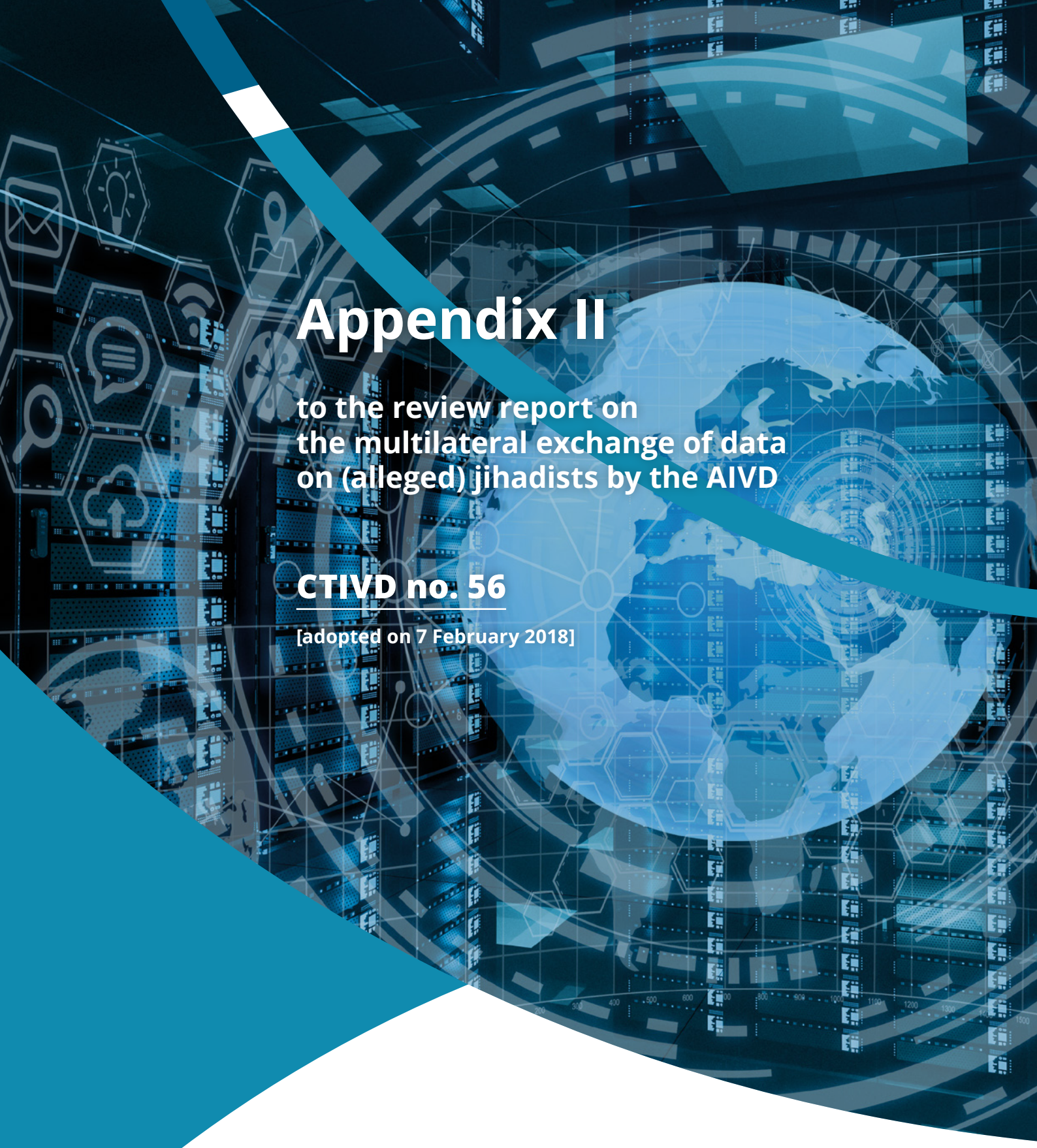

Appendix II

to the review report on the multilateral exchange of data on (alleged) jihadists by the AIVD

