Review report

The multilateral exchange of data on (alleged) jihadists by the AIVD

CTIVD no. 56

[adopted on 7 February 2018]

Review Committee on the Intelligence and Security Services

Review Committee
on the Intelligence and
Security Services

CTIVD no. 56

REVIEW REPORT

The multilateral exchange of data on (alleged) jihadists by the AIVD

Content

CTIVD no. 56

SUMMARY

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

The threat emanating from violent jihadism is a complex and diffuse one Terrorist attacks like those committed in Brussels, Paris and London are prepared and performed within terrorist organisations, cross-border networks, small cells and, sometimes, by lone wolves. Recognising, and then removing, the threat they pose is not a simple task.

The Netherlands has elected to adopt a comprehensive approach to fighting jihadism. The General Intelligence and Security Service (AIVD) plays an important part in this approach. On the international level, a very broad range of cooperation initiatives exists, both within and outside of Europe. The multilateral cooperation with foreign services is essential to obtaining insight into the threat posed by violent jihadism to national and international security. The AIVD often plays a leading role in such cooperation and maintains intensive and far-reaching cooperative relations with the intelligence and security services of other countries in this connection.

The Review Committee on the Intelligence and Security Services (CTIVD) performed an in-depth investigation into the exchange of personal data on (alleged) jihadists by the AIVD within the Counter-Terrorism Group (CTG) and within the framework of cooperation in the field of *signals intelligence* (sigint). Sigint cooperation concerns the exchange of data generated through all sorts of telecommunications. The Military Intelligence and Security Service (MIVD) is also involved in this Sigint cooperation. The investigation examines the exchange of personal data from the beginning of 2015 to mid-2017. This is the first in a two-part study. the second part will look at data exchange on (alleged) jihadists in a national context. This second report will be published in the spring of 2018.

Multilateral data exchange on (alleged) jihadists takes place with services both within and outside of Europe and is conducted in various ways. The CTIVD notes a clear development towards faster and more effective exchange of data. New ways of (automated) data exchange and of physically bringing the cooperating partners together have and are being sought, for instance by way of the recently set up database and the so-called operational platform of the CTG. The multilateral cooperation between the AIVD and intelligence and security services of other countries has strongly intensified over the past few years.

Against this backdrop, the CTIVD has examined the legal basis for certain forms of cooperation and the way the multilateral cooperation as a whole has been organised and functions. The investigation examined the extent to which the system of the multilateral exchange of data contains adequate safeguards for the protection of the individual, having regard to the level of protection provided by our Constitution, the European Convention on Human Rights (ECHR) and, in particular, the ISS Act 2002 (and ISS Act 2017). Additionally, it investigated the extent to which the AIVD's internal policy provides adequate safeguards. The CTIVD assessed this on the basis of the legal requirements of necessity, due care, propriety and reliability in force for the processing of personal data. These requirements continue to apply in full under the new ISS Act 2017. The CTIVD performed random checks of its application in practice.

In a sense, the results of this investigation provide a picture of the current state of cooperation. This concerns a snapshot, showing where, at this point in time, adequate safeguards for the legal protection of the individual are in place and where they are not, and what the possible risks are. In this way, the CTIVD has aimed, in its investigation plan, its findings, its conclusions and its recommendation, to do justice to the developments that the multilateral cooperation is currently undergoing.

The CTIVD finds that, as of yet, insufficient safeguards for the protection of the individual in the context of the exchange and further processing of data within the framework of the investigated multilateral cooperation exist. For the exchange of data by the AIVD to be lawful, it is important that the current situation is not allowed to continue and that the degree of legal protection is improved.

The CTIVD is of the opinion that, where the multilateral cooperation of the AIVD with foreign services lead to the joint retention and processing of personal data or the joint exercise of (investigatory) powers, a *joint responsibility* exists. Each of the cooperating services is responsible for the whole i.e. for the consequences of potential unlawful actions. It is necessary in this connection that the cooperating services decide together which concrete *multilateral* safeguards they will *jointly* establish for the protection of the rights of the individual. The general data protection principles are leading here. The CTIVD finds that the multilateral safeguards within the CTG have only been implemented to a limited extent. In the context of sigint cooperation there is a higher degree of data protection.

The CTIVD assessed the exchange of data by the AIVD against the ISS Act 2002 and the ISS Act 2017. It is of the opinion that the current practice of this data exchange is largely within the limitations set by the legal requirements. There are two counts of structural unlawful conduct: the failure to perform a risk assessment on the basis of the (legal) criteria applicable to the cooperation with foreign services and the failure to provide an indication of the reliability of the data provided by the AIVD. On one count there is incidental unlawful conduct: for a five-month period there was no authorisation by the Minister of the Interior (and the Minister of Defence) to provide unevaluated data in the context of sigint cooperation. Except for these instances of unlawful conduct, the CTIVD has not come across any personal data provided by the AIVD in a multilateral context that did not meet the requirements of necessity, propriety and due care.

Because of the threat emanating from jihadism and its cross-border nature, it is necessary for the AIVD to cooperate with the intelligence and security services of other countries. However, the CTIVD has identified certain risk areas where insufficient safeguards exist for the protection of the individual. One example is the risk of the cooperating services constantly lowering the threshold for the exchange of data, which may compromise the protection of the fundamental rights of citizens. Another risk is the development of a growing database, in which it is not sufficiently clear how to assess the correctness and reliability of the data it contains. Another conceivable risk concerns the increasingly frequent exchange of personal data orally. These and other risks have not yet or very rarely manifested themselves in practice. Nonetheless it is of vital importance that these risks are already taken into account, as they may in the near future result in unlawful conduct on the part of the AIVD in its multilateral cooperation with foreign services. The CTIVD makes recommendations aimed at creating additional safeguards in order to prevent unlawful conduct from occurring. With this, the CTIVD aims to ensure a more stringent protection regime and to allow for effective oversight.

In 2015, the CTIVD initiated a joint project on mutually agreed oversight of multilateral cooperation in the fight against violent jihadism. In collaboration with the oversight bodies of Belgium, Denmark, Norway and Switzerland investigation methods are compared, legal questions are interpreted and unclassified findings are collated. The aim of this joint project is to take the first steps in bridging the boundaries of national oversight. These oversight bodies aim to prepare a joint public report in early 2018.

CTIVD no. 56

REVIEW REPORT

**The multilateral exchange of data
on (alleged) jihadists by the AIVD**

1 Introduction

Background to the investigation

The threat emanating from violent jihadism is a complex and diffuse one. Not only those persons who left for the conflict areas in Syria and Iraq and returned constitute a threat to the Netherlands: but also sympathisers who remain in the Netherlands. The timely identification, and subsequent removal, of the threat they pose is not a simple task.

The Netherlands has elected to adopt a comprehensive approach to fighting jihadism. In 2014, the 'Integral Approach to Jihadism' action programme was set up for this purpose. The organisations that are involved in this action programme contribute to protecting the democratic state under the rule of law, combating and weakening the jihadist movement in the Netherlands and removing the breeding ground for radicalisation. The General Intelligence and Security Service (AIVD) is one of the organisations involved in the performance of the Action programme and forms an important link in the chain.

On the international level, a very broad range of cooperation initiatives exists. Within the United Nations and the European Union different bodies are looking to organise joint strategies against violent jihadism. The cooperation between intelligence and security services is a continuation of these strategies, but one that is separate from these institutions. The AIVD maintains intensive cooperative relations with the intelligence and security services of other countries in this connection. The exchange of data on (alleged) jihadists takes place with foreign services both within and outside of Europe.

Context of the investigation

The CTIVD announced its investigation into the exchange of data on (alleged) jihadists by the AIVD on 10 March 2016. The investigation is aimed at data exchange from 2015 onward in international context and data provision by the AIVD from 2016 onward in national context. The investigation involves two stages. Each stage will at any rate result in a publicly available review report.

The first stage of the investigation initially focused on all international exchanges by the AIVD of data on persons who (allegedly) travelled to and returned from the Syria/Iraq area. After some initial investigation, the CTIVD further narrowed it down, deciding to exclusively focus on the multilateral exchange of data by the AIVD (between the AIVD and foreign services in the context of the cooperation within a group). This first review report therefore addresses the exchange of data by the AIVD within a number of multilateral cooperative partnerships. This form of cooperation underwent some significant developments in the past few years. The multilateral sigint cooperation also involves the Military Intelligence and Security Service (MIVD).

The second stage of the investigation was started on 1 February 2017. That part of the investigation addresses the provision of data in the national context. Official messages provided by the AIVD to the Public Prosecution Service, the Immigration and Naturalisation Service (IND) and mayors, among others, are examined in this stage. The related report will be published in the spring of 2018.

Scope of the investigation

The multilateral cooperation between the AIVD and foreign services in the field of counter-terrorism is intensive and far-reaching. There is a high level of trust in the foreign services cooperated with. The services are increasingly open about their level of knowledge, the *modus operandi* (working methods) used and, sometimes, even about the instruments or sources used to obtain information.

The exchange of data on (alleged) jihadists realised in this connection takes place in various ways. Over the investigation period, from early 2015 onwards, a clear development towards faster and more effective sharing of personal data is visible. New ways of (automated) data exchange and of physically bringing the cooperating partners together have and are being sought. Examples include the setting up of a database and an operational platform within the Counter Terrorism Group (CTG), a European cooperative partnership of security services. In these developments the AIVD played an important pioneering role.

While these are promising developments in the international fight against violent jihadism, new forms of cooperation also give rise to consequences, whose lawfulness must be assessed legally.

Investigation plan

The CTIVD has observed that the developments in multilateral cooperation have swiftly progressed over the course of its investigation. The AIVD often adopted a pragmatic course of action in this connection, which has also led to a relatively quick intensification of the multilateral cooperation between intelligence and security services In its investigation, the CTIVD constantly posed the question of what the AIVD's responsibilities are in these ever-changing circumstances and whether they are adequately implemented on the basis of the ISS Act 2002.

Against this backdrop, the CTIVD opted for a broad, systemic approach in its lawfulness review. It reviewed the way multilateral cooperation as a whole is organized and its effectiveness. In this connection it investigated whether the system of the multilateral data exchange contains sufficient safeguards for the protection of the individual from the perspective of the Dutch Constitution, the European Convention on Human Rights (ECHR) and, in particular, the ISS Act 2002 (and ISS Act 2017). Additionally, it investigated the extent to which the AIVD's internal policy provides such safeguards. It also performed random checks of its implementation in practice.

