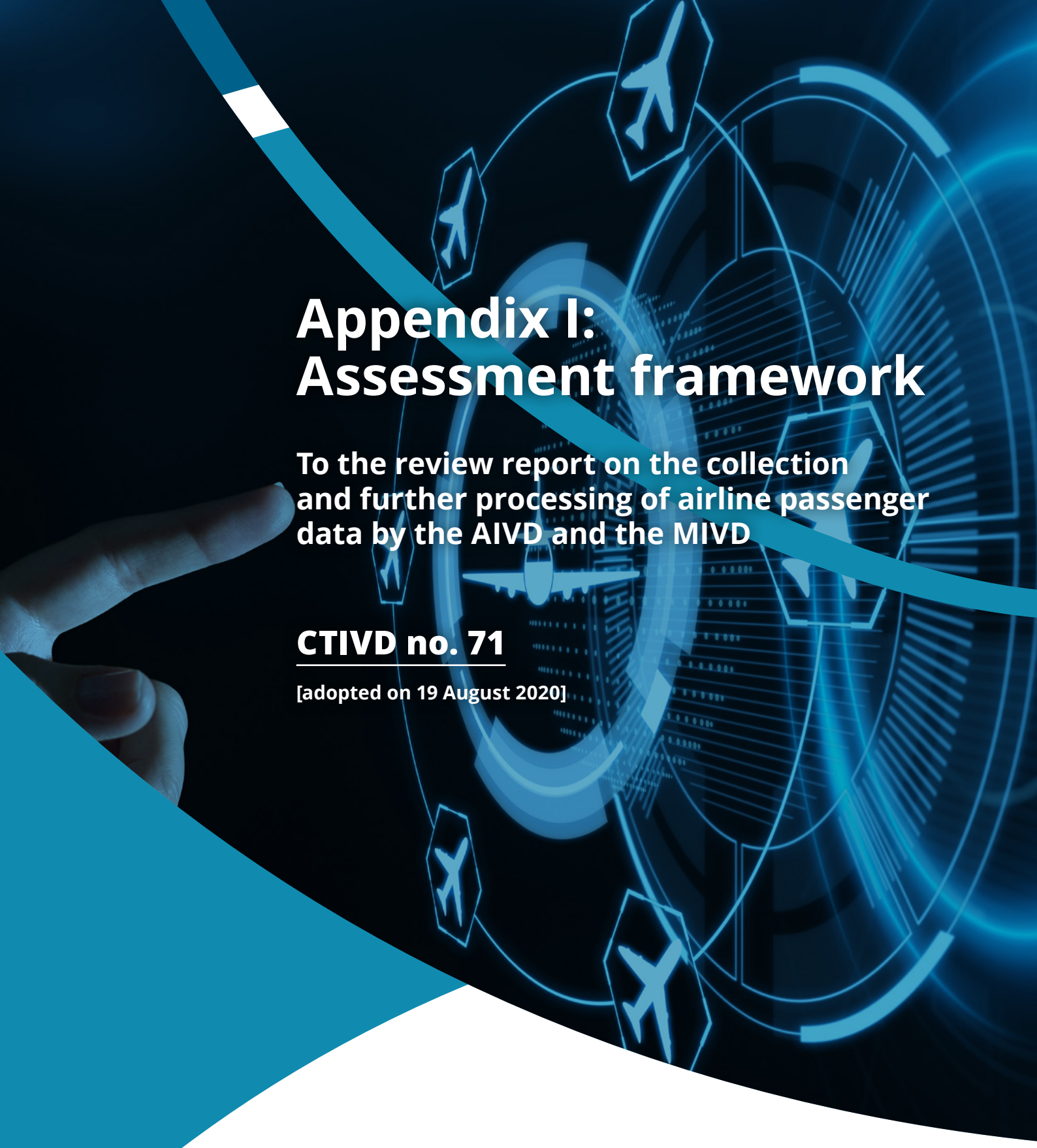

Appendix I: Assessment framework

To the 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]

CTIVD
Review Committee on the Intelligence and Security Services

Review Committee
on the Intelligence
and Security Services

CTIVD no. 71

REVIEW REPORT

To the review report on the collection and further processing of airline passenger data by the AIVD and the MIVD

Inhoudsopgave

CTIVD no. 71

APPENDIX I

To the review report on the collection and further processing of airline passenger data by the AIVD and the MIVD

1. Introduction

The underlying assessment framework focuses on the collection and further processing of airline passenger data which the Royal Netherlands Marechaussee (KMar) submits to the AIVD. More specifically it concerns *Advance Passenger Information* (API data). 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 provides them with an understanding 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.

API data

API data is stored by the airlines and they must provide this data to the KMar under the EU Directive 2004/82/EC (API directive). The KMar processes the data for its own task – 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).