CTIVD no. 56

[adopted on 7 February 2018]

CTIVD
Review Committee on the Intelligence and Security Services

Review Committee
on the Intelligence and
Security Services

CTIVD no. 56

APPENDIX II

**to the review report on
the multilateral exchange of data
on (alleged) jihadists by the AIVD**

Findings of the CTIVD on the safeguards for the multilateral exchange of data

1 Introduction

Safeguards for the multilateral exchange of data on (alleged) jihadists may be derived from, *inter alia*, the general principles laid down in the EU Charter, the European Convention on Human Rights (ECHR), Convention 108 and the case law of the Luxembourg and Strasbourg courts. This, *inter alia*, concerns the principles that the processing of personal data must be necessary for a certain legitimate objective, is proportional and takes place with due care. This final requirement at any rate means that the processing of data must be adequate, relevant, accurate and up to date. Other protection mechanisms, such as having a retention period in place, protecting certain special categories of personal data, implementing technical and organisational measures to protect personal data, and ensuring compliance are also essential. In addition, safeguards with respect to independent, adequate and effective oversight are laid down.

As a rule, the general data protection principles have been transposed into the national legislation regulating the activities of the intelligence and security services. This is also true for the Netherlands. The ISS Act 2002 (and the new ISS Act 2017) contain multiple data protection provisions. In section 2 of this Appendix, the CTIVD explains what the legal requirements of necessity, propriety, due care and (the indication of) reliability entail in the context of the multilateral exchange of data on (alleged) jihadists by the AIVD.

This Appendix also addresses the extent to which these safeguards are reproduced in multilateral agreements concluded within the context of the CTG and sigint cooperation or in the AIVD's internal policies. The CTIVD is not allowed to extensively discuss the contents of the multilateral agreements in this public appendix due to them constituting state secrets. They are further detailed in Appendix II to the classified review report.

In addition, the CTIVD assessed (by way of random checks) whether the AIVD observes the policy in practice. The CTIVD's findings are summarised in sections 3 and 4, below. On the basis of these findings, the CTIVD has drawn conclusions on the current practice. These conclusions are detailed in Chapter 7 of the review report. Wherever data protection safeguards are lacking or are (as yet) insufficiently embedded, risks exist. The CTIVD discusses this in Chapter 8 of the review report.

2 The legal requirements

2.1 Necessity

Pursuant to Article 12(2) of the ISS Act 2002 / Article 18(1) of the ISS Act 2017, the provision of data to a foreign service must be necessary to achieve a specific, legitimate objective. In concrete terms, this means that the AIVD:

1. must have an objective that is detailed in advance and is in line with the statutory tasks of the AIVD;
2. must have the reasonable expectation that this objective is served by the provision of the data to the foreign service or services concerned;
3. is able to substantiate this.

A similar methodology applies to the use of data which the AIVD has received and to the (joint) analysis of data. Each form of data processing must be necessary to achieve a specific, legitimate objective. This forms an important safeguard for the protection of the fundamental rights of the person whose data is being processed.

Multilateral objective

In the case of the provision of data within a multilateral cooperative partnership, the objective is always a relatively general one. This is inherent to the multilateral sharing of data, in particular in a larger group. The AIVD expects that the provision of data on (alleged) jihadists to the other foreign services participating in the cooperative partnership contributes to the international fight against jihadism. The objective here is to improve the common information position, that is, to improve the existing image of the threat posed by jihadism, in order to counter this threat. The necessity assessment is virtually the same for each target whose personal data is provided by the AIVD. The multilateral nature of the exchange of data means that a more concrete objective cannot be properly specified.

Threshold

The value of the necessity assessment can be questioned in light of the above. How does it provide a safeguard for the protection of fundamental rights? Even though this assessment can only be a general one in the practice of multilateral cooperation, the CTIVD is of the opinion that it does constitute a *threshold* for the exchange or analysis of data. This threshold is higher the more specifically it is laid down what exchange or analysis of data is required to achieve this objective. This threshold is lower the more general the description and when the description is susceptible to multiple interpretations.