In a sense, the results of this investigation provide an image of the current cooperation. This concerns a snapshot, showing where, at this point in time, sufficient safeguards for the protection of the individual are in place and where they are not, and what the possible risks are. In this way, the CTIVD has aimed, in its investigation plan, and in its findings, conclusions and recommendations, to do justice to the developments that the multilateral cooperation is currently undergoing.

Investigative questions

The following question was central to this investigation:

> *How has the multilateral exchange of data on (alleged) jihadists by the AIVD been organised and is this exchange of data lawful?*

This core question can be subdivided into the following sub-questions:

1. *What is the AIVD's role in the multilateral approach to international jihadism? Within which multilateral cooperative partnerships does the AIVD exchange personal data in the context of dealing with jihadists?*
2. *How is personal data exchanged? What (new) forms of cooperation are there?*
3. *What is the legal basis for the identified forms of data exchange?*
4. *Are there adequate safeguards for the protection of fundamental rights? How does the AIVD implement these safeguards in practice?*
5. *Are there any risks that need to be addressed?*

Structure of the report

In Chapter 2, the CTIVD presents an overall view of its findings. Chapter 3 provides an overview of the multilateral cooperative partnerships and forms of cooperation that have been investigated. Chapter 4 provides a short summary of the legal framework that applies to the AIVD's cooperation with foreign services and the exchange of personal data within that framework. Chapter 5 addresses the legal basis and political context of the cooperation and the forms of cooperation that have seen extensive development within that context. Chapter 6 looks at the safeguards for the protection of fundamental rights that apply to these forms of cooperation and the way the AIVD implements these safeguards. The CTIVD's conclusions are presented in Chapter 7. In Chapter 8, the CTIVD discusses the risks currently present or foreseeable for the near future and makes recommendations. In addition, the report contains four appendices, addressing the investigation methodology (I), the findings on the safeguards (II), the definitions of terms used (III) and an experts' report (IV).

A classified version of this report has also been prepared. The classified review report features more extensive and detailed versions of Chapters 3, 5, 6 and 8, and of Appendix II. The introduction, the overall view, the legal framework, the conclusions and Appendices I, III and IV are exactly the same in both reports.

Experts' report

On the basis of Article 76 of the ISS Act 2002, the CTIVD had an experts' report on the legal basis and division of responsibilities with respect to a specific form of cooperation prepared. The contents of the experts' report are discussed in more detail in section 5.5. The experts' report is included with this review report as Appendix IV.

Cooperation with other oversight bodies

In 2015, the CTIVD took the initiative to launch a joint project with the oversight bodies of Belgium, Denmark, Norway and Switzerland. All of these oversight bodies conduct an investigation into the exchange of data on (alleged) jihadists, each within their own national context and mandate. The aim of the project is to compare investigation methods, interpret legal questions and collate unclassified findings.

The joint project was started up with the aim to take the first steps to overcome the limits of national oversight, also referred to as the *accountability deficit*. Comparing findings and conclusions results in a more complete overview of the international cooperation between intelligence and security services. At the same time, it provides more insight into the limitations of the sum total of the various countries' national oversight. The project participants strive to publish a joint public report in 2018.

2 Overall view

The CTIVD's overall view is that the AIVD's multilateral cooperation with foreign services with regard to the fight against jihadism is far-reaching. This cooperation has become more intensive over the past few years. In addition, other, more effective forms of data exchange have been sought. The AIVD played a pioneering role in this, particularly during the Dutch presidency of the CTG in the first half of 2016 and the following period.

The CTIVD observes that within the context of broad multilateral cooperative frameworks with a large number of participating services, it is not easy to launch new initiatives and agree on the organisation of the cooperation. These processes involve a lot of debate and require time and patience. Nevertheless, the developments in this field have at times progressed very quickly. The AIVD actively works to realise this and in collaboration with other services has managed to come to a wide range of multilateral agreements.

It is not easy to find the proper balance between the sometimes contrary interests: on the one hand, there is the operational necessity and political desirability of exchanging as much relevant data as possible in the shortest possible time, and on the other, there is the interest of implementing the exchange of data in a durable and legally sound manner. The AIVD has always chosen a pragmatic course of action, focusing on what seemed to be feasible at any given moment.

Over the course of its investigation, the CTIVD observed that the developments in both fields have sped up and become more stable. The operational necessity to increase and improve the exchange of data as perceived after attacks such as those in Brussels, Paris and London, for instance, in particular serves as a catalyst for further intensification of cooperation. Such intensification is commonly followed by consolidation in the form of agreements or procedures, at which time the legal side of the exchange of data, too, receives more attention. These developments seem to follow a certain rhythm and should ultimately occur more or less simultaneously in the long term. For now, it is vital that the development phase the cooperation is in is followed by a consolidation phase to provide attention to establishing additional safeguards for the protection of the individual.

Even though the CTIVD observes that a lot is going on and much work is being done, it is critical. For instance, about the lack of so-called weighting notes and, consequently, about the lack of formal legal basis for the AIVD's multilateral cooperative relations. It is also critical about the legal basis for certain forms of cooperation and the responsibilities ensuing from these for the AIVD and its cooperative partners. The intensification of the cooperation is of such an order of magnitude that it may result in the development of forms of cooperation that potentially have far-reaching consequences for the individual, without this being counterbalanced by sufficient protection of fundamental rights and effective legal means of redress. It is vital to pre-empt this situation by establishing adequate safeguards in a timely fashion.

Such adequate safeguards must at any rate also be implemented at the multilateral level wherever personal data is jointly stored and processed or (investigative) powers are jointly deployed. The laying down of joint responsibilities is essential in this connection. Wherever the cooperation lacks safeguards, or wherever they are not laid down or are not strong enough, the protection of the fundamental rights of the citizen is at risk. Should such risks materialise, they may also result in unlawful conduct by the AIVD. The CTIVD has identified such risks in a number of fields (see Chapter 8).

3 Cooperative partnerships and forms of cooperation

3.1 Cooperative partnerships investigated

The CTIVD investigated cooperative partnerships in which there is multilateral exchange of personal data. Among others, this concerns the CTG, a cooperative framework of the 30 security services of the EU countries, Norway and Switzerland. The CTG was founded by the heads of a number of European security services in the wake of the 11 September 2001 attacks in the United States. The AIVD also cooperates multilaterally in the field of sigint. Sigint cooperation is partly aimed at combating terrorism. The MIVD also participates in this cooperation. The various cooperative partnerships have been founded on the initiative of the (like-minded) intelligence and security services involved and are not part of the EU, the UN or of any other international or supranational organisations.

Evaluated data on (alleged) jihadists is shared multilaterally both within the CTG and in the context of the sigint cooperation. Evaluated data is data which has been assessed for relevance to the intelligence process. This mainly concerns personal data.

In the framework of the sigint cooperation, also *unevaluated* data is exchanged multilaterally in significant amounts (bulk). In the context of the fight against jihadism, this so far concerns the exchange of communications metadata originating in or destined for a certain area. Another notable aspect of sigint cooperation is that joint intelligence products are created. These intelligence products do not derive from one of the participating services, but from the cooperating services as a whole.

The various cooperative partnerships do not directly collaborate. Some indirect connections between the cooperative partnerships do exist, however.

The multilateral cooperation investigated results in different forms of cooperation and data streams. The classified review report charts these in more detail. This public review report only allows for short descriptions of some of the forms of cooperation within the CTG.

3.2 Forms of cooperation within the CTG

The objective of the CTG is the intensification of the cooperation and the exchange of information in the field of counter-terrorism between the security services of the participating countries. The creation of a more or less independent setting, operating outside the EU system, was opted for.[1] The rationale behind this decision is that this allows the CTG to operate as an independent forum at the level of service heads and counter-terrorism directors and to facilitate the cooperation between the security services.

Europol, the United States security services, the EU Intelligence and Situation Centre (INTCEN) and the EU Counter-Terrorism Coordinator all have a sort of "observer" status at the CTG. This means that they are generally invited to be present during CTG (strategic) meetings. This does not apply to operational meetings. The CTG cooperative partnership does not provide personal data to these third parties. The CTIVD did not investigate this "observer" status further.

---

[1] The government recently indicated that the cooperation within the CTG takes place in conformity with Article 4.2 of the EU Charter and Article 73 of the TFEU; see also the Answers to the Parliamentary Questions posed by MP Verhoeven, *Appendix to the Proceedings II* 20172017/18, no. 202. This likely refers to Article 4(2) of the Treaty on European Union, which provides that national security remains the exclusive responsibility of each Member State.

The presidency of the CTG rotates in tandem with that of the EU. A significant intensification of the cooperation within the CTG in the field of tackling jihadism took place during the Dutch presidency in the first half of 2016. Data, including personal data, on (alleged) jihadists is exchanged in various ways and by various forums within the CTG. In this report the CTIVD limits its observations to the exchange of data via a database and within an operational platform.

CTG database

Starting in 2001, the services that participate in the CTG have been exchanging (personal) data on persons who travelled to and returned from certain conflict areas. A database was set up to facilitate the multilateral exchange of data. This database became active on 1 July 2017 and is (near) real-time available to all thirty services participating in the CTG. This means that whenever one participating service adds data to the database, it becomes (almost) immediately accessible by the other participating services. The database was and is used to store (personal) data on (alleged) jihadists. It runs on a server located in Dutch territory.

Operational platform

Also in 2016, important steps were taken for the creation of an operational platform, which was formally launched in January 2017. It allows for more detailed multilateral operational consultations, because the representatives of the participating services physically come together. The operational platform is accessible by all thirty CTG services. So-called "plots" are discussed during platform meetings: specific, relatively well-defined cases suitable for multilateral operational discussion. No investigatory powers are jointly deployed within the framework of the operational platform. The operational platform is also located in Dutch territory.

3.3 Forms of cooperation within sigint cooperation

The forms of cooperation within sigint cooperation are discussed in further detail in the classified review report.

3.4 Other cooperative partnerships

The AIVD is a participant in a number of other multilateral cooperative partnerships that directly or indirectly contribute to the international fight against jihadism. This concerns technical or analytical cooperation or cooperation within very small groups. The CTIVD has opted not to perform a further, in-depth investigation into all cooperative partnerships, either because the focus of such partnerships is not on the *multilateral* exchange of data or because *personal* data is exchanged to a limited extent only.

Also relevant in this context is that there is a multilateral cooperative partnership in the area of the jihadist Internet. This cooperative partnership was founded in 2007 to jointly tackle the threat of terrorism and the related (technical) developments on the Internet. Within this cooperative partnership, data is exchanged, *inter alia*, during annual meetings. These meetings focus on discussing operational experience, analyses and technological developments and do not, or only hardly, feature the exchange of *personal* data on alleged jihadists. For this reason, this cooperative partnership is not further discussed in this review report.