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 transport means;
- the total number of passengers transported by that means;

- border crossing point of arrival;
- first boarding point;
- other itinerary information;
- Passenger Name Record file location.[1]

The KMar may provide API details to the AIVD under Sections 39 or 94 of the ISS Act 2017. The AIVD may – in the context of cooperation – provide API details to the MIVD under Section 86 of the ISS Act 2017. The data-processing provisions from the ISS Act 2017 apply to the passenger data processed by the AIVD.

The above process of collecting and further processing passenger data by the intelligence and security services and the legal provisions from the ISS Act 2017 can be visualized in the figure below:

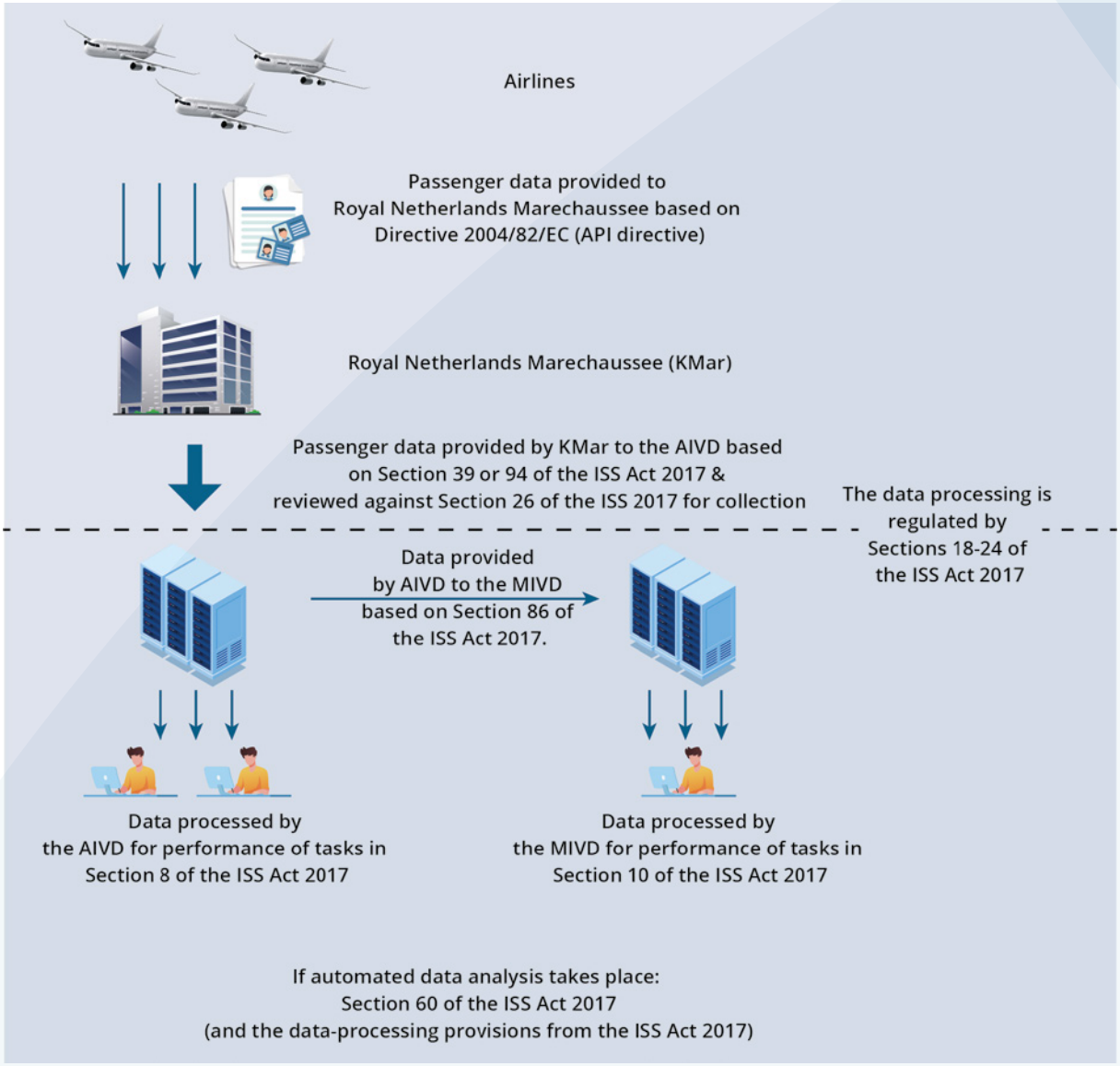

Figure 1: diagram of the data-processing procedure with relevant legal provisions

1 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, information on flights from a Dutch airport is also stored.

Figure 1 shows that in this investigation the processing of passenger data from airlines is divided into two stages. Firstly, the collection of this data by the KMar and secondly, the further processing (i.e. the use) of that data by the AIVD and the MIVD.[2] The assessment framework sets out the applicable legislation in the Intelligence and Security Services Act 2017 (ISS Act 2017) using the above figure. Figure 1 shows which part of the data-processing procedure the provisions relate to.