In other words, the necessity safeguard requires a clear definition of the cases allowing for the exchange of data. Does it concern persons who have actually left the country for conflict areas, persons who tried to do so or persons who had plans to do so? What about women and children who are taken along? Does it also concern persons recruiting jihadist fighters or facilitating travel to the conflict areas, for instance by funding or organising it? What threshold is applied to the exchange of personal data within the cooperative partnership?

2.2 Propriety

Propriety means that the objective of the data exchange is proportional to its negative impact on the person involved. In particular this relates to interference with someone's fundamental rights because data is provided to a group of foreign services that may use this data in their own intelligence process. The interference with the fundamental rights must be counterbalanced by sufficiently important interests, i.e., the objective the AIVD aims to realise. If the seriousness of the interference with fundamental rights outbalances the importance of the operational interests in question, this constitutes improper conduct.

Seriousness of the interference

The seriousness of the interference with someone's fundamental rights by multilaterally exchanging personal data is determined by:

1. The number of foreign services and/or other bodies the data is provided to;

The greater the number of bodies that have or gain access to the personal data, the greater the level of interference with the fundamental rights of the person whose data is provided. Not just the provision of data is relevant in this connection; so too is the degree to which that data is in turn provided to third parties. Multilateral agreements may be concluded to cover this aspect. Whether the AIVD may assume that its data is not simply provided to other bodies in turn is mainly one of trust and experience, as gained over the existence of the cooperative partnership. The risk assessment referred to in the above must conclude whether any risks exist in this connection.

2. The use of the data by those services and bodies;

If the provision of the data leads or may lead to the implementation of criminal-law, administrative-law, or other measures against the person concerned, the interference is more serious than if this is not the case. In this context it is important that the AIVD has a good notion of the nature and tasks of the service or services the data is provided to. The risk that the data provided by the AIVD will be used for taking measures against a person is greater in the case of provision to a security service with an investigatory task than in the case of a security service without any combined tasks. Such risks must be addressed in the weighting notes which are to be to be drawn up for each foreign service. Whether the AIVD may assume that the data is not used for other objectives or in other ways than what was agreed upon is also a matter of trust and experience gained in the cooperative relationship. The risk assessment referred to above must show whether any risks exist in this connection.

3. The amount of personal data and the sensitivity of the data provided.

There is a difference between only providing identifying data, such as a name, date of birth or telephone number, and providing also other personal data, such as the family situation of the person concerned or their social media activities. The seriousness of the interference is greater where especially sensitive categories of persons or personal data are concerned, such as data on minors or data related to someone's health or sexual life. Such categories require additional protection. The ISS Act 2002 contains additional safeguards with respect to special categories of personal data (Article 13(3) and (4)). Such data may be processed only in addition to the processing of other data and only to the extent this is unavoidable for the objective to be achieved.

Importance of the (operational) interests

The counterbalance on the other side of the scales is made up of the objective to be achieved by the exchange or analysis of data. As was stated above in the section on necessity the objective in the case of multilateral cooperation is of a general nature and similar for each exchange or analysis performed. In each case, the aim is to strengthen the (joint) information position for the purpose of the international fight against jihadism.

This objective is given more or less weight by the prioritisation of the target. "Prioritisation" refers to the importance attached to the person in question by the AIVD in the context of the investigation conducted by the service. This prioritisation can be can be substantially based on the threat a person poses, but other circumstances may play a role, as well. The threat posed by someone who has left the country for a conflict area, gained combat experience and returns to Europe is generally greater than the threat posed by someone who only provides financial support or recruits jihadist fighters, for instance. If a person returning from a conflict area is arrested and detained, this person's priority level is lower, due to their circumstances, than that of a returning fighter who is still able to move freely. The prioritisation determines the counterbalance to the seriousness of the interference with someone's fundamental rights.

2.3 Due care

The requirement of due care is laid down in Article 12(3) of the ISS Act 2002 / Article 18(2) of the ISS Act 2017 (data processing) and Article 16(a) of the ISS Act 2002 / Article 24(2)(2) of the ISS Act 2017 (data processing processes).