In addition, the participating services share unevaluated data, such as web fora, bilaterally. This does concern personal data. However, this does not concern the *multilateral* exchange of data.[2]

[2] The CTIVD has also assessed the exchange of web forums in Review Reports nos 39 (AIVD investigations on social media) and 49 (exchange of unevaluated data). These reports are both available in English on www.ctivd.nl.

4 ISS Act 2002 assessment framework

The CTIVD has detailed the assessment framework applicable to the conduct of the AIVD when cooperating with foreign services in previous review reports. There is no need to comprehensively reproduce the assessment framework once more in this report.[3] In short, the AIVD must make the following assessments when exchanging personal data, both under the current and under the new legislation:

1. Is a foreign service eligible for cooperation, based on the assessment of the risks that might apply to that cooperation?

The AIVD is allowed to cooperate with foreign services when these services are eligible for cooperation. This eligibility is determined on the basis of a risk assessment, in which the AIVD must identify the risks associated with the cooperation and define the circumstances under which these risks are acceptable.

This assessment must be laid down in a so-called weighting note. The degree to which the foreign service meets certain cooperation criteria, such as respect for human rights, democratic embedding and professionalism and reliability, must be included in the assessment. The results of the assessment determine the extent of the cooperation and the applicable limits.[4] The weighting note must be approved by the Minister of the Interior. The ISS Act 2017 allows for mandating the head of the service for this.

Whenever the AIVD subsequently provides data to, or receives data from, a foreign service in a specific situation and it wishes to use the data, the service must make two further assessments:

2. Does the exchange of data with the foreign service remain within the limits laid down in the weighting note?

If not, this has to be counterbalanced. The AIVD must lay down in writing the compelling operational interests which justify the service's stepping outside the limitations placed on the cooperation. In addition, authorisation must be received from a higher level of authority than is usual for the exchange of data. For the exchange of personal data, the Minister's authorisation is required in such a case.[5]

3. Does the exchange of data meet the requirements of necessity, propriety, due care and (indication of) reliability provided by the ISS Act 2002?[6]

---

[3] The assessment framework for the cooperation and exchange of data with foreign services has been addressed in, *inter alia*, CTIVD reports nos 22a, 22b, 38, 48, 49 and 50. Moreover, in report no. 50 on contributions of the MIVD to targeting, the assessment framework has been included in section 3.1 in the form of a diagram. All reports are available in English on www.ctivd.nl, except for report no. 22b which is only available in Dutch.

[4] For a detailed discussion, refer to CTIVD report no. 48 on the implementation of cooperation criteria by the AIVD and the MIVD, *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix), also available in English on www.ctivd.nl.

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

[6] For a discussion of these requirements, see the legal appendix to report no. 22b on the cooperation of the MIVD with foreign services, *Parliamentary Documents II* 2014/15, 29 924, no. 128 (appendix) (not available in English) and the legal appendix to report no. 38 on the processing of telecommunications data by the AIVD and the MIVD, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix) (available in English), also available on www.ctivd.nl.

These are requirements that apply to both the contents and the form of the exchange of data. For instance, the exchange of data must be necessary for a previously established purpose, must not result in a disproportional disadvantage, must be substantiated by underlying information and must contain a reference to a source or an indication of reliability. Personal data must, in principle, be exchanged in writing. Appendix II to this review report provides further detail on these requirements within the framework of multilateral cooperation. These requirements are not altered by the ISS Act 2017.

In certain cases, the assessments referred to under 3 cannot be properly performed, such as when exchanging unevaluated data with a foreign service. Unevaluated data is (commonly, large amounts of) data that has not yet been assessed for relevance to the performance of the tasks by the AIVD. When exchanging unevaluated data, the exact contents of the data provided or received cannot be precisely determined in advance. For this reason, it is impossible to sufficiently assess the necessity and propriety of the exchange of data provided by the Act. These requirements can only be generally substantiated when exchanging unevaluated data.

An additional safeguard was put in place for such situations. A motion of the House of Representatives adopted in April 2014 requests the government to only exchange such data once the Minister concerned has granted authorisation. The government agreed to this.[7] The Minister does not only examine whether the assessment laid down in the weighting note is justified, but also assesses whether the exchange of unevaluated data takes place within the limits set in the weighting note (under 2) and, to the extent possible, whether the exchange of data is allowed in the specific case (under 3). In this way, the Minister makes the (political) assessment as to whether the risks associated with the exchange of unevaluated data are acceptable. For this reason it is of vital importance that a weighting note on the foreign service concerned has been drawn up.

[7] For a detailed discussion, see 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 in English on www.ctivd.nl.

5 Cooperation basis

5.1 Introduction

The multilateral cooperation discussed in Chapter 4 is intensive and far-reaching. The exchange of data on (alleged) jihadists performed in this connection takes place in a variety of forms. There is a clear development in the direction of the faster and more effective sharing of (personal) data is visible in this connection. New ways of data exchange and of physically bringing the cooperating partners together are and have been looked into.

The CTIVD raised the questions of what the legal basis is for the exchange of data by the AIVD within the multilateral cooperation concerned and whether this basis is sufficient for the forms of data exchange involved.

No international, public-law basis for the cooperation exists. The cooperation takes place outside the EU, the UN or any other international or supranational organisations and has not been laid down in formal, legal binding agreements, such as a treaty. The basis for the exchange of data by the AIVD should therefore be found within national legislation. Nevertheless, international law, *inter alia* in the fields of state liability and data protection, remains relevant. Where the cooperation between intelligence and security services is concerned, these areas of law are still in the process of development. With this in mind, the CTIVD instructed two experts on the aforementioned fields of law to draw up an experts' report on the legal basis and the division of responsibility of the CTG database (refer to Appendix IV).

In this Chapter, the CTIVD will first address the political and administrative context of the fight against jihadism, as this may be of relevance to the legal basis of the cooperation by the AIVD. This cannot be seen entirely in isolation. The CTIVD next discusses the legal basis for the cooperation with foreign services as laid down in the ISS Act 2002 (and in the ISS Act 2017). In addition to providing a general basis for cooperation, the ISS ACT 2002 specifically authorises the exchange of data and the provision of support to foreign services, as does the ISS Act 2017. Next, the CTIVD will discuss the multilateral agreements that can further define specific forms of data exchange.

Each of these topics is also addressed in the final section of this Chapter, which tests the multilateral exchange of data against its basis. The contents of the experts' report (see Appendix IV) are explicitly taken into consideration in this assessment.

5.2. Political and administrative context of international cooperation

National policy

By way of its 'Integral Approach to Jihadism' action programme[8], the Dutch government has opted for a broad approach against the jihadist threat in the Netherlands. This approach is based on five policy lines, including exchange of information and (international) cooperation. The international efforts by the Netherlands partly follow from this Action programme, and the Netherlands actively participates in various political-administrative international forums working to counter the threat emanating from violent jihadism. Even though the AIVD does not directly participate in any of them, the international

[8] *Parliamentary Documents II* 2013/14, 29 754, no. 253 (appendix).

cooperative partnerships and strategies the Netherlands has politically committed itself to do form the backdrop against which the AIVD operates. Each of these forums (see below) emphasises the necessity of an intensive exchange of data.

United Nations

Resolution 2178 (2014) of the UN Security Council[9] calls on Member States to implement (criminal-law) measures against the threat posed by *foreign terrorist fighters*. Such measures must, *inter alia*, serve to prevent or counter the recruitment, organisation, transportation and facilitation of persons who leave the country for reasons of carrying out violent jihad. The UN Member States are also called on to intensify and accelerate the (operational) exchange of data on *foreign terrorist fighters*. The resolution also provides a definition of the term *foreign terrorist fighter*. The Netherlands is obliged to comply with Resolution 2178 (2014). The implementation of Resolution 2178 is given concrete shape in, *inter alia*, the *Global Counter Terrorism Forum* (GCTF) and the Counter-ISIS Coalition.

Global Counter Terrorism Forum (GCTF)

The GCTF is an international forum comprised of 29 member countries and the EU.[10] The forum provides a setting for sharing knowledge and experience on, and developing means and strategies to combat, terrorism. The Netherlands and Morocco have been co-presidents of the GTCF since September 2015. The Netherlands also plays a leading role in the GCTF's *Foreign Terrorist Fighters* working group. The GTCF issues recommendations for the creation of policy or the implementation of national measures with respect to jihadists. The international exchange of information is considered a precondition for effective counter-terrorism.

Counter-ISIS Coalition

In October 2014, the Netherlands joined the Counter-ISIS Coalition which, *inter alia*, conducts airstrikes in Syria and Iraq in its battle against ISIS. By now, more than 70 countries have joined the Coalition. The Netherlands contribute both militarily and diplomatically to the Coalition.[11] In addition, the Netherlands, together with Turkey, served as co-president of the Foreign Terrorist Fighter working group. The core focus of this working group is on the exchange of information between international organisations, such as Interpol, and governments, on the cooperation with countries in the region, and on the integrated approach to people returning from the conflict areas.[12]

European Union

Within the EU context, the Netherlands is a member of the EU core group on jihadists, which is active in harmonising the national approaches to jihadists.[13] Central to this core group's action plan is the exchange of information on persons leaving for conflict areas at a European level. The measures taken relate to border control, information exchange and optimisation of border passage signalisations for persons leaving for and returning from conflict areas, *inter alia*, by using existing instruments like the Schengen Information System.[14]

---

9 S/RES/2178 (2014), 24 September 2014, under 3.

10 The GTCF was founded by: Algeria, Australia, Canada, China, Colombia, Denmark, Egypt, the EU, France, Germany, India, Indonesia, Italy, Japan, Jordan, Morocco, the Netherlands, New Zealand, Nigeria, Pakistan, Qatar, Russia, Saudi Arabia, South Africa, Spain, Switzerland, Turkey, the UAE, the UK, and the US; also refer to www.thegtcf.org.

11 *Parliamentary Papers II* 2016/17, 27 925, no. 607.

12 *Parliamentary Papers II* 2016/17, 27 925, no. 607.

13 The core group is comprised of the Netherlands, Belgium, France, Sweden, Denmark, Italy, Spain, the United Kingdom, Germany and Ireland.