The applicable legal framework further consists of the Policy Rules of the ISS Act 2017, the services' applicable policy, the commitments undertaken by the Minister of the Interior and Kingdom Relations and the Minister of Defence, the standards ensuing from the European Convention on Human Rights (ECHR) and the case law of the European Court of Human Rights (ECHR) as well as the recommendations made by the CTIVD and adopted by the relevant minister.

It is important in this respect that the CTIVD classifies API data as a *bulk data set*. That means that it concerns a large collection 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. Collecting and further processing that data constitutes a serious infringement of fundamental rights which must be offset by adequate safeguards. The CTIVD also surmises that fact from case law by the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU).[3] Storing personal data such as this in large quantities to combat terrorism, for example, is only permitted under certain circumstances, such as an advance assessment of necessity and proportionality, with detailed rules on aspects such as the duration of storage, the use of data by authorized staff, measures to safeguard the integrity and reliability of the data and procedures for the destruction of data.[4] The CTIVD expresses reservations regarding these standards in that they cannot be applied point-blank to the processing of airline passenger data by the Dutch intelligence and security services, because the standards formulated in case law pertain to other types of data (such as DNA information and communication data) and do not always relate to data processing to protect the national security of states. Moreover, that case law is still being developed. However it does serve as an incentive to implement possible safeguards which the AIVD and the MIVD should take into account when processing data from bulk data sets. The services have specified part of these safeguards in their policy on bulk data sets.[5]

The assessment framework is structured as follows. Section 2 concerns the provisions relating to the collection of passenger data from airlines through the KMar. Section 3 looks at the provisions on processing passenger data for the operational process. Section 4 provides an overview of the legal requirements for the collection and further processing of airline passenger data by the intelligence and security services.

2 Section 1(f) of the ISS Act 2017 gives a definition of the term data processing or the processing of data. That includes in any case the collection and use of the data.

3 See also the Assessment framework to report no. 55 (2018) on bulk data sets offered on the internet by third parties. The Court of Justice of the European Union reviews against the Charter of Fundamental Rights of the European Union. Based on Article 4(2) of the Treaty on the European Union, regulation of the intelligence and security services' investigatory powers falls within the domain of the member states themselves. Nevertheless, the CTIVD does include the CJEU's case law in its assessment framework because the court's case law has a great many similarities when it comes to the collection of bulk data.

4 See in particular ECHR 4 December 2008, no. 30562/04 and 30566/04 ECLI:CE:ECHR:2008:1204JUD003056204 *(S. and Marper vs. The United Kingdom)*. ECHR 19 June 2018, no. 35242/08, ECLI:CE:ECHR:2018:0619JUD003525208 *(Centrum för Rattvisa vs. Sweden)* and European Court of Human Rights 13 September 2018, nos. 58170/13, 62322/14 and 24960/15, ECLI:2018:0913JUD005817013 *(Big Brother Watch et al. vs. The United Kingdom)* and ECHR 30 January 2020, no. 50001/12, ECLI:CE:ECHR:2020:0130:JUD005000112 *(Breyer vs. Germany)* and CJEU 21 December 2016, C-203/15 and C-698, ECLI:EU:C:2016:970 *(Tele2 Sverige AB vs. Post-och telestyrelsen and Secretary of State for the Home Department vs. Tom Watson et al.)*. Case law is still being developed because a number of these cases will be heard in 2020 in the Grand Chamber of the European Court of Human Rights and the CJEU still has to rule on similar questions.

5 See the post 'Working with large data sets' on aivd.nl and the 'AIVD and MIVD policy on the acquisition and processing of bulk data sets' of 1 May 2018.

2. Collection of passenger data

The ISS Act 2017 has two grounds on which the AIVD and the MIVD may collect API data from the KMar, i.e. the investigatory power to use informants (Section 39 of the ISS Act 2017) and the provision of data by the KMar at the request of the AIVD and the MIVD (Section 94 of the ISS Act 2017) in support of their work (Sections 8 and 10 of the ISS Act 2017). This section looks at both grounds as well as the data-processing provisions in the ISS Act 2017 and their specific application to bulk data sets.

2.1 The investigatory power to use informants (Section 39 of the ISS Act 2017)

The AIVD and the MIVD can obtain data from the KMar through the investigatory power to use informants.[6] Section 39 of the ISS Act 2017 prescribes that the services may approach administrative authorities, public sector workers and 'any other deemed able to provide the necessary information'. Briefly put, the service can turn to anyone with a request to provide information.[7]

Data provided by 'any other' on the grounds of Section 39 of the ISS Act 2017 is on a voluntary basis. The KMar can therefore be a body that provides data to the AIVD or the MIVD on a voluntary basis. The power to use informants is not a special investigatory power and consequently it is not subject to particular authorization requirements, such as an authorization by the responsible minister and the Investigatory Powers Commission (TIB). However, the services may interpret this in a specific way and impose 'requirements above the statutory minimum' on themselves. That is discussed in greater detail in Section 2.6.