Due care with respect to the data provided

Due care relates to the correctness of the contents of the personal data exchanged and to the correct reproduction of that data. The party receiving the personal data must be able to assume that the data is accurate, i.e., is supported by underlying data and reproduced correctly. It is important in this connection that the personal data is unambiguous and not susceptible to multiple interpretations. Accuracy of the data also refers to the data being sufficiently up to date, in particular where it concerns exchanged data that has been stored and is available for inspection by other services. The user must be able to assume that the data is not superseded by more other, more recent data.

The manner of providing the data is important as well. The ISS Act 2002 provides that personal data is provided in writing if the receiver is authorised to take measures on the basis of that data (Article 40). This can only be deviated from in urgent cases. The question whether a foreign service has this authority must be answered by way of the above-mentioned risk assessment on the basis of cooperation criteria. Charting the legal powers of the foreign service in question is part of this. If such an assessment is lacking, the AIVD must, in the opinion of the CTIVD, assume that the foreign service is indeed authorised to take measures. This means that the written provision of personal data is a basic condition for the exchange. Should personal data still be provided orally, because of an urgent situation, this must, at the least, be recorded in writing (Article 42).

Another element of due care concerns the destruction of data. The AIVD must regularly assess whether the data provided by the service that is accessible to other services (still) has relevance to the objective it has been processed for. If this is not the case, the data must be removed (Article 43(1) of the ISS Act 2002). Incorrect or wrongfully provided data must also be removed (Article 43(2) of the ISS Act 2002).

Due care with respect to the system

Due care also relates to (automated) data processing processes. To that end the ISS Act 2002 provides that necessary provisions must be made to promote the accuracy and completeness of the data processed (Article 16(a)). This also means that the system must provide functionality for the destruction of data. The ISS Act 2017, which has not yet entered into force, contains a more comprehensive duty of due care for the quality of the data processing (Article 24(2)(a)).

2.4 Reliability

Indication of the reliability of personal data

Reliability relates to the degree to which personal data has been established and verified. The source of the data, the reliability of that source and the probability of the data being accurate are important in this connection. Article 12(4) of the ISS Act 2002 provides that the data processed by the AIVD must be provided with an indication of the degree of reliability or of a reference to the source from which the data is derived.

It is difficult for another service to verify the reliability of data provided. To a large extent this is a matter of trust and is an extension of the estimation of the professionalism and reliability of the foreign service itself. This is one of the cooperation criteria the above-mentioned risk assessment is based on. Without such a risk assessment, it cannot be properly determined whether and to what extent risks exist in this area.

Reliability of the system

Reliability also relates to (automated) data processing processes, such as a data exchange system. Is the data sufficiently protected? Can the data be modified, deleted or destroyed by anyone just like that? Is the access to the data sufficiently limited? The ISS Act 2002 provides that the head of the service must ensure that the necessary provisions of a technical and organisational nature are in place to protect the processing of data against data loss, data corruption or unauthorised processing of data (Article 16(b)). This provision has also been included in the ISS Act 2017 (Article 24(2)(a)).

3 Safeguards for the exchange of data by the AIVD within the CTG

3.1 Necessity of data exchange within the CTG

To the extent no clear, multilateral definition of the cases necessitating the exchange of data via the CTG database exists, the AIVD must apply its own threshold. The CTIVD finds that until early 2017, the AIVD provided personal data within the CTG if it concerned a person who had actually left the country for a conflict area or for whom there were concrete indications that this person is involved in preparing an attack. This changed in early 2017. For some time now, data on persons who have not left the country and persons posing less of a threat is also being recorded in the database. Of some of the persons added to the database, it is not stated which terrorist activities necessitate their being recorded in the database. The CTIVD has established that in each case, the person involved is someone under active investigation by the AIVD.

In August 2017, the AIVD laid down which cases did and did not allow for provision of data in its internal policy. The policy states that it must concern "identified counter-terrorism targets" and that "sharing the data on these targets with all CTG partners must be necessary for the performance of the service's tasks". The CTIVD is of the opinion that this definition is of limited meaning: it is so general a definition that the group of persons whose data is shared is insufficiently limited. As a threshold for data exchange by means of the CTG database it is of little consequence.