14 Cover Letter to the Second Action Plan Progress Report, *Parliamentary Documents II* 2014/25, 29 754, no. 308.

Under the Dutch EU presidency the member states agreed at the meeting of the JHA Council on 10 June 2016 to the Roadmap to enhance information exchange and information management in the Justice and Home Affairs area.[15] This concerns law enforcement, counter-terrorism and border management. The Member States have committed themselves to the following agreements: 1) all relevant information is shared, unless there are compelling legal or operational reasons not to do so; 2) all work is performed on the basis of established principles, such as respecting fundamental rights and rules for the protection of data; and 3) the cooperation, quality and usefulness of systems are improved. At the same meeting, it was decided that the CTG can be a participant in the JHA Council whenever terrorism is an agenda item. The aim of this step is to promote the cooperation between the CTG and the EU bodies active in the field of counter-terrorism.[16]

EU policy and EU regulations are not directly the basis for the AIVD's activities. Pursuant to Article 4 of the Treaty on European Union, national security is outside of the scope of the EU. In addition, Article 73 of the Treaty on the Functioning of the European Union provides that the Member States are free to organise between themselves and under their responsibility cooperation and coordination between government services in the field of national security.

5.3. National legal basis for cooperation

The ISS Act 2002 does not provide an explicit legal basis for each form of cooperation. The Act provides that, prior to any cooperation with foreign services, an assessment must be made of whether the foreign service in question is eligible for cooperation. In addition, the ISS Act 2002 provides an explicit basis for the provision of data and for the granting of support.

Risk assessment

Pursuant to the ISS Act 2002, the head of the AIVD is responsible for the cooperation with the eligible foreign intelligence and security services (Article 59(1)). A risk assessment must be made to establish whether a foreign service is eligible for cooperation. The assessment determines the extent of the cooperation with a foreign service and which forms of cooperation are allowed. Subsequently, the consideration whether the risks identified in the cooperative relationship with the service concerned are acceptable is a political one. The assessment whether cooperation is lawful remains a legal consideration, however.

The assessment must take account of the extent to which a foreign service meets the cooperation criteria. These include cooperation criteria specifically relating to the foreign service concerned, such as respect for human rights, professionalism and the level of data protection in force. Criteria relating to the cooperation itself also exist, including the extent to which the cooperation serves the AIVD's performance of its tasks or its desirability in the context of international obligations. This last criterion concerns an assessment of whether the cooperation is desirable or undesirable given Dutch foreign policy and the obligations arising from the Dutch membership to international organisations, such as the United Nations.

The cooperation criteria arise from the legal history and the recommendations made by the CTIVD in its previous review reports that have been adopted by the Ministers involved. The assessment on the basis of these cooperation criteria is explicitly provided for in the new ISS Act 2017. Pursuant to a transitional provision (Article 166 of the ISS Act 2017), the implementation of this system, which already is in force under the current Act, is postponed by a period of two years for existing cooperative

[15] 9368/1/16 REV1.

[16] *Parliamentary Papers II* 2015/16, 27 925, no. 595.

relationships. As a consequence, the AIVD (and the MIVD) are, for the moment, formally not obliged to assess on the basis of the cooperation criteria whether a foreign service is eligible for cooperation and which forms of cooperation are allowed, in view of the identified risks.

By their letter of 15 December 2017[17], the Ministers of the Interior and Defence have committed themselves to having the weighting notes for the closest cooperation relationships of the AIVD (and the MIVD) drawn up by the time the ISS Act 2017 enters into force. These concern the foreign services participating in the CTG and the services intensively cooperated with in the sigint context.

Data provision

The ISS Act 2002 (and the ISS Act 2017) contain stipulations on the provision of data. Article 36 grants the AIVD the power to provide data to eligible foreign services within the context of the performance of its own tasks. The provision of data to promote the interests of the foreign service is also permitted (Article 59(2)). This may concern both evaluated and unevaluated data. These articles of law form the basis for each provision of data by the AIVD to a foreign service.

The Act does not contain any specific provision for the receipt and use of data from foreign services. The basis for these activities can be found in the power allowing cooperation (Article 59(1)). In addition, the processing of data received is generally subject to the same procedures as apply to data obtained by the AIVD independently. Moreover, the use of such data must meet the general requirements that apply to data processing (see also the assessment framework described in Chapter 3).

The manner in which data is exchanged is mostly unregulated. The Act provides some conditions for the way the data must be provided. The provision of data must be accompanied by the condition that the receiving party is not allowed to provide the data to third parties (Article 37).[18] Personal data must in principle be provided in writing (Article 40). The ISS Act 2002 (and the ISS Act 2017) does not place any further restrictions on the form in which data is exchanged.

Assistance

The ISS Act 2002 (and the ISS Act 2017) also provide a basis for the provision of assistance in the interest of a foreign service. Such provision of assistance may involve the use of investigatory powers. A written request from the foreign service concerned and prior authorisation by the Minister involved are required in such a case.

In the ISS Act 2017, there is also a provision which allows the AIVD (or the MIVD) to request assistance from a foreign service (Article 90). The requirements for such a request include that it may not relate to activities which are not in accordance with the Dutch services' powers as stipulated in the ISS Act 2017.

5.4. Multilateral agreements on forms of cooperation

Multilateral agreements between intelligence and security services can give further direction to specific forms of cooperation. The forms of multilateral cooperation investigated include agreements to which each party has committed itself, but which are not legally binding and cannot be enforced.

---

17 *Parliamentary Papers II*, 2017/18, 34588 no. 69.

18 In report no. 50 on contributions of the MIVD to targeting, the CTIVD recommended that, under certain circumstances, the condition that data may not be used for purposes that entail a violation of international law must also be attached (Chapter 6, recommendation 5), available in English on www.ctivd.nl. This recommendation was adopted by the Minister of Defence. On 19 May 2017, the head of the AIVD announced that the AIVD, too, will attach this condition under certain circumstances.

Within the CTG multilateral agreements have been concluded, detailing, for instance, the objective of the cooperation within the CTG, the organisation of the CTG and the decision-making structure. Agreements have also been concluded on membership, confidentiality and the provision of data to third parties. Procedures and working agreements have been laid down with respect to the database and the operational platform. These include the purpose of the database and the platform, the responsibilities of all related parties, how they are to be used and what their position in with regard to other instruments available in the fight against jihadism, such as national and international border control systems.

In the context of sigint cooperation, the decision was made to lay down agreements on specific forms of cooperation in a document signed by the Ministers of the Interior and Defence. While these multilateral agreements are of a somewhat more formal nature, they are still not legally enforceable. The agreements define the concrete cooperation. They also discuss the oversight over this cooperation by national oversight bodies.

Multilaterally concluded agreements are only valid to the extent national legislation allows for this. The CTIVD considers such documents to be the international equivalent of internal policy documents. The AIVD has committed to the multilateral agreements contained in these documents. They therefore form part of the regulatory framework the AIVD must adhere to. As applies to the AIVD's internal policy, oversight can examine the question whether the policy conforms to the ISS Act 2002 (and, in the near future, to the ISS Act 2017) and whether the policy is observed in practice by the AIVD.

The above does not alter the fact that multilateral agreements are essential to complying to national legislation and contribute to protecting the fundamental rights of the citizen.[19] For this reason, Chapter 6 addresses the way the AIVD implements the safeguards arising from multilateral agreements in further detail. The associated risks are addressed in Chapter 8, with a view to the protection of fundamental rights the ISS Act 2002 (and the ISS Act 2017) aims to provide.

5.5 Assessment of the basis for the multilateral exchange of data

5.5.1 Risk assessment per foreign service

The AIVD does *not* meet the requirement of assessing whether a foreign service is eligible for cooperation.[20] So far, no weighting notes have been drawn up with respect to the foreign services the AIVD cooperates with multilaterally. As a result, the legitimacy of the cooperative relationship of the AIVD with each of these foreign services is insufficiently guaranteed. After all, the assessment is a constituent factor in the cooperation. It is the basis for the AIVD to build the cooperative relationship on. It determines the bandwidth of the cooperation within which the AIVD can operate responsibly. Operating outside of this bandwidth is, in principle, too risky and permissible only in cases where considerable operational interests are at stake. Since 2009, the CTIVD has emphasised the importance of this in various review reports and recommended that sound weighting notes are drawn up for each foreign service. For without a proper assessment, the cooperation lacks a formal basis.

To the CTIVD, this raises the question of what this lack means for the lawfulness of the exchange of data on (alleged) jihadists by the AIVD within the CTG and the multilateral sigint cooperation investigated. Are the foreign services concerned actually *eligible* for these specific types of cooperation? In the case

---

[19] See also the experts' report in Appendix IV to this review report.

[20] CTIVD report no. 48 on the implementation of cooperation criteria by the AIVD and the MIVD, *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix), also available in English on www.ctivd.nl.

of data exchange in the fight against violent jihadism this is, however, quickly a given. In view of the compelling interest involved, which is widely subscribed to in both nationally and internationally, and in view of the international obligations the Netherlands is a part of in this context, it would not be realistic to state that these services are not eligible. The necessity of the joint fight against violent jihadism quickly outweighs the possible risks associated with multilateral cooperation.[21]

This does not alter the fact that it is nevertheless of great importance for the AIVD to show whether any risks exist in the context of the exchange of data with the foreign services cooperated with and, if so, what these risks are. Even in the context of counter-terrorism the AIVD must account for this. A risk assessment laid down in a weighting note is not likely to result in limiting the cooperation with the foreign services concerned in the field of fighting jihadism or in the reduction of data exchange. It will, however, force the AIVD to establish additional safeguards whenever risks exist or may manifest themselves in the future.

5.5.2 Legal basis for the CTG database

The CTG database established in 2016 and located in the Netherlands constitutes a new form of the multilateral exchange of data in which the AIVD is a contributor. The CTIVD has posed the question how this data exchange relates to the provisions of the ISS Act 2002 (and the ISS Act 2017).

A distinction can be made between, one the one hand, the data in the database and, on the other, the database system. A general principle underlying the cooperation between intelligence and security services is that the service providing the data is responsible for the lawfulness and quality of that data and that the national legislation of that service applies in this connection. The question remains, however, which party is responsible for the data *after* it has been provided and made available in the database. Also for the database system, the question exists as to which party is responsible and what legislation applies. It would seem obvious that the service that has developed and is maintaining the system, the AIVD, bears this responsibility. This raises the question whether this means that the ISS Act 2002 (and, in the future, the ISS Act 2017) applies in full to the database system.

The CTIVD has further examined the legal basis and division of responsibilities with respect to the database and finds as follows, also on the basis of the experts' report (Appendix IV).

Data in the database

The personal data registered in the database is in fact composed of exchanged personal data.

For each piece of data, the database shows which service it originates from, i.e., the service that has added the data to the database. The service that has provided the data is responsible for ensuring that it has been lawfully obtained. One could argue that this means that the methodology of exchanging personal data via the database hardly differs from the other means of exchanging data, such as the multilateral sending and receiving of messages containing personal data. It basically concerns the same (type of) data exchange and the same group of services to which the data is provided.

What makes this data exchange different, however, is firstly the fact that the personal data is stored in a database. The personal data is almost immediately available to all participating services after having been added and remains available in real-time to them. As such, it concerns personal data provided to all 30 participating services and which therefore belongs to all of them. The personal data

[21] This consideration may be quite different in the case of other areas of interest.

may have been entered by one of the participating services (the original "data owner"), but it has been exchanged with all of them.

A responsibility exists to treat the personal data added to the database with due care, for instance by ensuring that it is accurate and up to date. This applies not only at the moment the personal data is provided and entered into the database, but also afterwards, as the data continues to be available to all participating services in *real time*. This is another aspect in which the exchange of data via the database differs from the other, more traditional forms of data exchange.

Another difference is related to the dynamics of the use of the database. The multilateral exchange of data now takes place more quickly and easily than was previously the case. It also leads to all data on a person being available at one central location, making it easier to use the data in the service's (own) intelligence process and allowing for more direct accessibility of the data.

This dynamic may also have legal consequences. The pooling of data with respect to a person and the possible joint further analysis of this data results in greater interference with the right to privacy in the context of the cooperation than merely sharing the data does. In that case the interference, after all, partly takes place outside of the cooperation, in the national context, governed by national safeguards. Moreover, a database gathering data from multiple sources may become a "force multiplier": by pooling data, the interference can have a more significant effect. As the interference within the context of the multilateral cooperation is greater, adequate safeguards must be in place with respect to this cooperation.

Responsibility for the data in the database

The question presents itself which party is responsible for the data exchanged by way of the database and which party is responsible for data protection in this context. Which legal regime applies here? Who is responsible for oversight?

According to the experts' report (Appendix IV), international law does not preclude an informal cooperative partnership between intelligence and security services, in which data is exchanged. The partnership is informal, because it is based on agreements to which each party has committed itself, but which are not legally binding. The lack of a formal public-law framework, such as a treaty explicitly assigning the powers and responsibilities of the participating parties to, for instance, an international body, has a drawback. It means that the services participating in the CTG hold *joint responsibility* for the storage and processing of the personal data in the database.

The CTIVD is of the opinion that this joint responsibility requires clear agreements on the exchange, storage and processing of data and the powers and obligations of each participating party, including with respect to the data protection which must be jointly provided. It is crucial that each of the 30 participating services is fully aware what the responsibility they jointly bear entails. This joint responsibility may in fact lead to each of the participating services being held accountable in case of a violation of data protection rules (joint and several liability).

In this liability there is, however, an important role for the legally acknowledged principle of legitimate expectations. Unless sufficient concrete circumstances indicate otherwise, the cooperating services may trust that each of them keeps to the legislation and international obligations applicable to it.[22] This not only applies to the way the personal data is entered into the database, but also to the further processing of that data. The cooperating services may expect each other to comply with common standards, also in the area of data protection. This principle of legitimate expectations therefore

[22] See in this connection the judgement of the The Hague Court of Appeal in Citizens v. Plasterk, ECLI:NL:GHDHA:2017:535.

may mitigate the liability each service has in a case where an individual's rights are infringed by a cooperation partner. Joint and several liability can only apply if there are clear indications that the principle of legitimate expectations has been violated. To be able to invoke the principle of legitimate expectations, it is however necessary that these common standards have been explicitly defined within the cooperative partnership.

The experts' report (Appendix IV) states that the common data protection standards can 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. As a rule, the general data protection principles have been transposed into national legislation regulating the activities of the intelligence and security services. 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 means, among other things, that the processing of data is 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 of importance. In addition, safeguards with respect to independent, adequate and effective oversight are laid down. The experts' report states that oversight is a fundamental component of the required data protection.

It is necessary that the aforementioned data protection principles receive concrete implementation in the CTG cooperation. For what purpose is the data entered in the CTG database and under what circumstances do the services jointly consider this necessary? What level of threat must a person's actions pose to be proportional to the interference with that person's right to privacy? What interpretation is given to the terms adequate, relevant, accurate and up to date in this connection? As mentioned before, the "force multiplier" effect is also important. By pooling data from different services and, possibly, jointly analysing it, there may be a greater interference with the privacy of the persons whose data is concerned than would have been the case if the data was to be examined independently, in the national context. This dynamic process requires additional safeguards.

It is, therefore, of importance that the services participating in the CTG jointly determine how adequate legal protection is to be provided and what safeguards, derived from the general data protection principles, must be in place. The level of data protection provided in this connection must be at least equivalent to the level of protection provided by the ECHR, including the possibilities for independent, adequate and effective oversight. If this is absent or inadequate, risks of future unlawful conduct may arise (refer in this connection to section 8).

Responsibility for the database system

The database system was built by the AIVD in consultation with a number of other CTG participants. The server the data is stored on is located in the Netherlands. Again, there is a question of which party is responsible, not for the exchange of data in itself, but for the quality of the system enabling such exchange. "Quality" in this connection refers to the proper functioning of the system and the protection of data that must be embedded in it. Is this a joint responsibility of the CTG participants, or the responsibility of the AIVD alone? Which legal regime applies here? Who is responsible for the oversight?

The answer to these questions is, according to the expert report, identical to the one described above. As no formal, legally binding agreements explicitly allocating responsibilities exist, all participating parties bear joint responsibility. This means that the CTG participants are, in principle, jointly responsible for the quality of the system. This requires that the interpretation of this term by the participating services is clearly laid down, and the implementation of data protection in this context.

To the extent the responsibility for the quality of the database has informally been assigned to the AIVD by the CTG participants, this concerns a derived responsibility only. The cooperating services (including the AIVD) continue to bear joint responsibility; the AIVD can only be charged with the execution. Under data protection law, such a party is also referred to as a "processor": a party who, on behalf of the controllers (the 30 cooperating services) performs certain data processing activities. It is important in this connection that there are a clear instructions or a common framework on the basis of which the processor (the AIVD) can carry out its derived responsibility for the quality of the system. In the absence of such instructions or framework, the AIVD will initially have to fill in this responsibility itself. This means that the AIVD must ensure that the system works properly and that there are sufficient safeguards for data protection embedded in the system. If it is to be avoided that the AIVD implements there unilaterally, then it is necessary that the cooperating services provide a common framework for system quality.

In addition, the AIVD plays a special part, due to its actual control and influence over the database. As the database administrator, the AIVD is more directly involved than any other service. This implies that the AIVD may be held accountable for negligence with respect to safeguarding the general data protection principles sooner than a party that is not an administrator. The AIVD therefore has a duty of due care: a best-efforts obligation to ensure the protection of personal data and to prevent infringements. This not only means that the system's architecture must provide adequate legal safeguards (see above), but also that the AIVD must monitor their functioning in practice.

Implications for the AIVD

The joint responsibility of all CTG participants creates the necessity to provide a jointly defined data protection framework. In other words, it is of the essence that the participating services jointly determine which concrete safeguards they put in place for the protection of the rights of the individual. The general data protection principles are leading in this connection. The AIVD carries this responsibility, just as the other 29 CTG participants. This means that the AIVD must endeavour to realise an adequate level of data protection for the CTG database.

In the context of the AIVD's responsibility as an administrator and the associated duty of care, the AIVD must itself provide sufficient legal safeguards. This means that the framework provided by national law must be considered first.

Chapters 6 and 8 and Appendix II specify the data protection safeguards arising from the ISS Act 2002 (and, in the future, the ISS Act 2017) and the way these can be translated into multilateral agreements, internal policy and the measures to be implemented with respect to the quality of the system.

Implications for the oversight of the database

Bearing joint responsibility also requires joint, multilateral oversight. After all, the different national oversight bodies will each face the question whether the service they are overseeing gives sufficient implementation to the joint responsibility that the service bears. National oversight alone is insufficient in this case. The government recently agreed that there must be multilateral oversight.[23] Right now, there is no such multilateral oversight within the CTG.

To an extensive degree, the oversight body will assess the exchange of data and its further processing on the basis of its own mandate and within its own national legal framework. This does not alter the fact that there is a joint aspect here that requires further embedding. For this reason, it is necessary that the safeguard of independent, adequate and effective *joint* oversight is included in a common data protection framework for the CTG database.

---

[23] Answers to the Parliamentary Questions posed by MP Verhoeven, *Appendix to the Proceedings II* 2017/18, no. 202.

There are various ways to organise such joint oversight. For instance, there could be a limited cooperation between the oversight bodies, based on each body performing its own national oversight task pursuant to its own national mandate. The CTIVD points out that, in this regard, there already is cooperation between five oversight bodies in a joint project on data exchange concerning (alleged) jihadists. A limitation of this cooperation is that the oversight bodies are all under the legal obligation of secrecy, which prohibits them from mutually discussing matters classified as state secrets. This results, for instance, in the national oversight bodies being unable to discuss the contents of the multilateral agreements concluded within the CTG and applicable to all of the services. A more far-reaching form of cooperation between the oversight bodies would therefore be necessary, so that such limitations may be put aside. This would need to be embedded in a common data protection framework.

Another option would be to explicitly divide the oversight tasks, with one or a few oversight bodies being charged with organising the joint oversight. A parallel can be drawn with the relation between the "controller" and the "processor" under data protection law. One or more oversight bodies could be assigned the responsibility to perform the oversight on behalf of all of them. Again a common framework or instruction would have to form the basis for this. The controllers retain the primary responsibility in this.

A third option would be to institute overarching, international oversight. To that end a new international oversight body would have to be created, to which certain oversight powers are assigned. This is the most far-reaching option and would require a public-law basis, such as a treaty between States. As the multilateral cooperation between the intelligence and security services is not based on formally binding agreements, but on informal ones, this method of organising joint oversight does not seem appropriate.

5.5.3 Legal basis for sigint cooperation

The multilateral sigint cooperation investigated entails both joint data processing and the joint use of (investigatory) powers.

Joint data processing

Where there is joint data processing within sigint cooperation, such as the storage of exchanged data, the same considerations as presented in above in relation to the CTG database apply. The joint data processing takes place under the joint responsibility of all participating services, as formally binding agreements are lacking. They must, together, provide an adequate level of data protection. The CTIVD finds that this is indeed the case to an important extent. In section 6.4 and Chapter 8, the CTIVD discusses in which areas these adequate safeguards are lacking and what risks this could present.

The joint processing of sigint data can be connected to the joint use of (investigatory) powers. The CTIVD applies an additional framework in this connection, as discussed below.

Joint use of powers

The CTIVD posed the question whether there is a legal basis for the use of certain powers under joint responsibility, resulting in joint (sigint) intelligence products.

As indicated in section 5.3, the ISS Act 2002 (and the ISS Act 2017) contains a general basis for cooperation of the AIVD with foreign services and specific provisions for the provision of (personal) data and of assistance. There are no specific regulations for the use of powers under joint responsibility.

The CTIVD is of the opinion that the AIVD (and the MIVD) is in principle allowed, on the basis of the general power to cooperate with foreign services, to seek a *division of effort* in its cooperation, i.e., to divide tasks and the deployment of personnel and resources. This may also entail that a certain power is executed jointly, under joint responsibility. The following conditions apply in such a case:

1. the AIVD must itself hold the power to be used;
2. the legislation applicable to such use (such as the ISS Act 2002) must be observed;
3. data the AIVD (or the MIVD) cannot obtain on the basis of its own powers may not systematically or knowingly be received from foreign services;[24] and
4. effective oversight must be possible.

These conditions ensure that the same level of legal protection is in place when cooperating with foreign services as exists in the national context.

At present, the involvement of the AIVD in multilateral sigint cooperation meets the first three conditions. The CTIVD does not observe any conduct inconsistent with the ISS Act 2002. To the contrary: the multilateral agreements concluded in this framework actually provide additional safeguards that the above-mentioned conditions are met. With respect to the second condition, the observance of national legislation, the CTIVD has identified a problem in relation to the new ISS Act 2017. The ISS Act 2017 provides a more stringent framework for investigation task-related interception and the further processing of the intercepted data than currently applies to untargeted interception pursuant to the ISS Act 2002. It discusses this subject in further detail in the classified review report.

With respect to the fourth condition, the possibility to perform effective oversight, agreements have been made in the context of multilateral sigint cooperation for certain forms of cooperation. As concerns the oversight performed by the CTIVD, these agreements entail that it can examine the use of powers by the AIVD and, to a limited extent, the use of data provided to the AIVD by other participating services. However, a restriction is imposed on the national oversight bodies in this context. This restriction is of such a nature that national oversight cannot be fully effective because of it. The CTIVD finds it necessary that there are provisions for joint oversight on the use of data. Various options to organise such oversight have been detailed in section 5.5.2. In addition, it is important that such oversight is made technically possible.

Furthermore, it is necessary that effective oversight of the destruction of data provided by the AIVD becomes possible. The multilateral agreements allow for this possibility, but it has not yet been realised.

[24] This component arises from the Citizens v. Plasterk judgment, ECLI:NL:GHDHA:2017:535.

6 Safeguards

6.1 Introduction

The CTIVD investigated to what extent the AIVD has implemented the legal safeguards for the protection of fundamental rights in the multilateral exchange of data on (alleged) jihadists. The ISS Act 2002 (and the ISS Act 2017) lists four requirements in this connection: necessity, propriety, due care and (indication) of reliability. Appendix II to this report details the meaning of each of these requirements in the context of the multilateral exchange of data. This is presented in a diagram in section 6.2, below.

This Chapter 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. In addition, the CTIVD, by way of random checks, assessed whether the AIVD observes these agreements in practice. The CTIVD's findings are summarised in sections 6.3 and 6.4. Appendix II provides a more detailed discussion of the CTIVD's findings. The CTIVD is not permitted to extensively discuss the contents of the multilateral agreements in this public report as they are classified state secret. They are further detailed in the classified review report.

On the basis of these findings, the CTIVD has drawn conclusions on the current practice. These conclusions are detailed in Chapter 7 of this review report. In areas where data protection safeguards are lacking or are (as yet) insufficiently embedded, there may be risks of future unlawful conduct. The CTIVD discusses this in Chapter 8 of this review report.

6.2 Safeguards for the multilateral exchange of data

Necessity	• Does a clear definition exist of the cases allowing for the exchange or analysis of data (threshold)?
Propriety	• Is the seriousness of the interference with fundamental rights proportional to the importance of the (operational) interests served? The seriousness of the interference is determined by: – the number of services data is provided to; – the use of the data provided; – the quantity and sensitivity of the data. The importance of the operational interests is determined by the priority level of the target.
Due care	• Is the processed personal data reproduced correctly, accurate (i.e., substantiated and up to date), provided in writing, still relevant? Is data destroyed when this is not or no longer the case? • Have the necessary measures been implemented to promote the accuracy and completeness of the data processed?
Reliability	• Is there an indication of the reliability? • Have the necessary technical and organisational measures been taken to ensure data protection?

6.3 Safeguards for data exchange by the AIVD within the CTG

Necessity

To safeguard the necessity of the data exchange, a clear definition of the cases allowing for this must exist. This definition must serve as a threshold for data exchange.

At the meetings of the operational platform, a necessity threshold is applied, because, so far for each case discussed, there has in advance been a clear delineation of the group of persons the operational exchange of data may relate to. The personal data provided by the AIVD falls within this delineation.

The AIVD itself determines with respect to which persons data is exchanged via the CTG database. The AIVD operated on the basic principle that the service would only provide the data of persons who had actually left for conflict areas or, if they were still in the country, were very high on the priority list. This guiding principle was abandoned in early 2017. The August 2017 policy states that the subjects should be "identified counter-terrorism targets". 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.

However, the CTIVD has not identified any specific cases where the exchange of data by the AIVD was not necessary. It has observed a shift in the "type" of targets whose personal data is shared by the AIVD via the database from early 2017 onward.

The CTIVD believes that, if the threshold for the exchange of data becomes lower, risks will come to exist. This is discussed in Chapter 8.

Propriety

The seriousness of the interference with the fundamental rights of the persons whose data is being provided may be considerable, in particular due to the number of services the data is provided to. Safeguards must be in place in this connection. It is important, for instance, that the use of the data provided and the further provision of the data to third parties is limited. Furthermore, additional safeguards may be put in place for the exchange of sensitive data or for data on certain categories of persons, such as minors.

The interference with fundamental rights is counterbalanced by the operational interest of the exchange of data. It is necessary to safeguard that each target added to the database has been assigned a sufficiently high level of operational interest. This is also referred to as prioritisation of the target.

The exchange of data by the AIVD can thus far be deemed to be proper. Data is used only for the purpose of the intelligence process and is provided to third parties under strict conditions only. The exchange of data by the AIVD is limited in terms of the amount and sensitivity of data per target. The AIVD has set up no additional safeguards for the provision of data on minors. The CTIVD believes it important that such safeguards are set in place. This is discussed further in Chapter 8.

The AIVD has adopted internal policy on the method of prioritising targets. The persons whose data has been provided by the AIVD have generally been assigned a high priority level, also in view of the threat they pose. Here the CTIVD notes a shift that has taken place in this connection from early 2017 onward.

Due care

To implement the requirement of due care in the context of data exchange, it is important that conditions apply for the correct reproduction and the substantiation of the data exchanged, for keeping it up to date and for its timely destruction.

Mechanisms have been implemented in the system of the database to promote the accuracy and completeness of the data exchange. There are no mechanisms in place for keeping the data up to date and for its timely destruction. The CTIVD sees various possibilities for the AIVD to reinforce existing safeguards or to set up additional safeguards. This is discussed further in Chapter 8.

The CTIVD has only identified a small number of cases where certain aspects of the exchange of data by the AIVD through the CTG database were negligent. These cases concerned a difference between the personal data as recorded in the national systems and in the CTG database. The personal data as present in the database was insufficiently complete or not yet brought up to date. This has been remedied in the meantime.

The data exchange which takes place at the meeting of the operational platform is recorded in writing. The CTIVD has identified certain risks with respect to the oral provision of personal data. This is discussed in Chapter 8.

Reliability

As concerns the reliability of the exchanged data, a certain minimum reliability level or an indication of reliability must exist.

The database offers the feature of marking uncertain data with a red tag. The AIVD has also implemented measures to protect against data loss, data corruption, or unauthorised data processing. The system ensures, *inter alia*, that only the contributing service can edit the data, with the exception of the database administrator. The CTIVD has no doubts as to reliability of the system. No further restrictions are in place for the access to the system and the possibility to add data.

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. 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.

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

Necessity

It is inherent to the exchange of unevaluated data that its necessity can only be established in general terms and outlines. It is impossible to provide a well-delineated definition of the jihadists whose data is provided when it is not clear in advance to which persons the data relates. The necessity thresholds that apply here cannot, therefore, be directly compared to the necessity thresholds applying to the exchange of evaluated data. Multilateral agreements within sigint cooperation provide substance to the necessity requirement.

Propriety

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.

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. It is, therefore, of crucial importance that such weighting notes exist. These are currently lacking.

The CTIVD has found that, between 30 June 2016 and 6 December 2016, there was no valid Ministerial authorisation for the provision of unevaluated data.

Due care

Multilateral agreements provide an implementation of the requirement of due care in the exchange of *unevaluated* data. The origin of this data and its destruction are regulated. In addition, the principle that data is provided in writing applies.

The multilateral agreements on monitoring and oversight of the careful processing of data within sigint cooperation are of crucial importance to this assessment. However, in practice effective oversight is not yet entirely possible because of technical and organisational reasons. It is expected that this will be possible in 2018.

With respect to one specific form of the exchange of *evaluated* data, there are insufficient safeguards in place to meet the requirement of due care. There are no adequate safeguards ensuring 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 the data is insufficiently clear.

Reliability

The AIVD fails to meet the legal requirement that data is provided with an indication of reliability or a reference to a source where the exchange of *evaluated* data is concerned.

7 Conclusions

Conclusions with respect to the legal basis

General cooperation basis

The ISS Act 2002 provides a basis for the cooperation by the AIVD in multilateral cooperative partnerships with foreign intelligence and security services. The ISS Act 2002 requires that the foreign services the AIVD cooperates with, must be eligible for such cooperation. This means that the AIVD must perform a risk assessment on the basis of cooperation criteria for each foreign service. On the basis of this risk assessment, it must determine the risks that exist, which forms of cooperation are allowed with the foreign services in which fields, and the intensity of the cooperation. This must be recorded in a weighting note. This is an operational, legal and political assessment, to be ultimately endorsed and accounted for by the Minister.

No weighting notes containing risk assessments have been drawn up for the services the AIVD cooperates with in the context of the multilateral partnerships investigated (within the CTG and in the field of sigint).

- First of all the lack of a risk assessment formally calls the legitimacy of the cooperation into question. Without a risk assessment, the basic condition for cooperation is not met. The CTIVD finds the lack of these assessments to be **unlawful**. However, the ISS Act 2017 contains a provision that delays the implementation of the weighting notes system for a period of two years with respect to existing cooperative relationships. The Ministers of the Interior and Defence have committed to having the weighting notes for these services drawn up by the time the ISS Act 2017 enters into force.

- Secondly, this leads to the question whether the foreign services concerned are substantively eligible for the specific forms of cooperation investigated by the CTIVD in the context of this investigation. The CTIVD finds that this is the case for the services concerned, given the compelling interest of the international fight against jihadism and the necessity of intensive cooperation in this connection. This view is also promoted politically and governmentally on the (inter)national level. It does, however, remain of constitutional importance that the AIVD maps out where the risks lie in the cooperation with each of the foreign services concerned. Even in the context of the international fight against jihadism, the AIVD must render account of this and where necessary establish additional safeguards for the protection of citizens' fundamental rights.

Specific forms of cooperation

The specific informal forms of cooperation studied during this investigation are aimed at intensifying the multilateral exchange of data on (alleged) jihadists. These forms of cooperation are not, as such, explicitly regulated under the ISS Act 2002 (nor under the ISS Act 2017). However, the law does not provide a mandatory rule on the way the cooperation and the exchange of data must take place and, thus, in principle provides room for these forms. The principles of international law also do not oppose the informal nature of these cooperative partnerships.

- The CTG database, launched in 2016, is an example of these new forms of exchange of data. The database is located in Dutch territory. The CTIVD posed the question of how the exchange and further processing of data in the database relates to the provisions of the ISS Act 2002 (and of the new ISS Act 2017). Also on the basis of the experts' report (Appendix IV), the CTIVD finds as follows.

- Data is stored and processed in the CTG database jointly. The cooperating security services bear *joint responsibility for this*. This joint responsibility relates to the data in the database, the management of the database and the data protection to be provided. This requires clear agreements on data exchange and of the setting up of common standards applicable to each participating party. The CTIVD finds that such has been provided to a limited extent only.

- These common standards can be derived from the general data protection principles. This, *inter alia*, concerns the principles that the processing of personal data is necessary for a certain legitimate objective, that it is proportional and takes place with due care. This final requirement means, *inter alia*, that the processing of data is 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. Also mentioned are safeguards with respect to independent, adequate and effective oversight.

- It is necessary that these principles of data protection receive concrete implementation within CTG cooperation. For what purpose is the data entered in the CTG database and under what circumstances do the services jointly consider this necessary? What level of threat must a person's actions pose to be proportional to the interference with that person's right to privacy? What interpretation is given to the terms adequate, relevant, accurate and up to date in this connection? The services participating in the CTG must, therefore, jointly determine how adequate legal protection is to be provided and what safeguards, derived from the general data protection principles, must be in place.

- The AIVD plays a special part, as the administrator of the database and is therefore, responsible for the quality of the system. It is important in this connection that there are clear instructions or a common framework on the basis of which the AIVD can carry out its derived responsibility for the administration of the database. In the absence of such instructions or framework, the AIVD will have to establish adequate legal safeguards itself. Due to its actual control and influence over the database, the AIVD is more directly involved with it than any other participating service is. The AIVD therefore has a duty of due care: a best-efforts obligation to ensure the protection of personal data and to prevent infringements.

- The specific nature of this cooperation, where there is a joint responsibility, requires *joint oversight*. This is currently not in place. There are multiple ways to organise such joint oversight. For instance, there could be a limited or more far-reaching cooperation between the oversight bodies, an explicit division of oversight tasks or overarching oversight. The safeguard of independent, adequate and effective joint oversight must also be included in a common CTG data protection framework .

The multilateral sigint cooperation investigated entails both joint data storage and processing and the joint use of (investigatory) powers.

- The joint data processing takes place under the joint responsibility of all participating services. They must, together, provide an adequate level of data protection. The CTIVD finds that this has been provided to an important extent.
- In addition, forms of cooperation take place which involve the joint use of (investigatory) powers. The CTIVD is of the opinion that the AIVD is in principle allowed, on the basis of the general power to cooperate with foreign services, to seek a division of effort in its cooperation, i.e., to divide tasks and the deployment of personnel and resources. This may also entail that a certain power is executed jointly, under joint responsibility. The following conditions apply in such a case:

1. the AIVD only uses the powers granted to the service by law;
2. the AIVD acts in conformity with Dutch legislation when participating;
3. data the AIVD cannot obtain on the basis of its own powers may not systematically or knowingly be received; and
4. effective oversight must be possible.

- These conditions, which also apply in full to the MIVD, ensure that the same level of legal protection is in place when cooperating with foreign services as exists in the national context. The CTIVD finds that the AIVD meets the first three conditions. The oversight on the use of the data is, as yet, insufficiently effective, as the national oversight is limited and joint oversight has not yet been provided for. Moreover, the oversight is not effective because no access can be granted to the relevant data at the moment, due to technical reasons. This is supposed to become possible in 2018.

Conclusions with respect to current practice

The CTIVD investigated to what extent the legal safeguards for the protection of fundamental rights are implemented in the context of data exchange on (alleged) jihadists between the AIVD and the foreign services within the CTG and sigint cooperation. The ISS Act 2002 (and the ISS Act 2017) lists four requirements in this connection: necessity, propriety, due care and (indication) of reliability (see also Appendix II).

Necessity

Necessity, in concrete terms, means that the AIVD, when providing data 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; and 3) is able to substantiate this.

The fact that the assessment of the necessity is virtually the same for each piece of personal data exchanged is inherent to the exchange of personal data within an extensive multilateral partnership. The importance of the necessity requirement is that it forms a threshold for the multilateral exchange of data. This threshold is higher the more clearly it is described and laid down with respect to which persons or cases the exchange of data is deemed to be necessary. This threshold is lower the more general the description and when this is not laid down. In other words, the necessity of the multilateral exchange of data requires a clear definition of who or what it concerns.

In its internal policies, the AIVD provides that the data it adds to the CTG database should relate to "identified counter-terrorism targets". This definition is so general that it does not form a meaningful threshold. However, the AIVD does properly meet the necessity requirement in practice. In the database, the CTIVD has not come across any personal data provided by the AIVD which was not necessary. In addition, the AIVD keeps within the limits applied to each case in the operational platform of the CTG.

In the context of the sigint cooperation, a distinction between unevaluated and evaluated data applies. The threshold for the exchange of *unevaluated* data is sufficiently high, because multilateral agreements have provided a framework for the necessity requirement. Matters are different where a specific form of the exchange of evaluated data is concerned. In this case there is no clear definition of the persons whose data may be exchanged or the cases in which this may take place.

Propriety

Propriety means that the seriousness of the interference with someone's fundamental rights is reasonably proportionate to the importance of the (operational) interests the AIVD has in providing the data.

Propriety requires the existence of safeguards to limit the use of the data provided and the further provision to third parties and to restrict the provision of sensitive data or data on certain categories of persons, such as minors. It is also necessary to ensure that each target whose data is provided has been assigned a sufficiently high operational interest.

The CTIVD is of the opinion that the data exchange by the AIVD can as yet be deemed to be proper. The AIVD does not unreservedly permit the provision and use of data outside of the intelligence process. In terms of the quantity and the sensitivity of the data, the exchange of data by the AIVD is limited and it usually concerns targets assigned a high priority level.

The propriety requirement has less meaning in the context of the exchange of *unevaluated* data as part of multilateral sigint cooperation. With this type of data exchange, propriety can only be broadly assessed without it being possible to attach concrete weight to each side of the scales. Because of this, the additional safeguard that authorisation from the Minister is required for the exchange of unevaluated data is in place. The Minister assesses whether the risks associated with the data exchange are acceptable in the specific situation and must, in doing so, test the exchange against the applicable framework set by the weighting note. If weighting notes are lacking, as is currently the case, this test loses its meaning. Certain forms of cooperation require at least annual authorisation by both the Minister of the Interior and the Minister of Defence. This authorisation by both Ministers was lacking for a period of five months. The CTIVD finds this to be **unlawful**.

Due care

Due care is a quality requirement. It relates to the correct reproduction of the data and its accuracy, which, inter alia, means that the data must be substantiated and up to date. Personal data must in principle be provided in writing, except where there is call for urgency. The data processing processes should contain measures to promote the accuracy and completeness of the data.

In the context of the CTG database and the exchange of unevaluated data within the sigint cooperation, the system contains safeguards for the accurate reproduction of data and provides clarity on the origin of the data. The system also shows when the personal data has most recently been altered and by which service. As its administrator, the AIVD has a responsibility for the CTG database. The CTIVD finds that the AIVD has, in practice, sufficiently implemented this responsibility, but sees various possibilities for the AIVD to reinforce existing safeguards.

The due care provided by the AIVD when exchanging data is dependent on the standards the service itself maintains. It is up to the AIVD to ensure the quality of the contents of the data and to update and correct them. The AIVD's internal policy must ensure that its own national standard meets the requirement of due care. At the moment of writing this report, a working instruction on the exchange of data by the AIVD within the CTG is being drafted by the AIVD. The CTIVD has identified a small number of cases where certain aspects of the exchange of data by the AIVD through the CTG database were negligent. This has been remedied in the meantime.

With respect to one specific form of the exchange of *evaluated* data in the context of sigint cooperation, there are insufficient safeguards in place to meet the requirement of due care. There are no multilateral agreements ensuring that the data is reproduced accurately, is sufficiently substantiated and is up to date. In practice, the origin of the data is insufficiently clear.

In the context of sigint cooperation, the ultimate retention term of certain exchanged data exchanged has been laid down multilaterally. The retention term for exchanged unevaluated data is shorter than is required by the ISS Act 2002 (and the ISS Act 2017). This multilateral agreement therefore provides an additional due care safeguard. In addition, multilateral agreements have been concluded on monitoring and oversight of the careful processing of data within sigint cooperation. The CTIVD considers this to be an important safeguard. In practice effective oversight is not yet possible because of technical reasons.

Reliability

Reliability is also a quality requirement. It relates to the extent to which personal data is established and verified and to the extent this is recorded or indicated. Reliability also relates to the functioning of the data exchange processes and to data protection in that connection.

The ISS Act 2002 requires processed data to be provided with an indication of the degree of reliability or a reference to the source from which the information is derived. The data the AIVD provides does *not* contain such an indication or reference. This is **unlawful**. The CTIVD has no indications that the data provided by the AIVD is in fact insufficiently reliable.

With respect to the reliability of the data exchange systems, the law only provides that measures must be implemented to protect against data loss, data corruption, or unauthorised data processing. As the administrator, the AIVD bears responsibility for the CTG database. The CTIVD finds that the AIVD has sufficiently filled in this responsibility in practice.

Final conclusion

Given the compelling interest of the international fight against jihadism and the necessity of intensive cooperation in this connection, the CTIVD finds that the current practice of the AIVD is largely within the limitations set by the legal requirements. It has identified two counts of structural unlawful conduct: the failure to perform a risk assessment on the basis of the (legal) criteria applicable to the cooperation with foreign services and the failure to provide an indication of the reliability of the data provided by the AIVD. On one count there is incidental unlawful conduct: the lack of authorisation for a five-month period to provide unevaluated data.

Except for these instances of unlawful conduct, the CTIVD has not identified any evaluated or unevaluated data provided by the AIVD that failed to meet the requirements of necessity, propriety and due care. To the extent the AIVD is responsible for the careful and reliable organisation of data exchange systems, it has sufficiently implemented this responsibility. The multilateral exchange of data on (alleged) jihadists by the AIVD can thus far in practice be deemed to be **lawful**.

However, for a number of issues, the safeguards for the protection of the fundamental rights of the citizen have not been sufficiently anchored. Within the CTG there are few agreements which provide adequate legal protection to the individual. While this has been implemented in the context of the sigint cooperation, there are reasons to reinforce existing safeguards or set up additional safeguards. The social and technical developments in the field of the fight against jihadism are progressing rapidly. The CTIVD notes that risks exist in a number of areas that, should they become manifest, may result in unlawful conduct by the AIVD. In the next Chapter, the CTIVD addresses these risks and makes recommendations.

8 Risks and recommendations

8.1 Introduction

In this report, the CTIVD addresses how the legal requirements of necessity, propriety, due care and (the indication of) reliability are implemented in the multilateral exchange of data on (alleged) jihadists by the AIVD (Chapter 6 and Appendix II). In Chapter 7, it concludes that, also in view of the compelling interest of the international fight against jihadism and the necessity of intensive cooperation in this fight, the current practice remains largely within the limitations set by the above-mentioned requirements.

However, the social and technical developments in this field are progressing rapidly. In some areas, the safeguards for the protection of the fundamental rights of the citizen have not (yet) been sufficiently anchored. To prevent this dynamic from resulting in unlawful conduct, the risk-management approach currently used by many organisations has been applied. The CTIVD has identified risks that already exist but have no or only limited effect and risks that may occur in the (near) future. In this Chapter, it addresses these risks in more detail and makes recommendations for preventing their (further) manifestation.

The CTIVD discusses the risks it has identified from the perspective of the ISS Act 2002 (and the ISS Act 2017). For the multilateral data exchange by the AIVD to be lawful, it is necessary that when the AIVD participates in certain forms of cooperation, the level of legal protection in place is not lower than the level of legal protection provided by the ISS Act 2002 (and the ISS Act 2017). This does not mean that every specific requirement in the ISS Act 2002 (and the ISS Act 2017) must be addressed in multilateral agreements. It does mean that sufficient safeguards for the protection of the individual must exist when exchanging and processing data in the context of the multilateral cooperation investigated.

8.2 Risks with respect to the CTG database

There are many operational advantages to the CTG database, compared to other, more traditional modes of data exchange. The data is exchanged more quickly and more easily. A sizeable number of services can be reached in a short amount of time. The data has been brought together in a clear manner and is available in real time. The use of the data in the services' own intelligence process has become simpler and more direct. However, these and other operational advantages do carry certain risks or responsibilities. The most important of these are discussed below.

8.2.1 Risks with respect to the legal basis

- The cooperating security services are *jointly* responsible for the CTG database. This joint responsibility relates to the data in the database, the administration of the database and the data protection to be provided in this connection. This makes it necessary to establish clear multilateral agreements and common data protection standards.

Recommendation: The CTIVD recommends that the AIVD strive to give a concrete implementation to a common data protection framework for the CTG database and to draw up clear instructions on the administration of this database, on the basis of multilateral agreements.

8.2.2 Risks with respect to necessity

- It is vital that a sufficiently high threshold for recording data in the database exists. There is a risk that personal data is recorded in the database that does not belong in it. It must be sufficiently clear for each database user which criteria or circumstances allow for adding a person to the database. If this is not the case, the use of the database might go beyond the purpose for which it was created. At the moment, the necessity threshold is dependent mainly on the threshold applied by each participating service.

Recommendation: The CTIVD recommends that the AIVD strive to arrive at a multilaterally agreed definition of the targets to be recorded in the database and, in anticipation of this agreement, to at least internally lay down a sufficiently limited definition.

8.2.3 Risks with respect to propriety

- As the data that is shared in the database increases in quantity and includes more sensitive data, there is a risk that the interference with fundamental rights will also increase and will, at a certain point, outbalance the importance of the operational interests served by the provision of the data. This risk primarily exists when personal data is of a sensitive nature, for instance, when it concerns someone's health or relates to a vulnerable category, such as minors. It is necessary that such personal data is made more clearly visible in the database in order to monitor the balance between interference with fundamental rights and operational interests. One example would be to add a distinctive tag to data relating to minors. This reference would directly identify this as data which presents a more serious interference with fundamental rights.

Recommendation: The CTIVD recommends that the AIVD add a distinctive tag to the exchange of data with respect to minors and special categories of personal data in the database, immediately identifying this as data which presents a more serious interference with fundamental rights. It also recommends that the AIVD provide further guidelines in its policy on which data is, and which is not, eligible for exchange via the database.

8.2.4 Risks with respect to due care

- Due care requires that the database is kept up to data by destroying data that is incorrect or no longer relevant and by adding new data. The quality of the database as a whole is dependent on the degree to which it is carefully maintained. This upkeep is currently dependent on national standards. However, these may deviate strongly from each other. Clarifying which data has been added to the database at which point in time may show more clearly whether it is up to date. The CTIVD finds that the AIVD has modified the CTG database in the Autumn of 2017 and currently provides for this. In view of the total amount of personal data recorded in the database and the expectation that this amount will only grow in the time to come, it is necessary that multilateral agreements are made on updating and destroying the data. A regular quality check of the contents and a maximum retention period for the data exchanged multilaterally may be agreed upon, for instance.

- During the period of the investigation, there was no AIVD policy on how the data in the database which has been provided by the AIVD will be kept up to date and, where relevant, destroyed, or on who is responsible for this. This has by now been implemented. The AIVD adopted policy to this effect in August 2017.

Recommendation: The CTIVD recommends that the AIVD strive to come to multilateral agreements on a mechanism for keeping the data in the database up to date and on destroying data that is no longer relevant. Safeguards embedded in the system that ensure that data that has not been updated or viewed for a certain length of time is destroyed may be part of this.

- 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. The CTIVD has identified this as an important risk for the protection of the fundamental rights of the individual. Where national legislation obliges a participating service to destroy certain personal data, for instance because it has been processed unlawfully, it should not be the case that this data can be unreservedly copied by another service and remain present in the CTG database. This would mean that national safeguards would be circumvented.

Recommendation: The CTIVD recommends that the AIVD strive to come to a multilateral agreement which limits the copying of personal data to those cases where the destruction of the personal data is not required under national law. It also recommends that the AIVD internally adopt an instruction on the copying of personal data that includes this limitation.

8.2.5 Risks with respect to reliability

- There is a risk that personal data with a low degree of reliability is entered in the database without this being indicated and that this data forms the basis for actions.

- In August 2017, the AIVD adopted an internal policy for its own exchange of data that provides that only data with a certain degree of reliability may be shared by way of the database.

Recommendation: The CTIVD recommends that the AIVD strive to conclude multilateral agreements on standards for, the reliability of personal data in the CTG database or the indication of this reliability.

- The AIVD has not, as the administrator of the system, provided specific limitations for access to the database system and for the possibility of adding data.

Recommendation: The CTIVD recommends that the AIVD strive to conclude multilateral agreements on the circle of persons granted access or authorised to add data to the database.

8.3 Risks with respect to the CTG operational platform

8.3.1 Risks with respect to due care

- The CTIVD finds there to be risks in the oral exchange of data by the AIVD within the operational platform. The law provides that the exchange of personal data to services that may act upon it must be done in writing. The main reason for this obligation is to make it possible to trace back the data that forms the basis for measures that may have legal consequences to a citizen. It is doubtful whether the records made of the meetings of the operational platform provide a sufficient safeguard for the requirement that personal data is provided in writing, as these records are adopted only some time later and contain a variety of data. Because of the fact that the data exchange may result in measures being taken against persons, extra care is required. An agreement could be made that personal data which is provided orally may not result in measures being taken, except in matters of urgency. No safeguard currently exists in this connection.

- In addition, the CTIVD finds there to be a risk in the cooperation by the AIVD outside of the platform meetings, as the representatives of the participating services work alongside each other permanently and on a daily basis. This permanent physical presence promotes the AIVD orally exchanging personal data with one or more services. Even though the bilateral exchange of data is not considered in this phase of the investigation, the CTIVD does believe it important to address this risk.

Recommendation: The CTIVD recommends that the AIVD strive to conclude multilateral agreements on limiting the oral provision of personal data within the operational platform and that it draft an instruction to its own staff in this connection.

8.4 Risks with respect to the forms of cooperation within sigint cooperation

The recommendations listed in this section also apply to the MIVD.

8.4.1 Risks with respect to the basis for a certain form of cooperation

- In view of the condition that national legislation must be followed when cooperating with foreign services, the CTIVD sees a problem arising with the entry into force of the new ISS Act 2017. The ISS Act 2017 provides a more stringent framework for investigation task-related interception and the further processing of the intercepted data than currently applies to untargeted interception pursuant to the ISS Act 2002.

Recommendation: The CTIVD recommends that the AIVD (and the MIVD) chart the consequences of the new ISS Act 2017 for the continued cooperation by the AIVD (and the MIVD) in a certain form in the area of sigint.

- While it is of great importance that multilateral agreements have been concluded on control and oversight, effective oversight is not yet possible. Expectations are that this will become partly possible in 2018.

Recommendation: The CTIVD recommends that the AIVD (and the MIVD) strive to conclude multilateral agreements which provide for joint oversight on the use of data and which make such oversight (technically) possible.

8.4.2 Risks with respect to due care

- With respect to one form data exchange, there are insufficient safeguards in place to meet the requirement of due care. Even though only limited use is made of this data, the risk exists that this may eventually result in the unlawful use of powers.

Recommendation: The CTIVD recommends that the AIVD (and the MIVD) strive to conclude multilateral agreements which safeguard the accuracy of the data. This concerns ensuring that the data is factually correct, is up to date and relevant, and that the source of the data is clear. It also recommends that the AIVD (and the MIVD), in anticipation of these agreements, lay down internally how this is ensured and who is responsible for this.

Tijdelijk adres:
Frederikkazerne, gebouw 35
Van Alkemadelaan 786 | 2597 Den Haag
Postbus 90701 | 2509 LS Den Haag

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