Direct automated access

Section 39 explicitly states that the services may gain access to data from third parties by direct automated access or by the provision of automated data files. Direct automated access means that an online connection is made in realtime between the service and the individual or organization providing the data. Data is requested or provided without human involvement on the part of the individual or organization.[8] These are routine search requests.[9]

Legislative history underlines that search requests must be made on a hit/no-hit basis, i.e. the data is only provided if the search request yields a hit. These search requests are therefore targeted and based on specific characteristics, such as the name of an individual. That prevents unnecessary access to data of people who are not the object of the services' search.[10] Further rules have been set out by a General Order in Council for direct automated access.[11]

Providing data files

A second way to obtain data is that administrative authorities, public sector workers or any other person provides automated data files. Those files are usually provided to enable the *further processing* of the data. That includes for example automated data analysis in the sense of Section 60 of the ISS Act 2017, such as searching for profiles or patterns, whether or not in combination with other files.

6 Section 39 of the ISS Act 2017.
7 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 56.
8 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 58.
9 *Parliamentary Documents II* 2016/17, 34 588, no. 75, p. 2.
10 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 58 and *Parliamentary Documents II* 2016/17, 34588, C, p. 10.
11 See the 'Decree on measures for direct automated access by the intelligence and security services', *Bulletin of Acts and Decrees* 2018, 115.

Those data-processing activities are preferably conducted within the AIVD and MIVD's own screened-off IT domain for privacy and security reasons.[12] This does not entail a targeted search request.

2.2 Provision of data by the KMar (Section 94 of the ISS Act 2017)

The AIVD and the MIVD can also ask staff from the KMar to provide data. On request these public sector workers will provide the information on behalf of the Commander of the KMar.[13] The provision of information on these grounds is not voluntary, in contrast to the investigatory power to use informants. The KMar, the tax authorities and the police may also provide information on their own initiative.

The regulation in Section 94 of the ISS Act 2017 is apparently intended to give the AIVD and MIVD the authority to request data from the police, the KMar and the tax authorities. That means they have a duty to provide information, it is not a voluntary decision.[14] The text of the Act does not preclude the provision of airline passenger data by the KMar to the AIVD and the MIVD based on this section.

The ISS Act does not set any different authorization requirements for the use of the investigatory power under Sections 94 or 39 of the ISS Act 2017. For this investigatory power also, no particular authorization requirements apply, such as an authorization by the responsible minister and the subsequent lawfulness assessment by the TIB.

On the grounds of Section 94 of the ISS Act 2017 data may also be provided in a 'direct automated way'.[15] The General Order in Council, that further regulates this manner of access under Section 39 of the ISS Act 2017 also applies to Section 94 of the ISS Act 2017.[16]

The difference with Section 39 of the ISS Act 2017 is that Section 94 of the ISS Act 2017 does not refer to the possibility to provide automated data files.

2.3 Provision of data between the services (Section 86 of the ISS Act 2017)

The AIVD and the MIVD must cooperate where they can.[17] That cooperation may consist of providing data for the services to carry out their tasks (Section 86(2) of the ISS Act 2017). The section was included in the ISS Act 2017 following the recommendation of the Committee Dessens which resulted in an amendment of the Act from 'provide assistance' to 'the duty to cooperate'.[18]

That cooperation can consist of the services exchanging information and thereby also exchanging passenger data from airlines.. This section of the Act is phrased as an investigatory power. The general data-processing provisions in the ISS Act 2017 remain in force.[19]

12 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 57.
13 Section 94 of the ISS Act 2017. Section 91 of the ISS Act 2017 states that public sector workers are subordinate to the Commander of the KMar. Based on Section 94 of the ISS Act 2017, the AIVD and the MIVD are authorized to request data from public sector workers at the police and tax authorities.
14 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 168.
15 Section 94(2) of the ISS Act 2017.
16 Decree on measures for direct automated access by the intelligence and security services, *Bulletin of Acts and Decrees* 2018, 115.
17 Section 86(1) of the ISS Act 2017.
18 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 155-156.
19 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 156.