Within the operational platform, it is decided on a case-by-case basis which group of persons the investigation can focus on. So far, a sufficiently clear delineation of such groups of persons is applied. The personal data provided by the AIVD falls within this delineation.

3.2 Propriety of data exchange within the CTG

Seriousness of the interference

Within the CTG, data is commonly provided to 29 services. Each piece of data added to the database is (almost) immediately accessible to all participating services. Data shared within the operational platform is usually shared with a more limited group of participating services, depending on the participants. All 30 services may participate.

The data may not be provided to other bodies. This rule, also referred to as the third-party rule, has been enshrined in law for the AIVD (Article 37 of the ISS Act 2002 / Article 65 of the ISS Act 2017). For each piece of data provided by the AIVD, the database states whether the AIVD permits the provision of the personal data to national bodies active in the field of counter-terrorism.

The CTIVD has established the data provided by the AIVD within the CTG is meant for use within the intelligence process of the participating services. Use of the data outside of the intelligence process, for instance for the purpose of criminal-law proceedings, is permitted only if the third-party rule is observed (as outlined in the above). Use of the data outside of the objective of the international fight against jihadism is not permitted.

The provision of data by the AIVD via the CTG database does not automatically result in measures being taken, such as freezing someone's financial assets. For this, other national and international procedures apply which are separate from the data exchange within the CTG. The data provided may,

however, result in alerts being placed in national or international alert systems, such as the Schengen Information System. The alerts make border control possible.

During its investigation, the CTIVD found that the AIVD, as yet, mainly exchanges identifying data and exchanges other personal data to a limited extent only. It is up to the AIVD itself to assess which data on a target it does and does not provide via the database. While it is possible for the AIVD to record a great amount and a wide variety of data on a target in the database, it has, so far, never done so. The CTIVD does identify a risk related to sharing more, and more sensitive, data. It discusses this risk in Chapter 8. Also within the operational platform the AIVD mainly shares identifying data, sharing other personal data to a limited extent only.

As yet, the CTIVD has not found any sensitive categories of personal data as referred to in Article 13(3) of the ISS Act 2002 that was provided by the AIVD in the database. Nor has it found that any such data has been shared within the operational platform by the AIVD. In the context of the multilateral purpose of the data exchange, the condition that sensitive personal data may only be exchanged when this is unavoidable will not easily be met.

The exchange of data on minors does occur. The AIVD's policy is to provide personal data on minors aged 9 or over who have left the country for conflict areas. According to the AIVD, minors may be deployed as jihadist fighters from that age onward.[1] The CTIVD has identified a risk with respect to the recognisability of this category of persons in the CTG database. It discusses this in Chapter 8 of the review report.

Importance of the (operational) interests

Each person recorded in the database by the AIVD is provided with a priority level. The AIVD applies a prioritisation system. The persons whose data has been provided by the AIVD have generally been assigned a high priority level, *inter alia*, on the basis of the threat these persons pose. The CTIVD finds that, from early 2017 onward, the AIVD has been adding relatively more persons with a lower priority level to the database.

Within the operational platform, the prioritisation of a specific target is determined jointly by the participating services. Whenever the AIVD provides data within the operational platform, this relates to targets with a high to mid-high priority level within the AIVD.

3.3 Due care of the exchange of data within the CTG

Correct reproduction

Every target added to the database by the AIVD is recognisable as such. When the AIVD adds data or supplements data added by another service, the source of that data is recognisable. By way of a random check, the CTIVD investigated whether the data added to the database by the AIVD is reproduced correctly. This is the case. Only a few minor errors have been identified in the data investigated in this connection. These have since been remedied by the AIVD.

[1] Also refer to the joint NCTV and AIVD publication "Minors with ISIS" of 6 April 2017, available on www.aivd.nl.