2.4 Tasks and requirements concerning data processing (Sections 8 and 10 of the ISS Act 2017)

Passenger data from airlines that is collected based on the above investigatory powers may be used for all tasks assigned to the AIVD and the MIVD. The AIVD may, in the interest of national security, process the data to conduct investigations relating to organizations or individuals who, briefly put, pose a threat to national security, because of other compelling interests of the state or who pose a threat to the continuation of the democratic constitutional state. Data may also be processed to promote measures to protect the above interests, to conduct investigations into other countries, to draft threat or risk analyses and to provide a report about certain individuals or bodies.[20] Lastly, the AIVD may also process data to conduct security screenings.[21]

The MIVD is authorized, in the interest of national security, to process data to conduct investigations into the potential and the armed forces of other powers, to enable the correct choice of structure and effective use of the armed forces and into the factors that could influence the enforcement and promotion of the international constitutional state insofar as the armed forces are, or expect to be, involved.[22] The MIVD may also process information to conduct investigation where necessary to take measures to prevent the activities that aim to damage the security or preparedness of the armed forces, to promote a correct process of mobilization and concentration of armed forces or to ensure an undisturbed preparation and use of the armed forces as referred to in the first task description. Data may also be processed to promote measures to protect the above interests and to protect the data.[23] Data may also be processed to conduct investigations concerning other countries and concerning subjects with military relevance.[24] The MIVD may also process that information to draft threat analyses for the security of individuals, the surveillance and security of the objects and services with military relevance specified in the ISS Act.[25] The data may also be processed on request in the cases listed in Section 10(2)(g) of the ISS Act 2017. Lastly, the MIVD is permitted to process data to conduct security screenings.[26]

General requirements of data processing (Sections 18-26 ISS Act 2017)

The general data-processing requirements apply each time to the data processed for the services' tasks. That means that data should only be processed for a certain purpose and only in as far as *necessary* for the services to carry out their tasks. The ISS Act 2017 refers to this as purpose limitation and the necessity requirement.[27] The data-processing objectives are set out in Section 19 of the ISS Act 2017. For example, it concerns processing the data of those people s uspected of being a threat to the national security or people who have granted authorization for a security screening. The purpose of the data processing must also be set out in the substantiation for a request to use an investigatory power.[28] The services should be confident that this purpose can be achieved by processing the data and they must be able to substantiate that.[29]

20 See Section 8(2)(c)(d) of the ISS Act 2017 in conjunction with Section 19(1) of the ISS Act 2017.
21 Section 8(2)(b) of the ISS Act 2017 in conjunction with Section 19(1) of the ISS Act 2017. If the data had been collected using a special investigatory power, this would not have been possible.
22 Section 10(2)(a) in conjunction with Section 19(2) of the ISS Act 2017.
23 Section 10(2)(c) in conjunction with Section 19(2) of the ISS Act 2017.
24 Section 10(2)(e) in conjunction with Section 19(2) of the ISS Act 2017.
25 Section 10(2)(f) in conjunction with Section 19(2) of the ISS Act 2017.
26 Section 10(2)(b) in conjunction with Section 19(2) of the ISS Act 2017.
27 Section 18 of the ISS Act 2017.
28 See also report no. 38 (2014), p. 29.
29 See report no. 56 (2018) on the multilateral exchange of data on (alleged) jihadists by the AIVD, Appendix II, p. 2.

In addition, the data processed by the services must be done properly and with due care.[30] The criterion of propriety is linked to the fulfilment of the proportionality requirement.[31] The infringement of fundamental rights involved when passenger data is processed must therefore, in the context of this investigation, be proportionate to the purpose (the weight of the operational interests).[32] Compliance with the legal requirements of necessity and propriety for collecting data overlaps considerably with the general requirements for the use of an investigatory power, as detailed in Section 2.5 below.

Careful data processing also relates to the accuracy and current relevance of the data that is processed.[33] The data that is to be processed must contain an indication of the level of reliability of the data or a reference to the document or source from which the data derives.[34] The reliability indication can also be helpful in assessing information derived from, for example, a data analysis or data aggregation.[35] These requirements must be taken into account when disclosing data on the services' digital infrastructure. The reliability assessment must be recorded.

2.5 General requirements for the use of investigatory powers (Section 26 of the ISS Act 2017)

The use of an investigatory power by the AIVD and the MIVD must be reviewed against the general requirements of Section 26 of the ISS Act 2017. Those general requirements are proportionality and subsidiarity.[36]

Proportionality

Proportionality means that an assessment must be made of the objective that is being sought and the disadvantage to the party involved, generally the corresponding infringement of fundamental rights. In those cases a check must be made whether the purpose of collecting passenger data for the AIVD and the MIVD's tasks outweighs the infringement of the involved party's fundamental rights that the collection of data entails. The use of the investigatory power should be proportionate to the intended objective.

The further processing of airline passenger data by the AIVD and MIVD also entails an infringement of the involved parties' fundamental rights because personal data is processed in the services' systems.[37] 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, i.e. a 'bulk data set'.

The data can be combined with other data and processed further. The above circumstances point to a severe infringement of the fundamental rights of those involved and for that reason, the services formulated a policy for bulk data sets (see Section 2.6).

30 See Section 18(2) of the ISS Act 2017. In its report no. 56 (2018) the CTIVD specifies in greater detail what the safeguards of necessity, propriety and due care entail in the provision of data to foreign partners. See also report 65 (2019).
31 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 31.
32 See also report no. 56 (2018), p. 11.
33 See also CTIVD report no. 56 (2018). The data must not be superseded by other, more recent data.
34 Section 18(3) of the ISS Act 2017.
35 See also CTIVD report no. 57 (2018).
36 During the current investigation, the requirement 'as targeted as possible' only applies to the use of investigatory powers, see 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, including exercising the power to use informants or the investigatory power to receive data from the Police, KMar and the tax authorities, based on Section 94 of the ISS Act 2017. The policy for bulk data sets, which exceeds the statutory minimum, does implement the requirement 'as targeted as possible' to a certain degree (see Section 2.6 below).
37 ECHR case law suggests that storing and further processing personal data constitutes an infringement of the right to privacy. Briefly put, based on this case law the following must be taken into account: (1) the context in which the data is collected, (2) the nature of the data and (3) the way in which that data is further processed and used. Any further processing of personal data means a more severe infringement of privacy. See report no. 55 (2018) for a more detailed discussion of this ECHR case law.

Subsidiarity

Lastly, the subsidiarity assessment means that the AIVD or the MIVD must opt for the investigatory power that is least invasive to the party involved.[38] It should be noted in this respect that exercising the investigatory power to use informants and the investigatory power to obtain information from the KMar are general investigatory powers, not special investigatory powers. The use of special investigatory powers such as intercepting communication is generally considered more invasive to the parties involved.

2.6 Policy on collecting bulk data sets

The AIVD and the MIVD published their policy on the acquisition and processing (use) of bulk data sets in May 2018. That policy was published after the Minister of the Interior and Kingdom Relations and the Minister of Defence adopted the recommendations in the CTIVD report no. 55 (2018) on bulk data sets offered on the internet by third parties.[39]

The AIVD and MIVD's bulk data policy states that in order to collect and further process data from the bulk data set, a written substantiation is required which includes (1) specifying the purpose, (2) describing the necessity and (3) weighing the interests. The policy further notes that it is not permitted to store more data than necessary for the purpose for which the data is collected. By applying this condition of data minimization, the amount of data is limited accordingly, for example by not collecting, storing and processing certain types of data (such as sensitive data) or by destroying data that is no longer relevant to the purpose.

The bulk data set policy further specifies that the head of service or the relevant minister must authorize the collection of bulk data, depending on the nature of the data.[40]

2.7 Record keeping (Section 31 of the ISS Act 2017)

Records are kept of the use of an investigatory power.[41] Any assessments made of the proportionality and subsidiarity of collecting passenger data must be recorded.[42]

The duty to keep records of the use of an investigatory power not only serves internal control purposes but also enables effective external review by the CTIVD. In addition it can play a role in issuing a notification report.[43]

The legislator leaves open the manner of reporting. Consequently, methods other than written records are possible. Automated recording (logging) can also be considered a form of record keeping.[44]

38 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 202.
39 See for example https://www.aivd.nl/onderwerpen/werken-met-grote-datasets.
40 Report no. 55 (2018), p. 13.
41 Section 31 of the ISS Act 2017.
42 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 41.
43 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 50. Incidentally, records do not need to be kept for the use of traditional media and public documents because this would cause a disproportionate administrative burden, according to the legislator.
44 *Parliamentary Documents II* 2016/17, 35488, no. 3, p. 50.

2.8 Interim conclusion

Now that the legal framework regarding the collection of passenger data has been considered, the following legal requirements can be defined:

- Collecting airline passenger data is given a legal basis in the investigatory 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 the proportionality and subsidiarity principles is required to use a general investigatory power (Section 26 of the ISS Act 2017). Records must be kept of the use 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 for data processing 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. 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 data may be processed for the purpose of the AIVD and the MIVD's tasks (Sections 8 and 10 of the ISS Act 2017), in so far as the general requirements of data processing have been met, including that the data is processed for a certain purpose and only in so far as necessary for the services' tasks (Sections 18 and 19 of the ISS Act 2017).
- The AIVD and the MIVD have the duty to cooperate. That cooperation can take the form of the AIVD and the MIVD exchanging passenger data from airlines (Section 86(2) of the ISS Act 2017).

3. The further processing of passenger data

AIVD and MIVD staff may further process passenger data to carry out their tasks.[45] The ISS Act 2017 sets additional rules for this data processing.

This section looks in more detail at the legislation on the further processing of passenger data. It goes without saying that the general requirements for data processing apply, as set out in Section 2.4. The careful processing of data is given further substance by the policy on processing data from bulk data sets, the rules on automated data analysis, the duty of care, the processing of special personal data, the removal and destruction of data, the handling of data from professionals entitled to privilege and the duty of care. The legal requirements are described briefly in this section.