Provisions to promote correct reproduction

A number of system-technical safeguards have been created by the AIVD for the correct reproduction of personal data in the CTG database. For instance, there is a fixed number of fields per target that have to be filled out and a fixed number that can optionally be filled out. There are also fields that have to be filled out in a fixed format, i.e., always in the same manner. Following these formats is not mandatory. Deviations are noted in red by the system. In addition, a system for the automated identification of data completed incorrectly, i.e., data not meeting the agreed-upon format, has been put in place. Whenever data is reproduced incorrectly, the providing service is notified of this incorrect reproduction by the system, which also proposes modifications. In addition, the CTIVD finds that the database is user-friendly and that it is easy to search for information in it. The fields to be completed are clear and provided with an information icon opening a more detailed explanation. In addition, a clear user manual is available and the AIVD gives training courses, both internally and to other services participating in the CTG. The above significantly contributes to the correct reproduction of the data in the database.

Accuracy and completeness

Accuracy of the personal data refers to the correctness of its contents and to it being up to date. This is not only important when adding a new target to the database. Whenever new data becomes available during the investigation into the activities of a person, it is up to the service that first provided the data to edit or supplement it. This is absolutely vital. After all, the participating CTG services must be able to assume that the personal data in the database is accurate and up to date.

Much depends on the standard applied by the service that provided the data, both for the contributing of data on a person and for keeping this data up to date. The national AIVD procedure must, therefore, sufficiently guarantee the accuracy of the data. This means that the data must, at the least, (still) be substantively correct and up to date. It is important, for instance, that the database is updated if it turns out that a person has joined another militia, travelled to another country or has died.

Within the AIVD, the head of a team must grant permission for adding a new target to the database. In addition, all newly added targets are checked by a team specifically focusing on prioritisation. This concerns an additional check. A processor is responsible for changing or supplementing data. The four-eyes principle applies in this connection: the action is supervised by a senior processor. At the moment of drawing up this Appendix, the procedure is being further detailed in an internal working instruction.

By way of a random check, the CTIVD investigated whether the data added to the database by the AIVD is accurate and up to date. This is true for the majority of the data. However, the CTIVD has also identified some data in the database that insufficiently corresponds to the data present in the AIVD's national systems, for instance because it is incomplete or not yet updated. This is addressed in further detail in Chapter 8 of the review report.

Provisions to promote correctness

The AIVD has put mechanisms in place that contribute to identifying inaccurate data. The possibility of other services adding data to data on a specific person recorded in the database is of prime importance in this connection. This allows for quality improvement. In the autumn of 2017, the database also shows when data has most recently been edited, and by which service. This may provide an indication when data is no longer up to date..

Written provision

The basic condition of provision taking place in writing plays a particularly important role in the framework of the CTG operational platform. This platform is organised in such a way that the representatives of the participating services are physically close together at one location. Meetings where data on a specific case is exchanged are held regularly. This concerns the exchange of personal data. The CTIVD finds that the AIVD makes records of these meetings. These records state which party has provided which data during the platform meeting. The records appear to be extensive and detailed. However, the CTIVD has identified certain risks with respect to the oral provision of personal data. It addresses these in more detail in Chapter 8 of the review report.

Destruction of data

The data in the database provided by the AIVD is stored independently of the national regime. The AIVD itself assesses whether the data provided by the service is still relevant or needs to be destroyed. During the investigation period, the AIVD had no policy in place on how the data in the database provided by the AIVD is kept up to date and, where relevant, destroyed, nor on who is responsible for this. This has by now been implemented. The AIVD adopted policy to this effect in August 2017.

The database does not provide system-technical destruction safeguards, such as alerts which are issued when personal data have not been supplemented or modified for some time and, therefore, might no longer be relevant or automatic destruction after a certain amount of time.

The AIVD is able to copy data recorded by another service and to be destroyed by this other service. No limitations are in place for this situation.

Data exchanged within the operational platform must be included in the records of the platform meetings. The records are submitted to the services that participated in the meetings concerned. The AIVD must regularly assess whether the records available to the service are still relevant to the objective they were processed for.

The CTIVD has also identified risks with respect to the destruction of data. These are addressed in Chapter 8 of the review report.