3.1 General requirements for processing data (Sections 18-24 of the ISS Act 2017)

The general requirements for data processing are set out in Section 2.4. Where the further processing of passenger data by service staff is concerned, that data should only be processed for a certain purpose and in as far as necessary for the services to carry out their tasks.[46]

In addition, data processing by the AIVD and the MIVD must be done properly and with due care.[47] Data that is to be processed must contain an indication of the level of reliability of the data or a reference to the document or source from which the data derives.[48] The indication of reliability can also be helpful in assessing information derived from, for example, a data analysis or data aggregation.[49]

3.2 Processing data from bulk data sets

As described in Section 2, the AIVD and MIVD's bulk data set policy applies to the processing of passenger data, because it concerns large amounts of data of which it is clear in advance that the majority of that data is not related to targets (people or organizations) of the service. Section 2.6 sets out that collecting data requires a written substantiation and – depending on the nature of the data – authorization by the head of the service or the responsible minister.

The severe infringement of the fundamental rights involved with processing passenger data is a reason to apply certain safeguards when the data is processed further. The policy on bulk data sets, published by the services, sets out 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 information to carry out their tasks. In other words, staff must be granted authorization to gain access to the data.

It is the CTIVD's view that other safeguards should also be considered, in particular where internal control mechanisms are concerned. In the context of careful data processing of bulk data sets offered on the internet by third parties, the CTIVD set out in its report no. 55 (2018) that actions relating to bulk data sets must be recorded by logging and that automated reports must be drafted on that basis for

45 Section 1(f) of the ISS Act 2017. See Section 2.4 on the AIVD and the MIVD's responsibilities.
46 Section 18 of the ISS Act 2017.
47 See Section 18(2) of the ISS Act 2017. In its report no. 56 (2018) the CTIVD specifies in greater detail what the safeguards of necessity, propriety and due care entail in the provision of data to foreign partners. See also report 65 (2019).
48 Section 18(3) of the ISS Act 2017.
49 See also report no. 57 (2018).

internal control purposes of the services and external control purposes of the CTIVD.[50] That provision may also be seen as an interpretation of the duty of care (see Section 3.7).

In addition, an assessment must be made whether the access to passenger data should be further restricted. That depends on the relationship between the operational necessity to use the data and the infringement made on the fundamental rights of the parties involved. In its report no. 55 (2018) the CTIVD considered the access by staff to already accessed information and the mechanism of internal authorization to be lawful.

3.3 Automated data analysis (Section 60 of the ISS Act 2017)

The AIVD and the MIVD are authorized to apply automated data analysis to the collected passenger data.[51] Automated data analysis consists in the current investigation of comparing the files in an automated way.[52]

The services are also authorized to use other forms of automated data analysis, such as searching data based on profiles or with a view to establishing certain patterns.[53] Legislative history states that if the services use new technologies for automated data analysis, they must explore the possibilities of the new technology beforehand and the pros and cons, including any possible privacy risks.[54] The data-processing provisions apply fully to automated data analysis as well, which means that data should only be processed for a certain purpose and only in as far as necessary for the services to carry out their tasks. In addition, the data processing by the AIVD and the MIVD must be done properly and with due care.[55] It is self-evident that, in a large-scale data analysis of passenger data, the recording and logging of the processing activities are also sufficient to enable internal control and assessment by the CTIVD of the lawfulness of the data processing involved (Sections 18-24 of the ISS Act 2017).

The use of automated data analysis is not subject to any authorization requirements where it does not concern the automated data analysis of data from investigation-related interception to identify people and organizations. When automated data analysis of passenger data is not combined with data derived from investigation-related interception, the special investigatory power for automated data analysis in not applied.[56] Promoting or taking measures based purely on the results from automated data analysis is not permitted – human intervention is always required.[57]

3.4 Sensitive personal data (Section 19 of the ISS Act 2017)

Sensitive personal data may in principle not be processed unless it is unavoidable (Section 19(4) of the ISS Act 2017). The use of the word 'unavoidable' indicates that the assessment here is more stringent than the general assessment of necessity of Section 18(1) of the ISS Act 2017.[58]

Sensitive personal data is data relating to someone's religious or personal beliefs, race, trade union membership, health or sexuality.[59] The current investigation focuses on API data collected under Directive 2004/82/EC. The directive includes a full list of the data which the airlines must store. The

50 Report no. 55 (2018), p. 18 and p. 22.
51 Section 60(1)(d) of the ISS Act 2017.
52 Section 60(2)(a) of the ISS Act 2017.
53 Section 60(2)(b)(c) of the ISS Act 2017.
54 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 132.
55 Section 18 of the ISS Act 2017.
56 Section 50(1)(b) in conjunction with Section 60 of the ISS Act 2017.
57 Section 60(3) of the ISS Act 2017.
58 *Parliamentary Documents II* 2016/17, 34588, no. 3, p. 34.
59 The ISS Act 2017 does not classify people's political affinity as sensitive personal data.

data on the list does not include sensitive personal data and consequently that list limits the type of data the AIVD and the MIVD can receive from the KMar.