3.4 Reliability of data exchange within the CTG

Indication of reliability

In general, intelligence and security services keep their sources secret. Providing insight into the exact origin of data is unusual, to say the least. The cooperation in the operational platform changes this somewhat. Being physically located together and intensively discussing specific operational cases results in the participating services granting more and more insight into their procedures and sources of information. In that context the reliability of data can be discussed orally.

The AIVD included the option to mark unreliable data with a red tag in the CTG database. This implies that all data not featuring such a red tag, is reliable. The exact definition of established or verified data can vary per participating service.

For the data provided by the AIVD itself, there is a legal requirement that it is provided with an indication of reliability or a source reference. The AIVD does not provide such an indication or reference. Nor do internal documents stipulate that the AIVD may only provide completely reliable data by way of the database or within the operational platform. In August 2017, the type of data that may be provided via the CTG database was laid down in the AIVD's internal policy.

The CTIVD has tested the reliability and/or source of the data provided by the AIVD through the database and to the operational platform by way of random checks. This has not resulted in any indications that the data provided is insufficiently reliable.

Reliability of the system

The AIVD has internally tested the functioning of the database in terms of data protection, assessing a number of system aspects and addressing the risks, responsibility and security measures. The conclusion was that the system is deemed suitable for the processing of data of up to the classification level "secret". The results of the accreditation performed were provided to all services participating in the cooperative partnership. The CTIVD has no reason to doubt the thoroughness of the AIVD's accreditation process.

Another element of the accreditation of the system concerned the access to the system and the authorisation to add, edit or destroy data. Access to the system has been granted to a large group of participants. The AIVD decides which of its own staff should have access. Within the AIVD, all members of staff active in the field of counter-terrorism have access to the database at any rate. Counter-terrorism team processors and some other members of staff are authorised to add and edit data.

Incidentally, only the service that has initially provided a piece of data is system-technically allowed to edit or destroy it. This means that another participating service cannot edit or destroy data added by the AIVD. An exception to this is the service responsible for the system's functioning. The AIVD, being the administrator, is in practice able to edit or destroy data.

4 Safeguards for the exchange of data by the AIVD within sigint cooperation

4.1 Necessity of data exchange within sigint cooperation

It is inherent to the exchange of unevaluated data that its necessity can only be determined in general terms and broad outlines. It is impossible to provide a well-delineated definition of the jihadists whose data is provided if it is impossible to know in advance who the data relates to. The necessity thresholds that apply cannot, therefore, be directly compared to the necessity thresholds applying to the exchange of evaluated data (as takes place within the CTG). Multilateral agreements within sigint cooperation provide substance to the necessity requirement. The threshold for the exchange of *unevaluated* data is sufficiently high. The same applies to the exchange of *evaluated* data.

4.2 Propriety of data exchange within sigint cooperation

Seriousness of the interference

The seriousness of the interference with fundamental rights is determined by the number of services personal data is provided to, the use of the data and the amount and sensitivity of the data. The propriety safeguard is of limited importance in the context of the exchange and analysis of metadata (in bulk) because it is not clear in advance exactly whose personal data is provided. The interference with fundamental rights can only be charted in a general sense, and not specifically for any one person.

Nothing can publicly be said about the number of services personal data is provided to within the context of sigint cooperation. However, it does concern fewer services than is the case within the CTG.

Multilateral agreements within sigint cooperation safeguard to an important extent that the use of the exchanged data and its provision to third parties is limited.

Importance of the (operational) interests

When determining the seriousness of the interference with the fundamental rights of persons whose data the AIVD has provided, the propriety safeguard has little meaning where the exchange of unevaluated data (in bulk) is concerned. It is not clear in advance exactly whose personal data is provided, making it difficult to chart the extent of the interference with fundamental rights. It is, however, possible to determine the extent of the interference in general terms on the basis of the quantity and the nature of the data. The other side of the balance, the importance of the data exchange for the international fight against jihadism, cannot be specified, either. This, too, can only be determined to a general extent. Overall, the seriousness of the interference is limited in the multilateral sigint cooperation concerned, while clear agreements on the use of the data and its provision to third parties exist.