3.5 Removal and destruction (Section 20 of the ISS Act 2017)

Data collected under a general investigatory power, such as the power to use informants, must be removed once it has lost its significance.[60] That is the case when the data is no longer relevant to the services' tasks. Removal means that the data is no longer accessible in the regular process (the services' tasks). The data may be made accessible again if the data becomes relevant again to the services' tasks. Removed data must be destroyed unless the legal rules on retention preclude this, notably the Public Records Act 1995.

The ISS Act 2017 therefore does not set any absolute limitation for storage of data collected with a general investigatory power. However, in the context of passenger data from airlines collected in bulk, the significance of that data must, based on the bulk data set policy, be checked periodically. The services' policy for bulk data sets stipulates that the AIVD and the MIVD must check periodically whether the bulk data set is still necessary to achieve the purpose for which it was obtained.[61] That evaluation must be accessible to the CTIVD.

3.6 Use against lawyers and journalists (Section 30 of the ISS Act 2017)

The ISS Act 2017 contains specific rules regarding the use of investigatory powers against journalists and lawyers. The Court of The Hague must grant authorization if the use against a journalist could lead to 'the acquisition of information about the journalist's source.'[62] The Court of The Hague must also grant authorization if a special investigatory power is exercised against a lawyer and this use could lead to the 'acquisition of data relating to the confidential communication between a lawyer and his client'.[63]

These provisions in the ISS Act 2017 relate to the collection of data using a special investigatory power and not to data collected using a general investigatory power. In the context of processing passenger data it is unlikely that the services will process data from the confidential communication between lawyers and their clients or that these data-processing activities reveal the source of a journalist.

3.7 Duty of care (Section 24 of the ISS Act 2017)

The heads of the AIVD and the MIVD are responsible for applying technical, staffing and organizational measures to ensure data is processed lawfully.[64] One new element compared with the former ISS Act 2002 is the duty to promote the quality of the data processing. The duty of care explicitly requires more from the AIVD and the MIVD than simply implementing the legal requirements imposed on them for collecting, analysing and use of the data by service staff.[65]

60 Section 20 of the ISS Act 2017.
61 See also report no. 55 (2018), p. 23.
62 Section 30(2) of the ISS Act 2017.
63 Section 30(3) of the ISS Act 2017.
64 Section 24(2)(a) of the ISS Act 2017.
65 See also report no. 59 (2018), p. 7.

The duty of care when processing data means that both services continuously monitor how they process data and ensure that this data processing is and remains in accordance with the applicable legal requirements (compliance). Policy, process descriptions and work instructions may have a contributory role, with a view to assigning positions and responsibilities.

This ongoing monitoring requires the services to use a number of instruments that provide a central overview of the functioning of processes and data-processing systems and that allow them to identify risks and take measures promptly.

3.8 Interim conclusion

Now that the legal framework regarding the collection of passenger data has been considered, the following legal requirements can be defined:

- The data must be processed for a specific purpose and be necessary to the services' tasks. Any further processing activities must be conducted in a proper and careful manner and the data must be reviewed on reliability and accuracy (Sections 18 and 19 of the ISS Act 2017).
- When using new technologies for automated data analysis an advance exploration must take place of the possibilities and risks to the privacy, among other things (Sections 18 and 24 of the ISS Act 2017).
- The policy for bulk data sets implements the obligation of careful data processing by requiring 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 as to enable sufficient 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 relating to data processing means that the services have 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).

4. Summary of legal requirements

Based on the assessment framework, the CTIVD has defined the following requirements for the collection and the further processing of airline passenger data:

- The data may be collected and further processed for the purpose of the AIVD and the MIVD's tasks (Sections 8 and 10 of the ISS Act 2017).
- Collecting airline passenger data is given a legal basis in the investigatory 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).
- The AIVD and the MIVD have the duty to cooperate. That cooperation can take the form of exchanging passenger data from airlines (Section 86(2) of the ISS Act 2017).
- The data must be processed for a specific purpose and be necessary to the services' tasks. Any further processing activities must be conducted in a proper and careful manner and the data must be reviewed on reliability and accuracy (Sections 18 and 19 of the ISS Act 2017).
- An assessment of the proportionality and subsidiarity principles is required to use a general investigatory power (Section 26 of the ISS Act 2017). Records must be kept of the use made of the investigatory power to use informants (Section 31 of the ISS Act 2017).
- The bulk data set policy further implements the general requirements for data processing in Section 26 of the ISS Act 2017 by requiring a written assessment. This 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 specified purpose. 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.
- When using new technologies for automated data analysis an advance exploration must take place of the possibilities and risks to the privacy, among other things (Sections 18 and 24 of the ISS Act 2017).
- The policy for bulk data sets implements the obligation of careful data processing by requiring 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 as 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 in place that form a practical interpretation of the legal requirements. 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).

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