Because the propriety assessment cannot be properly made at the level of the individual target, the requirement of authorisation by the Minister for the exchange of unevaluated data provides an important additional safeguard. The Minister must assess whether the risks associated with the exchange are acceptable, also in view of the importance of that exchange. This mainly concerns the risk that the AIVD does not exactly know which data it shares and, therefore, is unable to foresee the consequences of the use of that data by the foreign services concerned. The Minister assesses whether this risk is acceptable in the specific situation and must, in doing so, test the exchange against the applicable framework set by the weighting note. The CTIVD recommended that the authorisation

by the Minister for the exchange of unevaluated data be limited to a period of one year.[2] The Minister of the Interior adopted this recommendation by a letter to the House of Representatives of 30 June 2016.[3]

Authorisation for sigint cooperation in the field of the fight against jihadism was requested and granted in June 2014. After this, authorisation for the provision of unevaluated data was once again granted by the Minister on 6 December 2016, such in response to a substantiated request. The AIVD stated that the Minister had been kept properly and fully informed of the cooperation in the intervening period. In June 2016, the Minister authorised signing the MoU, which according to the AIVD, implicitly also meant that the Minister authorised the exchange of the unevaluated data.

The CTIVD only partially agrees with this argument. The authorisation granted did not specifically relate to the provision of unevaluated data for the purposes of counter-terrorism investigations. In view of the importance of the safeguard of ministerial authorisation and the Minister's undertaking in this connection, ministerial authorisation for the provision of unevaluated data should also have been granted between 30 June 2016 and 6 December 2016.

4.3 Due care of data exchange within sigint cooperation

The principle of due care is sufficiently adhered to in the exchange of unevaluated data. The origin of this data and its destruction are sufficiently safeguarded. In addition, the principle that data is provided in writing applies.

With respect to one specific form of exchange of *evaluated* data, no adequate safeguards are in place which ensure that the data is reproduced accurately, is sufficiently substantiated and is up to date. However, a final destruction term of the data has been agreed upon. In practice, the origin of this data is insufficiently clear.

Correct reproduction

The principle of due care plays a more limited role in the context of the provision of unevaluated data. This concerns raw data that has not been processed further. The data is provided shortly after the AIVD has collected it. This process is almost completely automated. In view of the amount of data and the unevaluated nature of it, no check of whether each piece of personal data is reproduced correctly is possible.

Accuracy

Joint agreements have been made on monitoring and oversight of the careful processing of data within the framework of sigint cooperation. The CTIVD deems the existence of these agreements to be of vital importance for the due care assessment. However, technical reasons currently bar the performance of effective oversight in practice. Expectations are that this will become possible in 2018.

Written provision

Multilateral agreements ensure that personal data is provided in writing.

---

[2] Refer in this connection to CTIVD report no. 49 on the exchange of unevaluated data by the AIVD and the MIVD, *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix), also available on www.ctivd.nl.

[3] *Parliamentary Documents II* 2015/16, 29 924, no. 142.

Destruction of data

Within the context of sigint cooperation the retention period of the provided data has been multilaterally agreed upon and laid down. This period is within the limits set by the ISS Act 2002 (and the new ISS Act 2017) for this purpose.

The CTIVD is still not able to properly verify whether the data provided by the AIVD has in fact been destroyed after the agreed-upon period. The CTIVD discusses this in Chapter 8.

4.4 Reliability of data exchange within sigint cooperation

Indication of reliability

With respect to the exchange and analysis of data within sigint cooperation, the reliability of the exchanged data is established where it concerns a technical source of that data.

This does not apply to data derived from another source. Pursuant to Article 12(4) of the ISS Act 2002, processed data must be provided with an indication of reliability or a reference to the source from which the data is derived. In practice this is not the case. The AIVD does not meet this requirement, which, incidentally, is also included in the new ISS Act 2017.

Reliability of the system

The CTIVD has no indications that the multilateral data processing systems are insufficiently reliable.

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl