Enhanced Exchange of Information in Financial Investigations

Geelhoed, Willem; Hoving, Roelf Anton

Enhanced Exchange of Information in Financial Investigations

Willem Geelhoed and Rolf Hoving

17 November 2021

Executive Summary

- FCInet entails an exchange of filters between the participating financial (tax and/or criminal) investigation units. The filters relate to persons involved in tax investigations and/or financial criminal investigations. The filters are sent by the sending participant to the receiving participant without prior request.
- The data in the filter (this can include for example names and dates of birth of natural persons)) are only revealed to the receiving participant if that participant already possesses identical data. The receiving participant thus is informed of the fact that the sending organisation most likely (because the data is subject to a purposefully applied incorrectness factor) also possesses that piece of data.
- The participating organisations exchange filters bilaterally and in a decentralised fashion without prior request. This exchange does not happen automatically, since the participants can specify the data to be exchanged and the frequency of the exchange to suit their preferences. This method can be characterised as spontaneous exchange of information.
- The sent filter is used by the receiving participant to identify natural persons that are known to the sending participant. In case of a match the receiving participant acquired new information and this information can be acted upon. Therefore the data in the filter that is sent should be regarded as (pseudonymised) personal data. As a consequence, data protection rules apply.
- Data protection regulations stipulate that personal data can only be processed to reach the objectives it was collected for, except if further processing is allowed. Data collected for purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties can only be shared for this purpose and not for – among others – tax purposes. Data collected for the purpose of levying taxes cannot be shared for purposes of criminal law enforcement if this this information is used in a manner which is incompatible with those tax purposes.
- FCInet enables participants to comply with international duties to share information which could assist in the investigation of criminal offences or tax fraud, while respecting privacy aspects as much as possible due to its nature of being privacy-by-design.
- Whether a legal basis in an international treaty or EU instrument is necessary to enable the spontaneous exchange of information depends on whether the national law of the participating organisations requires such a basis. If national law does not require this, indicating a common international legal basis may nevertheless clarify mutual commitments.
- There is no feasible basis in national and international/European law to share information across the domains of tax and criminal law on a regular basis. Organisations with criminal law competences and organisations with administrative (tax) law competences can sometimes exchange information, but only on a case-by-case basis.
- There are ample opportunities for participants to exchange information on tax matters on a common basis. The preferable legal basis for information exchange in tax matters is the OECD/Council of Europe Convention on Mutual Administrative Assistance in Tax Matters. Additionally, EU participants may use Council Directive 2011/16/EU on Administrative Cooperation in the field of taxation.
- The exchange of information in criminal matters is possible within a European context. The preferable legal basis for information exchange in criminal matters within the European Union is Framework Decision 2006/960/JHA. Alternatively, the 2000 EU MLA Convention affords a legal basis. There is no general international framework for the exchange of information in criminal matters outside the European context.

Contents

1 Introduction

1.1 Background

This report is the result of a research project focusing on several legal questions surrounding a method for international cooperation in financial and tax-related investigations, which is called FCInet. This entails the setting up of an international, decentralised network with the aim to exchange data between multiple participants on a bilateral basis, located in a variety of countries. The data to be exchanged can concern all information possibly relevant for other participant concerning investigations into financial (tax) irregularities or crimes. This can, among others, include the names and dates of birth of persons involved in these investigations. The personal data are compiled into a filter before they are sent by one of the participating organisations to another. The receiving participant can subsequently try to match the received filter against data that is already in its possession. If a match occurs, the recipient of the filter can infer from this that some information which is known to the recipient is likely also known to the participant that sent the filter. This can only be inferred with a certain level of certainty, since the method is designed to include a specifically set level of inaccuracy, resulting in a level of uncertainty with respect to every match. This method of cooperation is, for purposes of this report, labelled as 'enhanced exchange of information in financial investigations'. The method is not new, being already used in FIU.net, the cooperation between the financial intelligence units of the member states of the European Union.

Following a match, additional information may be acquired through traditional means of mutual legal assistance, be it of a judicial nature or rather a matter of cooperation between police authorities. This could also be facilitated within the software environment within which FCInet operates.

The method employed by FCInet is thought to significantly increase the success rate of financial investigations and the speed with which these are carried out. Because most financial investigations have clear international dimensions, FCInet initiators expect that exchanging data in this manner will benefit their operational output. These financial investigations may include investigations of a criminal nature as well as administrative investigations carried out by tax authorities.

FCInet was initiated by the Dutch FIOD (*Fiscale Inlichtingen- en Opsporingsdienst*, Fiscal Intelligence and Investigation Service) and the British HMRC (Her Majesty's Revenue and Customs). The goal was to include in FCInet a multiplicity of national bodies in other countries within and outside Europe, which are tasked with financial criminal investigations. Because countries distribute their functions in slightly different ways, it proved hard to find institutions in multiple countries that are completely identical in terms of their competences and powers. In order to strike a neutral tone, this report will refer to the bodies involved in FCInet as 'financial investigation units'. While FCInet explains its acronym as meaning 'financial and/or criminal investigations network', for reasons of simplicity we refer to the participating organisations as 'financial investigation units'.

1.2 Perceived need for FCInet and added value

FCInet management takes the position that FCInet is needed to address problems with classic forms of international exchange of information in financial investigations. These problems are thought to be overcome by using an enhanced system of information exchange, comparable to the system that has already been used in the exchange of information in money laundering contexts within FIU.net. This method is thought to have assisted in improving the way international exchange of information is carried out. Under traditional legal frameworks, investigative authorities must issue requests for information to multiple foreign authorities if they desire to enhance their information position with regard to a person who is the subject of an investigation. This can be done by sending the personal information about the person under investigation to multiple foreign authorities and asking for additional information on that person. The number of

authorities this request must be sent to can be substantial if the whereabouts of the person are completely unknown. This method is perceived to have some severe disadvantages. One obvious disadvantage is that it can be quite cumbersome. Each national authority needs to decide on the request, and each request needs to pass multiple steps in specific channels in order for a decision to be made. The precise procedure differs per country and exchange of information in this way may cost a considerable amount of time. Another disadvantage is that personal data is sent to a number of authorities that probably have no use for this data. They also often have no need to know that this person is under investigation in the sending state. The method used in FCInet is supposed to tackle both disadvantages at the same time. In doing so, the participants in FCInet expect to speed up the gathering of information and thereby increase the efficiency of their investigations and their fight against financial irregularities and crimes while protecting the personal data of the persons concerned.[1]

1.3 General characteristics of the technology used

The technology that is used within FCInet is called 'ma³tch'. The suppliers of this technology refer to it as enabling 'autonomous anonymous analysis' – hence the 'a³' in its name. This technology is already applied within FIU.net, the decentralised network of financial intelligence units within the EU, tasked with the fight against money laundering and the financing of terrorism. Ma³tch lets each user – one or more organisations in each participating country – select specific data from its own database or databases for purposes of sharing it with one or more of its collaborators in the other participating countries. The program generates a filter based on the selected records from the database. To generate the filter, ma³tch uses a sophisticated set of algorithms. The filter is sent to one or more of the participants, as selected by the sender. The receiving organisation can check whether (selected) records from its own database are present in the filter. This technology makes it possible to identify whether any records in the receiving participant's database contain information that is most probably also possessed by the sender.

Importantly, a match only indicates a probability that the information is known to both receiving and sending participant, for the software that generates the filters is set to introduce a certain amount of uncertainty in the filters. In addition, differences in registration cannot be completely prevented. Therefore, false positives may occur, the frequency of which being mainly dependent on the level of uncertainty introduced. Therefore, a match only indicates with limited accuracy that the information in question is the same. This being the case, when a match occurs within the compared filters, additional information may be requested in a targeted fashion through the commonly available channels for mutual legal assistance. The objective for this is to exclude the possibility that the match is a false positive, and to gain further information in the more likely case that the match is not a false positive.

Due to the fact that personal data is transformed into a filter in a specific manner, it is impossible to deduce which data was used to compile the filter in case the filter is intercepted. Even to a legitimate recipient, no information is made available as long as there is no match. If a match occurs, the recipient does gain knowledge of the fact that not only the recipient himself, but also the sender is in possession of a certain piece of information. In such a case, the sender of the filter is however not informed about the match. This is the reason that this technology is labelled 'anonymous': it enables the recipient to find a match using the filter received without disclosing that fact to the sending organisation. A more detailed account of this technology and the way it is implemented in the context of FCInet follows in chapter 2.

1.4 Aims and setup of this research project

While the participation of a multiplicity of partners is an end goal of FCInet, the technology was first tested in a pilot phase. In that pilot phase, the participants were the

—

[1] See Nunzi 2007.

FIOD in the Netherlands, the *Bijzondere Belastinginspectie* (BBI, Special Tax Inspectorate) in Belgium and Her Majesty's Revenue and Customs (HMRC) in the United Kingdom. A preliminary report by the research team concerned only that pilot phase of FCInet.[2] One of the main recommendations of the preliminary report was to avoid exchanging information across domains, that is exchanging information originating in the criminal law domain to the tax domain or vice versa. This recommendation was endorsed by the FCInet secretariat. This meant that the participating organisations were classified as belonging to either the tax domain or the criminal law (law enforcement) domain. Some participating organisations cover both domains, but these are also split internally in separate sections. Accordingly, FCInet incorporates participating organisations in two domains that cooperate in two separate networks for exchanging information. This recommendation is still relevant. Within this final report, there are still sections discussing the need for separation between the two domains. While FCInet already complies with these recommendations, the research team wishes to retain these as they form an integral part of the overall research project, and remain of relevance for the future.

This final report covers questions that were covered by that preliminary report and a number of additional questions. Following the preliminary report, the research team were commissioned to carry out further research. This entailed firstly the compilation of a practical summary of the preliminary report and a checklist to be used by organisations that were deciding on whether or not to join FCInet. Further, the research team agreed with the request to enlarge the project in such a way that it also involved Australia, Canada and the United States, and at a later stage, five additional countries, namely: Denmark, Finland, Iceland, Norway and Sweden. Lastly, the research was expanded to include research into the legal questions surrounding follow-up information requests following a match. In addition, the research team was requested to present the information found in the form of a matrix showing possibilities and impossibilities of information exchange between the authorities involved.

Taking all of this into account, the research aim of this entire project is to identify the legal questions surrounding the method for enhanced exchange of information that is used in FCInet, to identify and apply the legal framework to FCInet's specificities and to offer advice on the basis of the results of this application.

As to the research methodology, the research team received access to information on FCInet through the FCInet Secretariat, project members, associated personnel and members of the national authorities that were and are involved in FCInet operations. The research team also consulted independent experts, as well as practitioners such as public prosecutors. Information on the national laws of the participating countries (except for the Netherlands, which the research team covered itself) was gathered on request by the research team, which compiled a questionnaire that was presented to personnel within the national authorities participating in FCInet. This questionnaire is included in this report as Annex 4. The questionnaire was slightly changed as different versions were sent out to the initially participating countries, compared to the countries that were included later. One aspect which was changed was that later versions included questions on follow-up information requests. These questions were sent separately to the initially participating organisations, so that the answers to these questions were received from these participating organisations as well. Included as Annex 4 is the final version of the questionnaire, that was sent to the participating organisations in Denmark, Finland, Iceland, Norway and Sweden.

The answers to the questionnaire were of use for compiling a comparative overview of national laws relevant to FCInet, consisting of both national laws on data protection and national laws on information exchange in tax matters as well as in criminal law matters. The answers we received from the participating organisations were summarized in short country reports, which informed this report and particularly the overview

—

[2] Geelhoed, Hoving, Lindenberg & Renshof 2018.

offered in the three matrices in Annex 1, 2 and 3. The country reports are included in this report as Annex 5. For detailed information with regard to a specific participating organisation on a particular issue, please consult the relevant country report.

1.5 Research questions

This report tries to answer the various legal questions that surround the setup of the FCInet. The central question is: 'Which competences, duties and restrictions in national and international law apply to the exchange and matching of data as foreseen within FCInet?' By framing the question in this manner, the possible outcomes of the research in terms of the legal framework are divided into three types of legal rules. We expect to find rules on the competences conferred on the participating authorities in FCInet concerning the exchange of data and the use to which exchanged data may be put. We also expect to find rules that confer duties upon the participating authorities, obliging them to share with foreign authorities the data that are in their possession. Lastly, we expect to find rules that restrict the exchange of data and the use of data that is received for reasons of data protection. For all three categories of rules, there will probably be rules on the national level as well as on the international level.

In order to answer the central research question, this question is divided into subquestions each focusing on a part of the research question. First, a clear reconstruction of FCInet is necessary in order to test it against the relevant legal framework. The first subquestion therefore relates to the technology used and the way in which FCInet is organised. It reads: 'In what way does FCInet operate and which methods does it use?' This subquestion is answered in chapter 2, which reconstructs FCInet's design and methodology.

The second subquestion relates to relevant data protection rules, restricting data use: 'Which data protection rules apply in the context of FCInet and what do they entail for the exchange of data as envisaged in the project?' A key starting point for answering this question is characterizing the nature of the data. When the data can be characterised as anonymous data, no rules on the protection of personal data apply because they do not constitute personal data. If they do however, there is a considerable body of data protection rules applicable, both on a national and on an international level. Which rules apply exactly can however still depend on other factors. Data protection rules also recognise a category of 'pseudonymised' data. This is data which is encrypted or otherwise made meaningless to a person who possesses the data by chance or by way of a security breach. Pseudonymised data however retain the status of personal data because the data can be traced back to individuals by persons having additional information – a 'key'.[3] It is our starting point in answering this research question that the data that is exchanged and leads to a match within FCInet can be characterised as pseudonymised data, because it has been made inaccessible to an accidental possessor, but can be traced back to individuals by the participating authorities who can avail themselves of the common algorithms that FCInet participants have shared beforehand. There is some uncertainty whether the data retains the character of personal data at all times, or whether only the data that leads to a match can subsequently and retroactively been viewed as personal data. This subquestion is answered in chapter 3.

The third subquestion relates to treaties which lay down competences for the type of data exchange that FCInet envisages. Additionally, it focuses on possible duties to mutually exchange information. It reads: 'Which competences and duties exist, in multilateral treaties and EU instruments, relating to the exchange of data as envisaged in FCInet?' The treaties that come into the picture will primarily be of a multilateral nature, for instance concluded within the United Nations (UN), Council of Europe or OECD framework. Some bilateral treaties can also be of importance; however, attaining the objective of FCInet to enlarge the number of participants to include many countries will be much easier when a uniform legal framework is found. If that turns out to be impossible, alternative routes may be explored which can include the study of bilateral

—

[3] EU Agency for Fundamental Rights 2018, p. 94-95.

treaties. In addition to multilateral treaties, legal instruments adopted within the framework of the European Union (EU) will also be of relevance. All of these treaties and other instruments will naturally only be explored to the extent that they govern the relationship between two or more of the participants in FCInet. The starting point in answering this subquestion is that FCInet's design of decentralised information exchange can be characterised as the (albeit frequently executed) spontaneous exchange of information from one country to another. This analysis will include both instruments within criminal law cooperation as well as instruments enabling tax cooperation. It will also include both the exchange of filters and the exchange of information as a follow-up request following a match. It will also tackle the related issue, whether existing treaties that enable certain forms of data exchange have an exclusive effect, forcing countries to choose certain forms of collaboration and thereby in effect making FCInet impossible.

The fourth subquestion relates to the national law of the participating countries, more specifically to the competences and duties for the type of data exchange foreseen in FCInet. It reads: 'Which national rules exist governing the exchange of data in FCInet and the use of data obtained through it, in the participating countries?' The third and fourth subquestions will be dealt with in a number of separate chapters. Chapter 4 will discuss general issues related to the exchange of information. Following that, chapter 5 will discuss the exchange of information in tax matters, and chapter 6 will discuss the exchange of information in criminal matters. To some extent, the contents of these chapters will be interlinked and overlaps will not always be avoidable. In these three chapters, the focus is mostly on the details of national rules governing official records and the exchange of information between authorities, while chapter 3 deals more in general with data protection issues. Besides this, there is a connection between competences for data exchange in international instruments and in national law. National law not always, at least not clearly so, requires a treaty basis for information exchange. To some extent it could therefore be irrelevant whether there is a competence for the exchange of data, and the answer to the third subquestion might then be not very important.

Chapter 7 contains conclusions and points of discussion on this research project.

1.6 Applicability of research findings to the future of FCInet

This research regards initial phases of FCInet as well as some stages in which FCInet is employed to a wider collection of participating countries. To some extent, the findings in this report may be relevant for even later stages of FCInet. However, in that case the changed characteristics of the network that will arise when more participants are included should be kept in mind. To new participants, a different treaty framework may apply. To a certain extent, this report could inform the standards for cooperation with organisations from other countries than the ones which were included in FCInet until now and that are covered in this report. But this is not self-evident. Both the legal bases for cooperation and the data protection rules may differ. In addition, international law cannot offer a complete framework, as national decisions on the designation of competent authorities remain necessary. Moreover, a worldwide cooperation will be subject to data protection regimes that differ from the regimes within the EU context, which is quickly becoming a sort of standard model of data protection.[4]

To enable a future expansion, regulatory absences may possibly be remedied by concluding a specific treaty, regulations by the EU or other regional bodies or Memoranda of Understanding.[5] While this is certainly possible, it also may require lengthy negotiations. However, it is also possible that organisations from some of these countries may participate in FCInet without substantial difficulties as to the legal regime. But even in these cases, a (limited) research about the legal context will be inevitable.

An additional remark about the future applicability is that this research focuses on the exchange of names and dates of birth of natural persons. If FCInet would be

—

[4] De Busser & Vermeulen 2010. See also Commission Communication 2017, p. 13-16.

[5] An example may be Council Decision 2000/642JHA, offering a legal basis for FIU.net.

expanded and cover more types of data to be exchanged, additional legal questions may be triggered which are not all conclusively dealt with in this report. This is especially the case when types of personal data that are regarded as especially sensitive and therefore in need of a higher level of protection, are to be exchanged.

Be that as it may, we hope to lay down a line of reasoning that can be applied *mutatis mutandis* if and when FCInet will be expanded both in terms of participants and in the types of data that will be exchanged.

1.7 Project organisation

The research project which formed the basis for this report was carried out by researchers at the Department of Criminal Law and Criminology of the University of Groningen and financed by funds made available by FCInet. The main researchers were Dr. Willem Geelhoed (who also acted as project leader) and Dr. Rolf Hoving. Prof. Kai Lindenberg provided expert comments. Ms. Ananda Renshof, Mr. Marlo Post and Ms. Judit Kolbe offered assistance to the research team. The project reported to the FCInet Secretariat, for these purposes consisting of Ms. Gonnie de Graaff-van Dijk and Mr. Harry Krüter. The latter was replaced by Ms. Mariella Pinna in 2021.

This research project ran in its totality from June 2017 to November 2021, consisting of multiple, disconnected phases in which the research was conducted. Next to performing research into literature and (international) legislation, the research team interviewed a number of relevant experts.[6] Preliminary findings were discussed with a group of legal experts working at FIOD, in a meeting on 11 September 2017. The preliminary findings were furthermore presented to and discussed with representatives of FIOD, BBI and HMRC on 26 September 2017. A preliminary report was finalised on 16 January 2018.

After this preliminary report, the research team was commissioned by the FCInet Secretariat to compile practical guidance on the basis of the preliminary report and a checklist to be used by prospective FCInet participating organisations. This set of guidelines and checklist was finalised and sent to the FCInet secretariat on 6 September 2018. The preliminary findings were discussed during a number of meetings, among which two meetings of the FCInet Platform at the OECD, Paris, on 7 March 2018 and 31 October 2018.

Later, the research team accepted an extension of the research project. This concerned the inclusion of extra research questions into the nature and legal bases of follow-up questions following a match, and the presentation of all findings in the form of a matrix. Moreover, this extension concerned firstly the addition into the comparative overview of Australia, Canada and the United States and later also Denmark, Finland, Iceland, Norway and Sweden. All consulted officials that have assisted this research project by answering to the questionnaire are listed in Annex 4 to this report. A short comparative overview of the national laws of Denmark, Finland, Iceland, Norway and Sweden was compiled and finalised on 1 September 2021.

This final report was finalised on 17 November 2021 and presented at a symposium at the University of Groningen at that same date, titled ‘Enhanced Exchange of Information in Financial Investigations’.

—

[6] A list of all consulted experts and official functionaries within FCInet can be found in Annex 4 to this report.

2 The Technology behind FCInet

2.1 Introduction

In a globalised world, financial criminal or otherwise illegal activities – like tax irregularities and crimes, corruption, money laundering and fraud – are regularly committed on a transnational level. Consequently, it is possible that several organisations in different jurisdictions have gathered some information about these activities. This information can concern people who are suspected of committing an illegal activity, but it can also relate to persons or legal bodies, bank accounts, addresses, activities, etcetera that are of interest to investigating authorities.

FCInet is a method to share data between financial investigation units from various backgrounds. FCInet seeks a balance between on the one hand securing the sound and effective investigation, prosecution and prevention of international, cross-border financial criminal or illegal activities and on the other hand protecting personal data of the people involved. The idea is that by sharing data between financial investigation units international connections between criminal and illicit activities and their perpetrators can be found.

In this chapter, the concept and the technical specifications of FCInet will be elaborated upon. In doing so, this chapter will provide an answer to the first subquestion, 'In what way does FCInet operate and which methods does it use?' FCInet aims to share, among others, data involving the names and dates of birth of persons and entities involved in tax irregularities and/or criminal investigations (hereafter in short: suspects). These kinds of data can be regarded as exemplary data, and therefore the focus in this chapter will lie on these kinds of data. However, it is important to keep in mind that it is the intention of the FCInet partners to also share other kinds of data.

2.2 Concept

The investigation of criminal or illegal activities by a financial investigation unit can result in the suspicion that a person committed a crime or illegal activity. For the investigation, it is desirable to gather and analyse all incriminating and exculpatory evidence available. This information does not have to be held by the financial investigation unit that carries out the investigation, but can also be held by other organisations. On the national level information about suspects can be held by government bodies charged with the investigation and prosecution of criminal activities, like the police, customs and the Public Prosecution Service. Information can also be held by administrative or public organisations such as tax authorities, the central bank and chambers of commerce, and by private corporations, for instance banks. A suspicion is often not limited to a national level. Relevant information should therefore also be sought after on a transnational level. Just as it is the case on a national level all sorts of organisation can hold some piece of useful information.

The exchange of information about a suspect between jurisdictions is possible through mutual legal assistance. Several international and European legal instruments make it possible to share this information. However, a formal request for information about a suspect will only be done when the inquirer has a reason to believe that the information is available in the jurisdiction the request is sent to. Also, investigative organisations are often not aware of the information their international counterparts have. Often it is not feasible to ask whether the investigative organisations in other jurisdictions have some information about a particular suspect. This will be like looking for a needle in a haystack. Moreover, it is also undesirable to share information about a suspect with organisations in other jurisdictions, because of the duty to protect personal data and the need to secure national interests. For a sound and effective investigation of transnational criminal or illegal activities it is however advisable to have an appropriate level of information-sharing regarding suspects between investigative organisations in different jurisdictions.

FCInet makes it possible for financial investigation units to identify whether a foreign partner holds some information about a suspect, without sharing more or less information than needed. With FCInet the sending organisation shares an encrypted version of the personal data of the suspects held in the database of the sending organisation. Or, to say it more precise, the sending organisation shares a filter based on the personal data of the suspects. Such a filter is not exactly an encrypted copy of the original data, but captures the 'characteristics of the original data'.[7] To create a filter the personal data of the suspects are aggregated, encrypted and processed by algorithms. The advantage of a filter – in comparison with just an encryption – is that it is not possible to re-identify the personal data on the basis of the filter alone.[8] More details about the technical specifications of the creation of the filter will be given in the next paragraph.

Through FCInet the sending organisation shares the filter with (a selection of) the organisations connected to FCInet. This filter can be used to compare the population of suspects of the sending and receiving organisation. A receiving organisation can check whether a processed version of the personal data of one (single match) or more (cross match) of the suspects in their own database will pass the filter. If the processed data passes the filter there is a match (or a hit). A match means that it is likely that the same suspect is registered in the databases of both the sending and the receiving organisation. In other words, when there is a match, it is likely that both the sending and receiving organisation regard a certain person as a suspect of a criminal offence or a person of interest in an administrative procedure, and have collected some information about this person.

Sharing a filter through FCInet directly benefits the receiving organisation. The receiving organisation can check whether a particular suspect is likely to be found in the databases of the sending organisation. When there is a match, only the receiving organisation will know and gain information. It is free to decide whether or not it wants to collect additional information about the suspect from the sending organisation via a request for mutual legal assistance. The sending organisation will not get a notice when the receiving organisation found a match, unless the receiving organisation makes a formal request to receive more information about a particular suspect.[9] The sending organisation will benefit from the collaboration in its role as a recipient of filters, sent to it by the other participants. In that way FCInet as a whole upholds the idea of reciprocity.

FCInet is a peer to peer-network. This means that filters are shared decentralised between the organisations associated with FCInet. A filter can be shared with one or more partners, but the actual data on which the filter is based, stays within the control and responsibility of the sending organisations and does not leave this organisation. There is no central database in which the filter is uploaded. The sending organisation can update or delete a filter at any moment.

An alternative method for information-sharing is an international, centralised database with information, for example the Schengen Information System which supports border controls in the European Union. A centralised database contains the information that national investigative organisations have sent to the administrator of the database, because it was deemed as possibly relevant for the purposes to which the database is put. Within the scope of this report there are two advantages of a peer-to-peer network like FCInet in comparison with a centralised database such as the Schengen Information System. Firstly, in a centralised database more information might be shared than needed. Because a centralised database can be accessed by all associated partners of the database, it is dependent on how their rights of access are defined who of them has access to which information. This is a somewhat less secure method of safeguarding data access than the method used in a decentralised design. Secondly, in a centralised

—

[7] Balboni & Macenaite 2013, p. 332.

[8] Kroon 2013, p. 27.

[9] Balboni & Macenaite 2013, p. 338.

database it is possible to share less information than needed. Because the information in the international database contains a selection of the information that a national investigative organisation has at its disposal, it is possible that some information is not selected to be put in the central database, while the selecting organisation is unaware that this information is very relevant for a partner.[10]

In another respect FCInet can be compared with the Schengen Information System. Both have a hit/no-hit system.[11] In a hit/no-hit system a query can result in a hit (or a match) or a no-hit (or no match). The fact that there is a hit/match does not mean that the person who made the query gains access to the available information. This depends on the access rights to this information or on the necessity to request mutual legal assistance. This kind of system is viewed positively by the European Council. It states: 'The hit/no hit system provides for a structure of comparing anonymous profiles, where additional personal data is exchanged only after a hit, the supply and receipt of which is governed by national law, including the legal assistance rules. This set-up guarantees an adequate system of data protection, it being understood that the supply of personal data to another Member State requires an adequate level of data protection on the part of the receiving Member States'.[12]

2.3 Technical specifications

The process framework behind FCInet is called ma³tch. This is developed by the Dutch Ministry of Justice and Security. The name refers to its triple basis: autonomous anonymous analysis.[13] The mission of ma³tch is: 'getting the right information, at the right time, in the right way, from and to the right place'.[14] Ma³tch can use algorithms, such as fuzzy logic, hash tables, Bloom filters, transliteration, n-grams and approximation techniques to anonymise, aggregate and compare data.[15] This process framework is also used in other initiatives like FIU.net. FIU.net is 'a decentralised and sophisticated computer network supporting the Financial Intelligence Units (FIUs) in the European Union in their fight against money laundering and the financing of terrorism'.[16] FIU.net is authorised by the European Commission.[17] It is maintained by the European Commission. FIU.net is a success. The 4th Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) Directive prescribes that: Member States shall require their FIUs to use protected channels of communication between themselves and encourage the use of the FIU.net or its successor (article 56 under 1 of the Directive).[18]

To give a better insight in the mechanisms of FCInet it is necessary to describe the system in more detail. This will be done by describing the six steps that can be discerned between having a list of full personal data of possible suspects in one jurisdiction and a possible match in another. These steps are: 1) selecting the data, 2) standardising the data, 3) processing the data, 4) creating a filter, 5) sharing the filter and 6) using the filter.

—

[10] There are other advantages of a peer-to-peer network. One advantage is that the amount of information shared by an organisation in a peer-to-peer network can vary, dependant on the goals, the ambitions and the partner with whom the information is shared. In contrast, to have a centralised database it is necessary to make a joint agreement about the information that should be shared. Another advantage is that there is no need to fund the creation and maintenance of a centralised database.

[11] Balboni & Macenaite 2013, p. 338.

[12] Council Decision 2008/615/JHA, recital 18.

[13] For more information about these values, see Kroon 2013, p. 26.

[14] Presentation by FCInet project team, 24 April 2017.

[15] Kroon 2013, p. 27.

[16] https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net#fndtn-tabs-0-bottom-1 (on 15-6-17). Europol 2017.

[17] Council decision 2000/642/JHA.

[18] Directive (EU) 2015/849.

2.4 Selecting the data

The sending organisation has to decide which records with data will be processed into a filter. This selection can be very broad or very small. It is possible to turn records of all the personal data – names, dates and places of birth, addresses, bank accounts, etc. – of all suspects in a database into a filter, but a filter can also be based on a record with the name of only one suspect. Between these extremes there are possibilities to base filters on subsets of the population of suspects. Such a subset can be based on criteria such as the crime the suspect is suspected of – for instance, money laundering, fraud, corruption – the nationality of the suspect, the legal status of the procedure against the suspect or the source of the information the suspicion is based on. Other data can also be turned into a filter, for example non-personal data or personal data of persons who are not (yet) regarded as suspects. Selection is possible as long as the software provides the facilities to select certain criteria.

The receiving organisation can match the data in its own local server. In doing this, the receiving organisation is only to a certain extend bound by the selection the sending organisation made. The receiving organisation is not compelled to make the same selection as the sending organisation did. For example, the sending organisation can base a filter on a subset of money laundering-suspects. The receiving organisations can match their own money laundering-suspects with this filter, but is not barred from trying to match other suspects of, for example, fraud and corruption. The question can be asked whether this is desirable. However, even if the conclusion is that the freedom of the receiving organisation should be limited, it will be hard to find satisfactorily restrictions. It is likely that legal obligations or technical interventions that can harmonise the subset in the filter with the subset of the data that are to be matched with the filter are laborious and will require much deliberation. Because of the differences between jurisdictions with regard to, amongst others, the legal qualification of certain unwanted behaviour and the dividing line between criminal law and administrative law, the current national databases of financial criminal investigation units have their own distinct characteristics. These databases are not easily harmonised.

2.5 Standardisation of data

The data that are to be transformed into a filter have to be standardised to be comparable. National databases can use different formats to register personal data such as names and dates of birth. This can distort the matching process. Therefore, all data are standardised. This means that names are put in the same order, letters get the same case, dates get the same format and all special characters are removed. Algorithms are used to standardise the data. These algorithms make it possible to make a match with high accuracy, even when there are 'transliterations, permutations and approximations'.[19] The level of accuracy depends on the amount and sort of algorithms that are used to standardise the data. Especially when more approximations are allowed, the accuracy will drop.

2.6 Processing the data

The records with personal data in the database are further processed and anonymised with the help of additional algorithms. This is called hashing the data. Hashing can be seen as one way encryption. Hashed data cannot be decrypted. Hashing, instead of encrypting the personal data, uses algorithms to isolate some characteristics of the personal data while the rest of the information is thrown away. The characteristics alone are not enough to reconstruct completely the source data. Examples of characteristics that can be isolated are: the fact that the record starts with a 'J', the fact that the record does not contain an 'I' and the fact that the square of the numbers in the record is '506875650304'. These characteristics describe the original personal data, but are not the original personal data. It is playing the game 'Guess Who' and making statements

—

[19] Kroon 2013, p. 27.

like 'the person has a beard' and 'the person wears glasses'. Because the original personal data are described, it is possible that two wholly unrelated persons have the exact same characteristics. This will lead to an exact same hash. The possibility that the characteristics are too broad gets smaller if more characteristics are used.

The result of the transformation process is a 'hash'. This hash is always of the same length, irrespective of the length of the record with the original data. The transformation of the personal data into a hash can be illustrated with an example (see image 1). It is important to keep in mind that this is merely an example to illustrate how ma³tch algorithms can transform personal data records into characteristics, and the example is extremely simplified. It does not describe the way the algorithms really work, but provides an insight in the principles the system is based on. An additional remark: hashes are based on the entirety of all the selected personal data and not on the individual elements hereof.

Take as example the record with the personal data of the suspect Johhny Fontane, born on 7-1-1952.[20] The characteristics of the entire personal data (the name and date of birth) of this suspect can be described. In this simplified example discrete numerical values are used for the description (but other values could also be used). Characteristic 1 is the numerical value of the 10th letter of the record (a 'T') = 20. Characteristic 2 is the added value of the first two numbers in the record, times three ((7+1) x 3) = 24. Characteristic 3 is the amount of N's in the record = 04. Characteristic 4 is the multiplication of the last two numbers in the record (2x5) = 10. Characteristic 5 is the numerical value of the most used letter of the record ('N') = 14. Characteristic 6 is the added value of all the numbers in the record = 25. Characteristic 7 is the numerical value of the 7th letter of the record (a 'F') = 06.

The transformation from the data into characteristics, into a hash, must be repeated for all the records with personal data that the sending organisation has selected. The chosen characteristics are the same for each record. As a consequence the transformation of the personal data of one suspect will always result in the same values. As long as the personal data do not change, the values do not change.

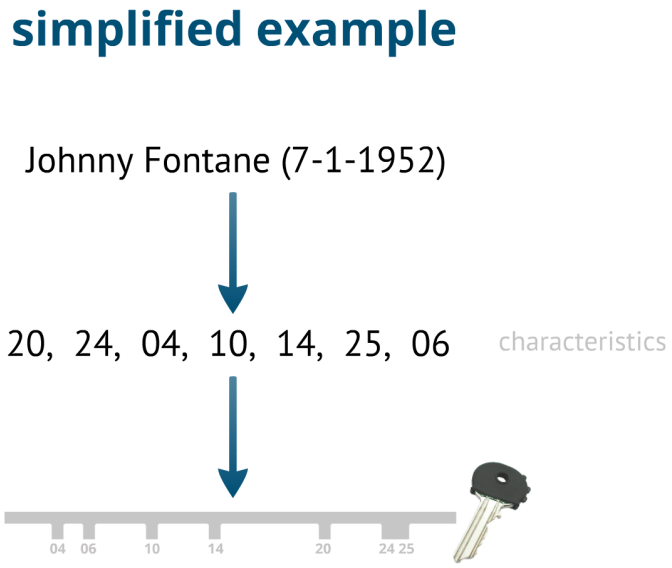

Image 1 - Source: Presentation FCInet

—

[20] Examples are based on Kroon 2013, p. 27 and a private presentation of FCInet on April 24th 2017. The elaboration of this example is made by the authors of this document.

2.7 Creating a filter

When the characteristics of all the records with personal data are gathered, a filter can be created. This is again done by algorithms. A filter contains the aggregated characteristics of all the records with personal data of each selected suspect. The creation of a filter can be illustrated with a continuation of the – still extremely simplified – example (see image 2). Besides Johhny Fontane, there are two additional suspects selected to be part of the filter: Philip Tattaglia and Luka Braassi. The characteristics of these two additional suspects are generated in the same way as with Johnny Fontane. This results in two additional sets of values: Philip Tattaglia (03, 07, 09, 10, 15, 24, 26) and Luka Braassi (02, 06, 09, 12, 17, 21, 28).[21] When all the values of all three records are taken together and put into increasing order, this results in this list of values: 02, 03, 04, 06, 07, 09, 10, 12, 14, 15, 17, 20, 21, 24, 25, 26 and 28. The filter is based on these values. More specifically, the values that are missing are taken and transformed into a filter. These values are (when the maximum value is set at 30): 01, 05, 08, 11, 13, 16, 18, 19, 22, 23, 27, 29, 30. The filter consists of binary numbers (1's and 0's) indicating whether or not a specific number is present in the filter. A 1 means the number is present, a 0 means the number is absent. So the filter in this example will be: 011101101101011010011001110100.

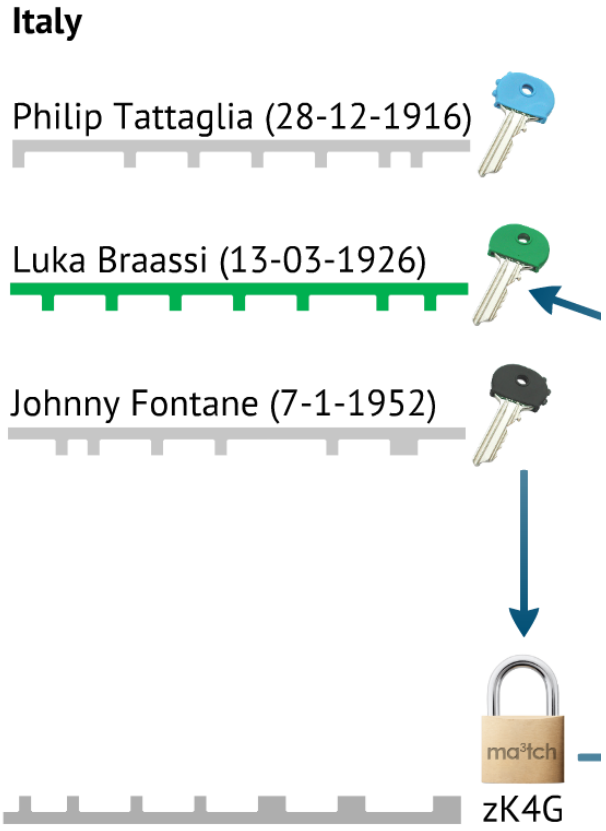

Image 2 - Source: Presentation FCInet

With the aggregation of values, the filter is minimised. The filter retains the essential information included within it, namely whether a characteristic of the personal data of a single person/record is present. The filter can have, for example, when the binary code is translated into letters, the name zK4G. The aggregation of the values is called 'hashing

[21] These values are random example. When the same rules as in the example of Johnny Fontane would have been applied it would have resulted in the values: Philip Tattaglia (28-12-1916) = 20, 120, 00, 06, 01, 30, 06 and (Luka Braassi (13-03-1926) = 19, 48, 00, 12, 01, 25 and 04.

the hash'.[22] To guarantee that the generated filter cannot be translated back into one set of characteristics representing one suspect, the personal data is hashed twice. It is hashed a first time when the personal data is transformed into characteristics, and it is hashed a second time when the aggregated characteristics are transformed into a filter. Data that is hashed once could in principle be traced back to identifiable information using a so-called 'rainbow table'.[23] Data that is hashed twice cannot be traced back to individuals without additional information.[24]

2.8 Sharing the filter

A filter is created by a national organisation. Multiple filters can be created on the basis of the same database. This seems obvious, because a national organisation can decide which parts of the database should be transformed into a filter. But even on the basis of the same selection of personal data multiple filters can be created. Which filter is created depends on the margin of error desired by the national organisation. The algorithms of the ma³tch-software ensure that there is a standard chance for a random false positive match. This is the precision of the system. The chance for a random false positive can be configured, but is never zero. This enhances the protection of the personal data in the filter. The precision of the system can be set high, which means that the chance of a random false positive match is very low, say 1 in 1000 (a precision of 99,99%). A low precision means that the chance of a random false positive match is very high, say 1 in 7 (a precision of 85,7%). An organisation could choose a lower sensitivity and accuracy to protect sensitive data.[25]

The organisation that creates the filter can decide whether or not it wants to share the filter. The national organisation can also decide which filter it wants to share with whom. It is possible to share different filters – with a different selection of personal data and/or a different precision of the filter – with different partners. If the organisation decides to share the filter, the sending organisation can place the filter within the context of FCInet at the disposal of the receiving organisations associated with FCInet. Within FCInet the sending organisation keeps the control of the filter. Only the sending organisation can delete and update the filter. The receiving organisation can use the filter, but not outside the context of FCInet.

To be up-to-date it is necessary to share new filters on a regular basis. Old filters can be deleted and replaced by the new filter. Replaced versions of a filter are not retained. The sending organisation can decide how often new filters are sent. The software does not set time limits. Therefore, filters do not have to be refreshed for many months. The receiving organisation can use a filter as long as it is not replaced or removed by the owner. A filter will not be deleted after a certain period of time, except for a regular cleaning of the system. How this will be done, and by which frequency such a cleaning will occur is to be further determined. However, it seems possible that a receiving organisation can still use a filter that is created year(s) ago by a sending organisation when it is not replaced.

2.9 Using the filter

The receiving organisation can use a filter to check whether a suspect in its database can also be found in the database of the sending organisation. This is done by checking whether the characteristics of the personal data of a particular suspect can be found within the filter. For example, the filter can be checked on whether it contains the characteristic that the record begins with a 'J'. However, the characteristics will be checked all at once. Therefore, the guesser only has one round and can only ask: 'Does

—

[22] Balboni & Macenaite 2013, p. 333-334 and 337.

[23] Balboni & Macenaite 2013, p. 333 and 337. A rainbow table is a precomputed table for reversing cryptographic hash functions, https://en.wikipedia.org/wiki/Rainbow_table (last checked 26 June 2017),Wikipedia 2017.

[24] Balboni & Macenaite 2013, p. 337.

[25] Kroon 2013, p. 27.

the person have a beard and glasses?' The relation between the filter and the characteristics of the personal data can also be compared with a key and a lock. As long as a key has the right shape, it can open the lock. But when the bits of a key do not fit the lock, the lock will not open. With FCInet, the 'lock' is the filter and the 'keys' are the characteristics of the personal data of the suspects.

The receiving organisation has to transform records with the personal data of the suspects in its own database into characteristics before it can use the filter. The same algorithms as the sending organisation are used to transform the personal data. These algorithms transform the personal data always in the same manner. Therefore, when the sending and receiving organisation both have the same suspect in their database, the same characteristics are found. These characteristics can be compared with the filter. This is done by the system.

To continue the simplified example (see image 3): assume that the receiving organisation (in this case in the United Kingdom) wants to know whether the sending organisation (in Italy) knows Luca Brasi. First it has to isolate the relevant characteristics of the personal data of Luca Brasi. One of the characteristics that was earlier mentioned was the multiplication of the last two numbers of the record. This is 12 in the case of Luca Brasi (2x6). The next step is to check whether this characteristic can be found in the filter. This is the case, because the characteristic of 12 is present (= 1) in the filter. And this is a clue that Luca Brasi is known in Italy. There is a match when all characteristics are present in the filter. (By the way, because of standardisation of data it is possible that a different spelling can still result in a match). The receiving organisation can also check whether other suspects are known. When it tries Moe Greene, the earlier mentioned characteristic is absent (= 0) in the filter (for 3x6=18). This means that there is no match.

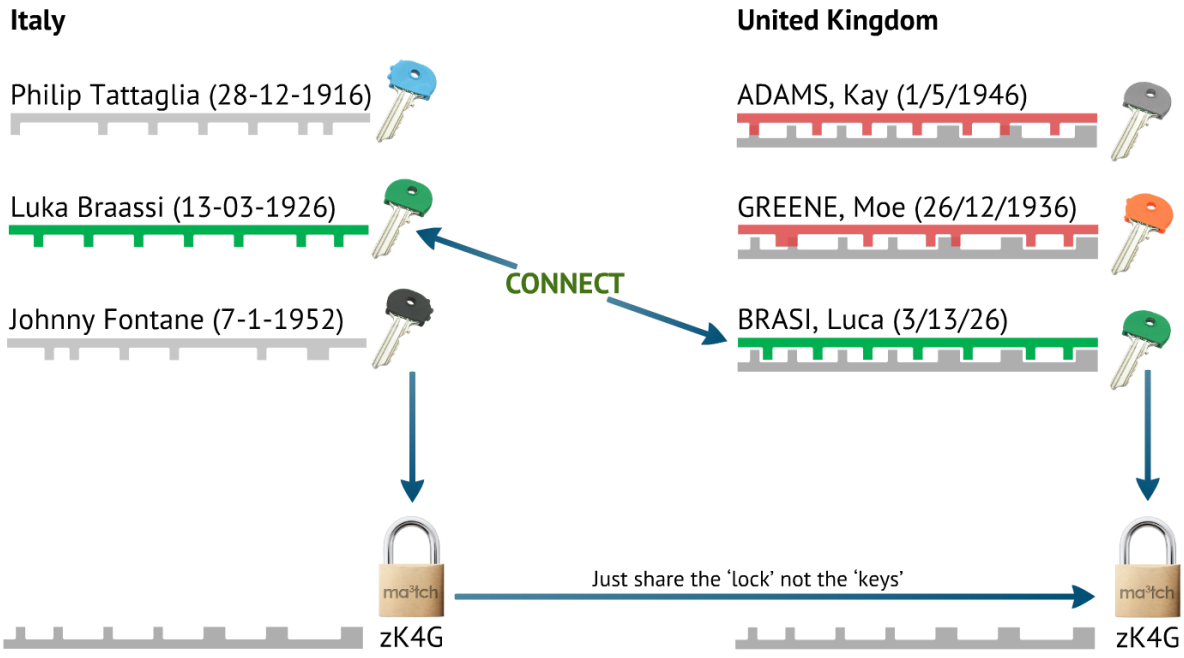

Image 3 - Source: Presentation FCInet

The receiving organisation can use the filters in FCInet to check whether one particular suspect is known in other jurisdictions. This is single matching and will be done when new suspects are added to a database. The receiving organisation can also use the filters in FCInet to check whether more suspects in the database are known in other jurisdictions. This is cross-matching and will be done when new filters are added to FCInet. Automatic cross-matching can be useful to be sure that new matches are found when a new or updated filter is shared through FCInet.

A query in FCInet can result in a no match (no-hit) or a match (or hit) – hit or match are seen as equivalents in this report. A no match means that the sending organisation does not know the same suspect as the receiving organisation, at least not under the name the receiving organisation knows the suspect. It is not possible to find no match when both databases have registered the suspect in the same way. No match, however, is possible when the sending and receiving organisation have registered the same suspect in a different way, for example with a different alias or when the spelling differences are so big that the algorithm is not able to standardise the spelling.

A match means that it is likely that the sending organisation has registered the same suspect as the receiving organisation. But it is not sure. There are two ways to get a match without an actual correspondence. Firstly, the ma³tch software produces standard random false positives. This is the consequence of the transformation of personal data into characteristics of these data. Because the same characteristics can describe a different person it is possible that there is match while this is not correct. The amount of false positives that are randomly produced depends on the sensitivity of the system. The amount of characteristics used and the amount of records about some individual in a filter determines the precision of the filter. The chance of this kind of false positive will be lower when more and more unique characteristics are used. But the chance at a false positive will increase when algorithms take into account transliterations and permutations. For example, it is possible that names that do differ in reality are taken as the same, as with 'Jon' and 'John'. This increases the chance that two distinct persons have the same characteristics. The sensitivity of the system can be adjusted manually, but not eliminated altogether. So there will be always a random chance of a false positive, be it possibly a very small one. But this random chance on a false positive can be set much higher to even chances in which the finding of a match is short of meaningless.

Secondly, a match without actual correspondence can result from the underlying personal data as it is registered in the national database. Features such as the first name, surname and date of birth do not have to be unique for a particular person. It is conceivable that there are two – wholly or partly – unrelated suspects having the same name and date of birth. For example, in the Netherlands 'Jan de Jong' is a common name and it is therefore possible that there are two (or more) persons called Jan de Jong with the same date of birth.

When there is a match the receiving organisation can make a request for information about the suspect via the formal channels of mutual legal assistance. This request will be necessary to be sure that the sending organisation indeed knows the particular suspect, especially when the sensitivity of the system is set low. With a low sensitivity the chance for a false positive is high. Therefore a match is only an indication that the sending organisation knows the suspect, not a guarantee. In addition – even with a high sensitivity – the knowledge that some person is likely to be regarded as suspect in a foreign jurisdiction can generally only be seen as starting information for a further investigation. The evidentiary value of a match in itself is low. Only in response to the request for mutual legal assistance more (and more detailed) information can be received.

2.10 Conclusion

This chapter considered the technical aspects of FCInet. It attempted to answer the first research question, 'In what way does FCInet operate and which methods does it use?' Some general characteristics of FCInet are striking. It has a decentralised design, allowing one participant to send data (filters) to another participant. The filters which are sent can be compiled according to preferences within the sending participant's organisation. The filters are compiled in such a way that the receiving participant only gains information on a person in case that person was already included in the database which the receiving participant uses to check for a match. The information which is gained by the receiving participant in case a match occurs with a person's data, is the fact that that person is very probably also known by the sending participant. A match never offers complete certainty of that fact, however, due to the applied sensitivity settings.

3 Data Protection within FCInet Operations

3.1 Introduction

This chapters aims at answering the second subquestion identified in this research project, which reads: 'Which data protection rules apply in the context of FCInet and what do they entail for the exchange of data as envisaged in the project?' In order to answer this question, this chapter will firstly elaborate on the legal characterisation of the data which is exchanged within FCInet. Secondly, the chapter discusses previous research on the protection of personal data which was exchanged using comparable technology. Thirdly, the chapter focuses on the concept of pseudonymisation and the use of additional information. Fourthly, this chapter will assess which rules on data protection apply to the activities that FCInet employs, given the characterisation of the data.

An essential starting point for this chapter is the fact that within FCInet, various participants from many countries collaborate, which do not necessarily share one single legal framework for matters of data protection. However, a number of FCInet participants is located in the European Union, and as a consequence EU law applies to these participants. This is relevant, because EU data protection law is arguably one of the most advanced frameworks for data protection in the world, and can be viewed as something of a standard for other legal frameworks. This is particularly the case since, in May 2018, the EU General Data Protection Regulation (GDPR)[26] entered into force. Since that moment, authorities of EU Member States are directly bound by the GDPR. Even before the GDPR entered into force, EU law exerted a strong influence on national data protection laws within the European Union. This was seen both in criminal law matters, where the EU adopted a Framework Decision in 2008,[27] as well as outside the criminal law sphere, where the EU adopted a Directive in 1995.[28] The GDPR has replace this 1995 Directive, while the 2008 Framework Decision has been replaced by the Law Enforcement Directive (LED).[29] This latter legal instrument is of notable importance for any processing of data within the criminal law domain.

The cooperation within FCInet is not restricted to EU Member States, so the framework laid down in the GDPR and its accompanying LED does not apply to many of the participating authorities. The exchange of information between an EU Member State and a non-EU Member State is however still covered by EU law, as the relevant EU legislation includes rules on exchange of information with third countries. The exchange of information between two non-EU countries is not covered by EU law. Specifically for these bilateral relations, other legal frameworks exist, among which of course national laws of the participating countries, but also some other, non-EU international legal instruments. The most relevant of those is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and its associated Protocols.[30]

—

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[27] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

[28] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[29] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[30] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, and the Additional Protocol to the Convention for

3.2 Character of the data

Within FCInet, a financial investigation unit shares a filter which is based on the encrypted and aggregated personal data of the relevant suspects in a national database. The question can be asked whether this filter should be seen as personal data. If this is the case, the rules about data protection are applicable. Alternatively, the filter could be regarded as containing non-personal or anonymized data, in which case the rules on the protection of personal data do not apply.

A preliminary question is, which definition of 'personal data' should be used in order to decide on the question whether or not FCInet processes personal data. In this report, we have chosen to use the definitions used by the European Union in the GDPR and its accompanying LED, since these legal instruments can be seen as the current standard in data protection law, and are applicable to a large part of FCInet operations.

Personal data is defined in Article 4(1) of the GDPR as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[31] It is clear that FCInet uses names and dates of birth of natural persons. As such, these are identifiers relating to a natural person.

A completely different question is whether a particular person can be identified on the basis of the filter that is the result of the encryption and aggregation process. In an encrypted form the personal data of the person involved is not directly accessible. In this way, the consequences of a data breach remain very limited as someone who is able to secure a filter is not able to gain any knowledge from it. It is however another issue whether it can be convincingly held that sharing the filter between partners in FCInet constitutes an exchange of anonymous data. The data could perhaps be characterized as anonymous, but it could also be classified as 'pseudonymised' data. These are personal data which cannot be used to identify the person to which they relate by an accidental user of the data, but they can be used to identify the person to which they relate by a user who possesses additional information. In other words, is the personal data used in FCInet encrypted in such a manner that no natural person can be identified on the basis of the filter or is identification still possible?

3.3 Previous discussions of ma³tch

The Ma³tch technology claims it enables the autonomous and anonymous analysis of personal data. Hence the reference to the three a's in its name. The anonymisation techniques it uses are non-trivial, in the sense that 'it is impossible to distinguish or link' the encrypted, minimised and aggregated data to individual personal records.[32] According to Balboni and Macenaite in a paper about the use of ma³tch-technology in the context of FIU.NET, the anonymising technology allows 'to perform link and analysis among data sets without disclosing personal data'.[33] They claim further that 'Ma³tch compares completely anonymous profiles and therefore arguably no personal data are processed. As a result, data protection duties and obligations fall away'.[34] To understand and critically evaluate this position it is necessary to look into their argumentation.

—

the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8 November 2001.

[31] Regulation (EU) 2016/679. In Article 2(a) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) personal data is defined as: 'any information relating to an identified or identifiable individual ('data subject')'.

[32] Kroon 2013, p. 26.

[33] Balboni & Macenaite 2013, p. 334.

[34] Balboni & Macenaite 2013, p. 338.

Balboni and Macenaite start with giving a definition of personal data. They discuss the distinct elements of the definition of personal data, as are laid down in Article 4(1) of the GDPR: 'any information relating to an identified or identifiable natural person'.[35] Noticeable is their elucidation of the concept 'identified' or 'identifiable'. In their elucidation, Balboni and Macenaite follow the GDPR in stating that identification has to be understood in a broad sense.[36] Identification means 'distinguishing a person from other members of the group'.[37] Balboni and Macenaite discuss Opinion 4/2007 of the Article 29 Working Party about the notion of identification, which can be found in recital 26 of the GDPR. This Opinion states that 'to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly'.[38] The criterion of 'reasonably likely to be identified' can be explained, according to the English Information Commissioner, as meaning that 'the risk of identification must be greater than remote'.[39]

Subsequently, Balboni and Macenaite delve into the concept of anonymous data. They define anonymous data as data that 'originally or after being processed, cannot be directly or indirectly connected to an identified or identifiable individual'.[40] This fits the elucidation of anonymous information in recital 26 of the GDPR: 'namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'.[41] The English Information Commissioner defines anonymous data similarly as 'data that does not itself identify any individual and that is unlikely to allow any individual to be identified through its combination with other data'.[42]

After this general definition of the concepts, Balboni and Macenaite narrow down the definition of anonymous data. They argue that data are sufficiently anonymised when 'the data cannot be reversed to the original identifying data'.[43] Irreversibility is not an absolute requirement. It is enough to establish that reversion will take an unreasonable effort. According to the Information Commissioner there is legal authority for the view that data could also be regarded as anonymous when the organisation that publishes anonymised data, that is, data in an anonymised form, still holds 'other data that would allow re-identification to take place'. As a consequence, the disclosure of anonymised data does not amount to a disclosure of personal data.[44]

To check whether the filters that are created with ma³tch are truly irreversible, and whether it is possible to re-identify an individual on the basis of the filters that are shared by a sending organisation, Balboni and Macenaite apply the 'motivated intruder'-test as developed by the English Information Commissioner. With this test they check 'whether a person, without any prior knowledge but wishing to achieve re-identification of the individuals to whom the information relates (a motivated intruder), would be able to do so'.[45] The motivated intruder can represent the receiving organisation within the framework of FCInet. After applying this test, Balboni and Macenaite conclude that it is unlikely that a motivated intruder can re-identify the individuals on which the filter was based. This is due to technical barriers and lack of other available relevant information.

—

35 Regulation (EU) 2016/679.

36 Balboni & Macenaite 2013, p. 336.

37 Balboni & Macenaite 2013, p. 335. See also Roosendaal 2013, p. 91.

38 Regulation (EU) 2016/679, recital 26; Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007, 01248/07, p. 15; Balboni and Macenaite 2013, p. 335.

39 Information Commissioner's Office 2012, p. 16.

40 Balboni & Macenaite 2013, p. 336.

41 Regulation (EU) 2016/679, recital 26.

42 Information Commissioner's Office 2012, p. 6.

43 Balboni & Macenaite 2013, p. 336.

44 Information Commissioner's Office 2012, p. 13.

45 Balboni & Macenaite 2013, p. 337.

Balboni and Macenaite also observe that none of the partners in a network would know that a receiving organisation used the filter and found a match until the regular process of information exchange starts.[46]

3.4 Identification and the availability of additional information

Having given a description of the argumentation of Balboni and Macenaite, it is possible to evaluate their arguments. The definitions used seem to be generally accepted and in accordance with international regulations such as the GDPR.[47] A striking turn in the argumentation is, however, the narrowing down of anonymous data to data which cannot be reversed to the original data. What is left unstated in this argumentation is the phrase *without the use of an official decryption device*. It can be submitted that it seems unlikely that someone is able to decrypt an FCInet filter into identifiable personal data without having inside information. However, this is hardly relevant in a context in which all partners of FCInet share the algorithms that transform the personal data of the sending organisation into a filter and compare the personal data of the receiving organisation with the filter. Of course it is important to protect the data against attempts to steal and hack this data by outsiders. But this is no reason to argue that the filter itself comprises anonymous data.

The fact that the personal data in the filter are hashed and made meaningless for a motivated intruder does not necessarily mean that it concerns anonymised data. The filter contains anonymised profiles of persons, which cannot be identified without additional information. However, the whole purpose of sharing filters within FCInet is that the receiving organisation can discover whether a particular person (or other information) likely is known to the sending organisation. By enabling that, FCInet is meant to convey to the recipient some additional information as long as the recipient already has some knowledge (about for example a person) to start with. The consequence of a positive match thus is that the receiving organisation gains additional personal data about the natural person involved: the recipient is informed that there is a significant chance that this person may be also a person of interest in an investigation within the sending organisation's jurisdiction. This is in fact the information conveyed when using FCInet and in case that use leads to a match in the filters.

The observation of Balboni and Macenaite about the fact that the sending organisation does not know whether the receiving organisation got a match is in this respect irrelevant. It is not the sending but the receiving organisation that gains additional personal information. Firstly, when a match occurs this personal information concerns the likelihood that the relevant person (or certain personal information) is known to the sending organisation's country. In addition, all information about the specificities of the filter – that is the selection criteria that the sending organisation used when creating the filter – are also transferred to the receiving organisation. When these filter selection criteria are known to the recipient, the extra information that the recipient gets following a match is this: for the person (or certain personal information) matched, the filter selection criteria that the sending organisation applied are true. For example, when a filter is based solely on persons suspected of VAT-fraud, a match conveys the information that the sending organisation knows the person AND that the sending organisation knows him in connection to VAT-fraud.

A match may of course be followed up by extra information requests. Those follow up requests then provide for additional information on the relevant person, on top of the information that was gained because of a match. For good reason the European Council stated – in the context of another hit/no-hit system – that 'a hit/no hit system provides for a structure of comparing anonymous profiles, where *additional personal data* is exchanged only after a hit [emphasis added]'.[48] The match itself already conveys information, perhaps not much, but still enough to start a further information request.

—

[46] Balboni & Macenaite 2013, p. 338.

[47] Regulation (EU) 2016/679.

[48] Council Decision 2008/615/JHA recital 18.

Moreover, it is exactly the purpose of FCInet to lay sufficient ground for further investigations by informing a participating organisation of persons that have a presence in a database of one of the other participating organisations.

In FCInet, the receiving organisation can use the received filter indirectly – via the algorithms of ma³tch – to identify a single suspect in its database which likely corresponds with a person in the database of the sending organisation. A point of contention could be what this means for the nature of the filters. Do they contain data, which due to it being hashed is pseudonymised, but it still being personal data? Or would the filters contain data that is not personal data unless the receiving organisation discovers a match, upon which event the relevant information in the filter in question becomes pseudonymised personal data, with or without retroactive effect from the moment of sending? The research team did not reach consensus on this point. However, they agree on the fact that in case a match has occurred, the consequence is that (pseudonymised) personal data has been transmitted from the sending organisation to the receiving organisation.

Because the data are hashed/encrypted, the filter can be regarded as containing pseudonymised data at the most. In Article 4(5) of the GDPR pseudonymisation is defined as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.

The concept of pseudonymisation is further elaborated in recital 26: 'Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.'

The filter can consequently be classified as containing pseudonymised data, in one interpretation this holds from the moment of compiling the filter and including all subsequent processing of it, while in another interpretation this nature of pseudonymised data only holds from the moment a match occurs, and then applies retroactively from the moment of compiling the filter.[49] This has as a consequence that in any case for successful matches, the data has retained the character of being personal data. It would only lose this character if the persons to whom the data refer would be untraceable by anyone, even with access to additional information. Since pseudonymised data that has led to a match can by definition be traced to individuals, having used the available additional information in the form of the applicable algorithms, the data has not been anonymised and therefore should be regarded as personal data. This means that the data must be protected. The fact that the personal data of the persons involved are pseudonymised can however greatly contribute to reaching the appropriate level of protection. After all, pseudonymisation is a technique that can offer 'privacy by design'. According to recital 28 of the GDPR 'the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations'. Which data-protection obligations should be met will be assessed in the following paragraphs.

—

[49] Both interpretations could be reconciled with the idea that pseudonymised data is data that retains its character of being personal data even if it became pseudonymised. See EU Agency for Fundamental Rights 2018, p. 94-95.

3.5 Data protection rules

3.5.1 Applicable legal frameworks

A multitude of data protection rules apply to the type of data processing envisaged in FCInet. These rules are partly of a national nature and partly of an international nature. In national law, rules are laid down with regard to the processing of law enforcement data as well as to the processing of data for taxation purposes. The norms laid down at an international level mostly seek to influence these national legal regimes. Some of the international legal frameworks are however directly applicable on the national level in their entirety or in part.

National data protection laws within the European Union are to a large extent replaced by the GDPR.[50] This regulation is directly applicable to data processing within the EU, rendering national legal regimes mostly obsolete. This includes tax and customs matters. The GDPR is not applicable however to data which is processed in criminal law matters, which are covered by the Law Enforcement Directive,[51] the substance of which resembles the GDPR closely, but not completely.[52] This Directive replaces the current Framework Decision on data protection in the field of criminal law.[53]

The Regulation and the Directive will obviously not apply to processing of data which remains entirely outside the EU. That type of processing is included in FCInet when it concerns the exchange of information between participants completely outside of the EU. When two of these partners, both outside the EU, exchange information with each other, the GDPR and the LED will not apply (as long as FCInet itself is not based on EU law, which it currently is not).

Some FCInet participants outside the European Union are signatories to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,[54] and have ratified it. This applies to the United Kingdom, Norway and Iceland. These countries have also signed, but not yet ratified, the Additional Protocol to this Convention.[55] The Convention, for the parties to it that have also ratified the additional Protocol, provides a data protection framework that is comparable with the GDPR. The additional protocol was designed during the development of the GDPR and is intended to provide equal safeguards. It can be viewed as laying down a comparable standard, and paving the way for making adequacy decisions.[56]

Because of this and because of the fact that the GDPR is viewed as setting a worldwide standard for data protection, we will below primarily focus on the relevant aspects of the GDPR for FCInet operations. However, it is important to keep in mind that strictly speaking, the rules in the GDPR and the LED do not apply to all FCInet operations. Nevertheless, in order to keep the operation of FCInet manageable it would be advisable to design it with a single set of data protection rules in mind, and not choose for a flexible approach, in which there would be a specific set of data protection rules for each of the many bilateral relationships within the larger structure of FCInet.

3.5.2 Basic Concepts in the General Data Protection Regulation

The GDPR refers to the fundamental right of protection of personal data (Article 1(2)). This fundamental right is, in the context of the EU, laid down in Article 8 of the Charter of Fundamental Rights of the European Union. This fundamental right should

—

[50] Regulation (EU) 2016/679.

[51] Directive (EU) 2016/680.

[52] EU Agency for Fundamental Rights 2018, p. 31-

[53] Council Framework Decision 2008/977/JHA.

[54] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981.

[55] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8 November 2001.

[56] Bertoni 2021.

ensure that personal data is processed fair, for specific purposes, and on the basis of consent by the person concerned or, alternatively, on a legitimate basis in law. Data subjects have a right of access to their data and a right to rectify these data (Article 8(2) Charter of Fundamental Rights of the European Union). An independent authority is charged with supervising these rules (Article 8(3) of the Charter): the European Data Protection Supervisor.

The GDPR 'applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system' (Article 2(1)). However, its application is excluded, as mentioned before, when it concerns processing of personal data 'by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' (Article 2(2)(d)).

Personal data must be processed lawfully, fairly and in a transparent manner (Article 5(1)(a)). Perhaps more importantly from a practical perspective, the Regulation contains a quite strict principle of purpose limitation. This is clear from its wording, where it declares that personal data shall be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes' (Article 5(1)(b)). This principle takes as its starting point the purpose for which data was originally collected, and prohibits its further processing for other purposes which are incompatible with the original purposes. In this manner, two aspects of the purpose limitation principle can be distinguished: the limits to the purpose of collecting the data and the limits to the purpose of (further) processing the data.

According to the Article 29 Working Party, the central criterion of incompatibility requires an assessment on a case-by-case basis. Particular account must be taken of four key factors: 1) the relationship between the purposes for which the personal data have been collected and the purposes of further processing, 2) the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use, 3) the nature of the personal data and the impact of the further processing on the data subjects, 4) the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.[57] As this principle of purpose limitation is worded almost equally in the GDPR and in the LED,[58] the application of the principle in the context of FCInet will be discussed in the next paragraph.

Furthermore, the GDPR contains provisions on data minimisation (Article 5(1)(c)), accuracy (Article 5(1)(d)), storage limitation (Article 5(1)(e)), integrity and confidentiality (Article 5(1)(f)) and accountability (Article 5(2)). These general principles are regulated in detail in the remainder of the provisions of the GDPR. If the activities of FCInet come within the scope of the Regulation, it must be designed in such a way as to be compliant with all these provisions. Some of these provisions are identical to the provisions of the LED. As FCInet – at the start of project – envisaged the cooperation and exchange of information between law enforcement authorities on the one hand and fiscal authorities on the other hand, the principle of purpose limitation will be one of the most problematic aspects of data protection rules to deal with. We will deal with this in more detail in the next paragraph.

—

[57] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013.

[58] The difference being that Article 4(1)(b) of the Directive speaks of 'processing' while Article 5(1)(b) of the Regulation speaks of 'further processing'.

3.5.3 The Law Enforcement Directive

Directive 2016/680/EU (the LED) lays down the rules which will be applicable to data protection by criminal law authorities after their transposition into national law. This LED obliges Member States to 'protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data' (Article 1(2)(a)). Its rules relate to the 'protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' (Article 1(1)). This last provision is important, since it includes a statement on the purpose of data processing, and thereby informs the application of the principle of purpose limitation. Additionally, the LED also does not preclude the exchange of data for data protection reasons by Member States when they are obliged to do so by EU law or by national law. That means that data protection rules cannot stand in the way of EU-level or national level obligations to exchange data. An example of such an obligation can be found in Article 7 of Framework Decision 2009/960/JHA, obliging Member States to spontaneously exchange data under certain conditions. The LED is therefore not to be interpreted in such a way that the conditions that apply to the exchange of information as envisaged by the Framework Decision no longer apply. These conditions include for instance that the exchange of information takes place in order to 'assist in the detection, prevention or investigation of offences referred to in Article 2(2) of Framework Decision 2002/584/JHA'. This means that the Framework Decision does not oblige Member States to exchange information for other purposes, e.g. taxation purposes, for which reason also the provisions of the LED are not rendered ineffective in that regard.

The exchange of data by FCInet falls partly within the scope of the LED, since the exclusion provision of Article 2(3)(a) does not apply: as long as the legal basis for the exchange is found in EU law, the activity pursued on that basis automatically falls within the scope of EU law and consequently the LED applies if it concerns exchange of information of criminal matters. Data collected and exchanged for other purposes, such as tax, come under the application of the GDPR.

The primary principles relating to data protection are listed in Article 4 of the LED. This includes the obligation to process data lawfully and fairly. Importantly, it also includes the obligation to process data in such a way that it is 'collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes' (Article 4(1)(b)). This means that the objectives of the collecting of data have to be specified by national law previous to their collection, that is to say, sufficiently defined to implement any necessary data protection safeguards and to delimit the scope of processing. These purposes also have to be made explicit, that is unambiguous and clearly expressed. The purposes also have to be legitimate, that is: there must be a justified objective in collecting them.[59] These matters pertain mostly to circumstances lying outside the scope of FCInet. FCInet as such is not directly concerned with the initial collection of data by government authorities, but with the subsequent exchange of these data on an international level. Therefore, it is logical to focus on the other aspect of the purpose limitation principle: the further processing. Nevertheless, in order to be compatible with data protection law, the processed data should still be collected according to these rules. It is therefore important to ascertain whether the data which are used were initially collected for specific, explicit and legitimate purposes. Furthermore, it is advisable that the systems which are used to exchange data are designed in such a way that, as a part of the metadata of each piece of exchanged data, there is the possibility to indicate the purposes for which that piece of data originally was collected. In that way, there is the possibility to continuously monitor the lawfulness of further processing and the compatibility with the original purpose of collecting the data.

—

[59] This interpretation of the criteria: Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, p. 12.

If these purposes somehow become disconnected from the data, it is impossible to assess the compatibility of further processing.

As a rule, that future processing of data must not be incompatible with the initial collection of the data. Whether the exchange of data as envisaged by FCInet fulfils the conditions of the LED is not entirely clear, as assessing this compatibility requires a case-by-case assessment. Moreover, the data which are included in the exchanging participants' databases do not originate from data sources which apply one single purpose for collecting their data. Nevertheless, the LED seems to be based on the principle that all data collected for law enforcement purposes may be processed for law enforcement purposes.

When we apply the four key factors as described above in 3.5.2, it is clear that the problematic issues arise regarding the further processing for criminal law enforcement purposes of data which have been collected for tax administration purposes, and the other way around. This finding has already given rise to the separation of FCInet into two separate networks. The legal basis hereof will be reiterated in the following, including some thoughts for future developments. It is safe to say that it is possible that this mode of processing could lead to violations of the purpose limitation principle, as interpreted in the way described above, with the four key factors which were identified. It is for instance clear that the purpose for which police data have been collected is quite different compared to the purpose of applying tax regulations and ensuring the lawful collection of government taxes. Clearly, there is also not necessarily a reasonable expectation from the perspective of a taxpayer that the data which that taxpayer forwards to the tax authorities may later be processed for criminal law enforcement purposes. The impact which the further processing of tax data for law enforcement purposes can have on the data subjects is significant. It could lead to criminal investigations being started, and, if successful, to a criminal conviction and punishment.

If appropriate safeguards are applied these may counterbalance the aforementioned issues with the further processing of data for other purposes. One of these appropriate safeguards is pseudonymisation, a technique which is employed by FCInet.[60] Other safeguards may also be put in place, such as a clear respecification of the purpose of the data if the data is exchanged from a law enforcement authority to a tax authority or vice versa. All in all, it seems to be possible to abide by the purpose limitation principle, albeit is not very clearly how this could be done in general. When cross-domain exchange of information is going to be implemented, safeguards must be in place, and the exact design of these could be of possible benefit to FCInet. Especially when the safeguards are designed in such a way as to compensate as much as possible the cross-domain nature of the international exchange of information. However, for the time being it could be advisable to not implement cross-domain exchange until FCInet's design has dealt with these issues adequately, as well as for separate reasons discussed below.

The provisions in the LED are not directly applicable, and have to be transposed into national law. Only after transposition it becomes clear which data national authorities may use for which purposes after it has been collected. For a detailed account on the current provisions in national law implementing this purpose limitation principle, we refer to the chapters below that deal with national laws. There it becomes clear that national law provides significant hurdles for the exchange of information between criminal law enforcement authorities on the one hand and tax authorities on the other hand, because of the principle of purpose limitation. Consequently, the general cross-domain exchange of data between the participants in FCInet is legally difficult to implement. As long as the exchange of data takes place for purposes that are closely related to the purposes for which the data were collected, no obstacles are to be expected from the principle of purpose limitation on a case-by-case basis. Nevertheless, when the exchange of data takes place for purposes other than the purposes for which the data were collected, strong safeguards must be in place. Unless these are designed in such a

—

[60] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, p. 27.

way as to adequately counterbalance the cross-domain nature of the exchange, the principle of purpose limitation will provide a major obstacle to the lawfulness of this type of exchange of information.

What makes it even more complicated is that the processing of personal data for criminal law enforcement purposes falls within the scope of the LED, and consequently will be dealt with by national law, while the processing of data for purposes of applying the law on fiscal matters falls within the scope of the (directly applicable) GDPR. This also means that future developments which will make the exact meaning of the principle of purpose limitation more clear than it is now, will, in this cross-border context, initially only apply to the GDPR-side of the exchanging pair of authorities. For these reasons, it is strongly advisable to postpone the setting up the cross-domain exchange of personal data, awaiting future elucidations of this aspect of data protection rules.

Other requirements that the LED sets to the processing of data is that this processing must be adequate, relevant and not excessive in relation to the purposes for which it is processed (Article 4(1)(c)). FCInet can be believed to comply with this. This is the case because the data that is exchanged is not meaningful for the receiving participant with regard to data on persons that the receiving participant does not know. Therefore, only when data is relevant, it is revealed. This is really a proportionate way of processing information.

Data must be kept accurate, and up to date (Article 4(1)(d)). If not, it is to be rectified, or deleted. It therefore is obligatory that FCInet-participants agree to effective procedures and an adequate organisational design to ensure the accuracy of the data. This also applies to security of data (Article 4(1)(f)). This aspect is partly ensured by using pseudonymisation techniques: the data that is transferred is encrypted in such a way that data breaches will likely lead to meaningless information for persons who manage to intercept the communication. Nevertheless, there must also be an adequate system in place within the participating authorities in order to secure the additional information that is processed, and the computer systems which are used to match the data, because unauthorised access to these systems may inflict data security.

Time limits for the storing of data must be in place, because retention periods of personal data for the identification of data subjects should be no longer than is necessary for the purposes for which they are processed (Article 4(1)(e) and Article 5). An adequate system of retention periods, and possibly automatic deletion, should be designed. Since there is a preference to update the filters that are exchanged on a regular basis, i.e. once a week, there does not seem to be much need for a long retention period. Therefore it could be appropriate to program the system in such a way that there is a period of for instance six months after which a filter is automatically deleted from all systems.

Since pseudonymised data are also personal data, data subjects retain their rights over these data also after the data is encrypted (Article 13 and 14). This means that data subjects have the right to be informed about the ways in which their data is processed and by whom, the right to lodge a complaint with a supervisory authority, and the right to request access to the data, rectification of the data and erasure of the data. These rights must be enforceable by the data subject. This means that the data subject must be able to obtain from the controller of the sending and receiving organisation confirmation as to whether or not personal data concerning him are being processed. If these data are being processed, the data subject must have access to the personal data as such, and furthermore to the purposes for which they are processed, the recipients to whom the data have been disclosed, the right to complain about the processing, etcetera.[61]

Data subjects' rights may however also be to a large extent restricted under the conditions listed in Article 13(3) and Article 15 LED. The reasons for restricting access refer for instance to the obstruction of official investigations, or prejudicing the investigation of criminal offences or the execution of criminal penalties. When a data subject's request to have access to his personal information has been refused for one of

—

[61] The exact rights of the data subject are to be found in Article 14(a)-(g).

these reasons, the data controller of the sending or receiving organisation must respond to the data subject also of the reasons for refusing access, unless doing so would also undermine one of the purposes listed in the LED. In any case, data subjects must be informed of their right to seeking a legal remedy against the data controller's decision.

3.6 Conclusion

The technology used in FCInet enables the participating authorities to exchange their data and find matches. When a match occurs, the receiving participant gains some additional knowledge about a person or other topic on which the participant has some knowledge. The addition is the fact that this person or other topic is involved in proceedings in the sending participant's country.[62] The data that are exchanged therefore do not contain completely anonymised data, at least not when they lead to a match. Rather, the data have been pseudonymised, meaning that its contents are only accessible to the receiving participant if that participant has access to additional information. After all, it is the direct objective of FCInet to exchange information regarding persons by exchanging data, and as such it cannot be the case that the data which is exchanged could be characterised as anonymised. Therefore the data which is exchanged retains its character of personal data, either all the time since it started being processed. Alternatively, the data can be seen as anonymised as long as there is no match, but at the moment a match occurs the data becomes personal data and should retroactively be regarded as such.

This means that in principle, the activities of the participants in FCInet should comply fully with the applicable data protection laws of their respective countries as well as the internationally adopted and directly applicable rules. These rules include some lower standards (for instance in case of data breaches) for personal data which is pseudonymised. Of the other standards included in the data protection rules, the principle of purpose limitation is the most problematic one. The cross-domain exchange of personal data between tax authorities and criminal law authorities could run contrary to this principle. Whether this in fact will be the case, however, is to some extent dependent on the national laws of the countries of the participating authorities, which are discussed below.

Since most of FCInet's operations are covered by EU data protection law, the above analysis has focused on FCInet's compliance with that law. To some extent, FCInet operations are covered by other laws which may cause other standards to apply. For sake of simplicity, it may be advisable to adhere to GDPR and LED standards when designing the specificities of FCInet, as these regulations form an almost worldwide standard, among others closely followed by the Council of Europe Convention for the Protection of individuals with regard to automatic processing of personal data, and its accompanying protocol.

Data protection law is to a certain extent laid down in national laws, particularly in the criminal law domain as the LED governing the processing of personal data by criminal law authorities has to be implemented into national law. The processing of personal data for tax purposes will, as opposed to the processing for criminal law purposes, be directly subjected to the GDPR. This possible difference that can occur between the general GDPR-framework and the national implementations of the LED diminishes the certainty with which FCInet's activities can be deemed to comply with current and future data protection rules. The most problematic aspect of this is again the purpose limitation principle. That is an additional reason why FCInet should continue to

—

[62] The exact information which is gained is dependent on the inclusion criteria which define the content of the filters that are exchanged. If only personal data is included of suspects in criminal investigations, a match means to the receiving participant that the person who already was known to that participant is a suspect in a criminal investigation in the sending participant's country. In case the inclusion criteria for the filter are broader than that, a match gives less information to the receiving participant. The broader the filter is compiled, the less information it conveys.

not include possibilities for cross-domain exchange of information (i.e. exchange of information between tax authorities on the one hand and criminal law authorities on the other hand), at least until more clarity has been offered of the future national rules implementing the LED. As discussed in the introduction, this recommendation has been presented to FCInet in an early stage, and was duly acted upon. Therefore the design of FCInet incorporates the idea of separation of domains: there is one network for exchanging information in tax matters, and another network for exchanging information in criminal matters. Nevertheless, this idea of separation remains important now and in the future.

4 Exchange of Information in General

4.1 Introduction

Financial investigations units can exchange information through FCInet. Before going into the specific national legal frameworks for the exchange of information of the participating organisations, we give some general specifics of the public international and EU law contexts in which FCInet operates. This is done in paragraph 4.2. It is also necessary to elaborate upon two general aspects of the exchange of information. The first aspect is that information is exchanged in two stages: the sending of the filter by the sending organisation (as described in chapter 2) and the request for additional information by the receiving organisation after a 'hit'. Paragraph 4.3 focuses on the legal qualification of these two stages of information exchange. The second aspect is the legal domain in which the information is exchanged. The material scope of FCInet is not entirely clear, but it is safe to say that the information exchanged within FCInet is about financial matters. In addition, all participating organisations are public, governmental institutions and therefore FCInet functions wholly within the sphere of public law. To be a bit more specific, the information exchanged within FCInet seems to regard two general domains: tax matters and criminal investigations. Paragraph 4.4 addresses the possibilities to exchange information across these domains.

4.2 General aspects of relevant international law

4.2.1 The relevant public international law framework

Some general principles of public international law are of importance for the legal context in which FCInet operates. Such is the case for instance for the basic idea of sovereignty. In principle, all states are free to arrange their own affairs within their territory. They can limit this freedom by entering into treaties with other states or in any other way agree upon a certain issue. In international cooperation in criminal and administrative matters, treaties are often important because they lay down the rules that the parties will apply if they process a request for assistance coming from one of the other parties. This gives all parties to the treaty a certain guarantee as to how their requests will be handled, so they do not have to rely on mutuality or on goodwill from the other party. When having entered into such a treaty, the freedom not to comply with a request is therefore limited. In national law, for some forms of legal cooperation a treaty basis is necessary. This mostly regards the use of coercive measures. Most states prefer to apply these only when based on a request coming from a trusted source, i.e. a country with which the receiving state has concluded a treaty.

When international legal cooperation takes the form of the spontaneous exchange of information, there actually is no limitation of sovereignty involved. The receiving state just receives the information, and is not forced to act upon it in any way. The sending state, if it freely decided to send the information, does not see its sovereignty limited by that act. The only way in which this type of cooperation can be seen to limit a state's sovereignty, is when a number of states between them agree to send each other certain information when that information becomes known to them. If such arrangements are made, it is advisable to have a treaty basis for the spontaneous exchange of information, so that all the parties can rely on each other's cooperation in the matter. A treaty basis is much less necessary from the viewpoint of safeguarding essential civil liberties. Notwithstanding the fact that the sending of information will have some impact on the lives of individuals, this impact will remain rather limited compared to the application of coercive measures.

4.2.2 General requirements in European Union law

The law of the EU provides a slightly different legal order than is defined by general public international law. The legal order of the EU is based on a few principles, mostly laid down in primary law: the Treaties, the Charter of Fundamental Rights of the

European Union and the general principles of EU law. These include for instance the principle of attribution, according to which the EU is not competent to legislate upon a certain matter unless an explicit legal basis is provided in the Treaties. As regards the spontaneous exchange of information as envisaged in FCInet, a legal basis for introducing a harmonising legal instrument regulating FCInet under EU law, if that would be deemed advisable and opportune, can be found in Article 87 Treaty on the Functioning of the European Union (TFEU), which empowers the EU to establish police cooperation involving (among others) special law enforcement services in relation to the prevention, detection and investigation of criminal offences. These measures may include the exchange of relevant information (Article 87(2)(a) TFEU). This is a shared competence, not an exclusive one (Article 4(2)(j) TFEU). This means that the Member States may opt to act in these matters, until the EU chooses to do so. To the extent that the EU has not provided any rules yet, the countries participating in FCInet could conclude a new agreement to regulate their activities. However, there is some clear activity from the side of the European Commission in this regard. The Commission has communicated it wants to propose a new legal instrument codifying all EU law that pertains to police cooperation, among others the Schengen Implementing Convention and the Framework Decision on simplifying the exchange of information.[63] If it would be viewed desirable, this proposal from the side of the European Commission could be used to lay down a clear legal basis for FCInet in European Union law. At the least, as soon as there would be an EU Police Cooperation Code, FCInet regulations could be reviewed with the intent to line up with this new Code.

Another basic principle of EU law is the principle of sincere cooperation. This entails that the EU and the Member States should assist each other in the execution of their duties arising out of the Treaties. A very general duty to that end is laid down in Article 4(3) Treaty on European Union (TEU). A more specific duty can be found in Article 325 TFEU. This obliges Member States to act in certain ways in matters which concern the financial interests of the EU, notably fraud. To some extent Article 325 TFEU refers to measures which the EU should take, and thus it depends on concrete implementation measures and is not completely self-executing. That does certainly not count for the principle of assimilation (Article 325(2) TFEU): Member States must take the same measures in countering EU fraud as they do in countering fraud affecting their own interests. This means that, if the FCInet pilot project is to include fraud cases, it cannot exclude cases affecting the EU's financial interests. On a more general note, Article 325 TFEU has a wide scope, including all Value Added Tax (VAT) fraud, and can oblige Member States to no longer apply certain rules of criminal law, such as rules on the prescription of offences.[64]

Somewhat related to this is the problem of conflicts of jurisdiction. When parallel investigations and prosecutions take place, they can lead to violations of the principle of *ne bis in idem*, or in less serious cases to inefficient proceedings, probably also harmful from a defendant's point of view. There is much need for instruments that can detect parallel proceedings in an early stage, so that the authorities of the countries involved can coordinate their efforts.[65] The EU has not yet proposed any legislation to this end, but it is thought that new instruments regulating the settlement of conflicts of jurisdiction will rely on the principle of sincere cooperation, leaving it to the Member States to organise the way in which parallel proceedings are detected and acted upon.[66] Methods such as the one used in FCInet can in an early stage detect whether there are multiple ongoing investigations in which a person is regarded as a suspect.[67] An example

—

[63] Inception Impact Assessment for an EU Police Cooperation Code, Ares(2020)5077685.

[64] Court of Justice of the European Union, 26 February 2013, C-617/10, ECLI:EU:C:2013:105 (Åkerberg Fransson); Court of Justice of the European Union, 8 September 2015, C-105/14, ECLI:EU:C:2015:555 (Taricco).

[65] Eurojust News 2016.

[66] European Law Institute Special Report 2017.

[67] Simonato 2011, p. 220.

of a project in which FCInet technology is used to identify possible parallel proceedings is the CIDaR project, in which prosecutor's offices in Limburg (the Netherlands) and Limburg (Belgium) participate.

Also included in the basic framework of the EU are its rules on data protection. This is now a fundamental right (Article 8 of the Charter of Fundamental Rights), and the EU provides for a comprehensive legal framework for these matters in the General Data Protection Regulation.[68] Chapter 3 of this report has delved into data protection issues; therefore, these are not included in this chapter.

In addition to this, within the EU there has been some discussion on the allocation of competent authorities for purposes of the exchange of information. As is set out below, many international conventions and agreements have been concluded which offer possibilities for the parties to these conventions and agreements to spontaneously exchange information. Most of these instruments also include provisions on the character of the authorities that are competent to use these information exchange provisions. However, the instruments themselves hardly ever designate these authorities by name. They often designate categories, such as 'judicial authority', which excludes investigative authorities. It is left to the parties to specify which of its authorities may use the powers that the treaty offers to the state. Sometimes EU instruments require the Member States to notify an EU institution of their choice for a certain competent authority. Most Council of Europe Conventions allow the parties to the convention to issue declarations; sometimes these are used by the parties to designate specific authorities as competent.

This state of affairs creates a patchwork of competent authorities. In order to create clarity, the Council of the EU issued Guidelines for a Single Point of Contact for international law enforcement exchange.[69] These Guidelines aim to streamline international cooperation by reducing complexity and distributing information about Single Points of Contact (SPOCs) which are available for purposes of channelling information to and from other Member States. These SPOCs ideally are a combination of multiple bureaus, and they can be composed of staff coming from 'different services and/or Ministries, including criminal police, border guards, customs and judicial authorities'.[70] If a national authority is a competent authority for a certain type of international cooperation according to the international instrument and to its national law, it could therefore be incorporated in the SPOC by sending a delegation of its staff to be based at the SPOC, from where it performs its activities. Whether it would be a good idea to incorporate the type of information exchange that FCInet envisages into the national SPOCs is not so clear. There are good reasons to dedicate a specific channel to such a method of information exchange,[71] as is the case with FIU.net. This decision is separate from the availability of a legal basis for the information exchange. It is currently not very clear how the discussion on SPOCs will continue: there are proposals to link this topic to the abovementioned proposal for an EU Police Cooperation Code.[72] If this path is taken, there might at least be a much clearer and more comprehensive framework for the organisation of information exchange between criminal investigative authorities within the European Union.

A list of competent authorities for the instruments that are in place for international cooperation is also included in an addendum to the Manual on Law Enforcement Information Exchange,[73] in so-called 'national factsheets'.[74] This includes competent authorities for the different types of information exchange under the Prüm Decision, Eurodac, the Financial Intelligence Units, etcetera. This manual also includes a list of

—

[68] Regulation (EU) 2016/679.
[69] Council doc. No. 10492/14.
[70] Council doc. No. 6261/17, p. 33.
[71] Simonato 2011, p. 224.
[72] Council doc. No. 10985/21.
[73] Council doc. No. 5825/20.
[74] See Council doc. No. 5825/20 ADD 1.

notifications pursuant to Article 2(a) of Framework Decision 2006/960/JHA, which define the competent authorities for this so-called 'Swedish Framework Decision'. Also included is a list of bilateral agreements that continue to apply after the entering into force of the Swedish Framework Decision.

4.3 The stages of information exchange

4.3.1 Sending the filter: spontaneous exchange of information

An important question when it comes to assessing the relevant legal framework for FCInet is how to qualify the nature of the operations within FCInet. The position taken in this report is that the sending of the filter by a participating FCInet organisation can legally be qualified as spontaneous exchange of information. The spontaneous exchange of information is a specific way of international cooperation in legal affairs. It can be applied in administrative matters or in criminal matters. It can be defined as 'the provision of information to another contracting party that is foreseeably relevant to that other party and that has not been previously requested.'[75] When applied to FCInet, we can note multiple things.

Firstly, the spontaneous exchange of information regards the provision of information from one party to another. This is a one-way process. The term 'exchange' could include bilateral exercises, but this is not necessary at all. Rather than that, a spontaneous exchange of information consists mostly just in the sending of information by one party to another. There can be an expectancy of reciprocity, but this is not necessary for the successful supply of information. The cooperation is complete upon receipt of the information. The receiving party can thereupon act in such a way as it deems necessary, as long as the applicable national law enables it to do so.[76] The method of cooperation within FCInet conforms to this idea. A participant in FCInet generates filters on the basis of its database. Then, it sends the filters to one or more of the other participants individually. After that, these other participants can ignore the information or use it for the fulfilment of their tasks. Among other actions to be potentially taken, the receiving participant could send a request for additional information to the participant that supplied the information. In paragraph 2.2 we will discuss this second step in more detail.

Secondly, spontaneous exchange of information regards information. It does not concern the exchange of material to be used in evidence or the transfer of persons for purposes of standing trial or executing punishment. The fact that it concerns information, however, leaves many possibilities open.[77] In the context of the first stage of information exchange via FCInet the information that is exchanged concerns the information on which the filter is based, but only when there is a 'hit'. Because of the design of the software that is used to exchange this information (see chapter 2), the receiving participant is only informed of persons, events or other data known to the sending participant if the receiving participant already has the same information in his database about these persons, events or other data. In case there is a match, the receiving participant is informed about the fact that information that was already in its possession, being present in its database, may very likely also be known to the sending participant. This is all the information that is exchanged in this first step.

The nature of the information that is exchanged can change somewhat, depending on the way in which the participants define the makeup of their filters. Suppose that all participants would generate filters referring to persons who have been considered a suspect in an ongoing investigation. In case a match occurs, the receiving participant knows that the person in his database with regard to whom the match occurred may be a suspect in an ongoing investigation in the sending participant's country. Suppose,

—

[75] OECD Manual on the implementation of exchange of information provisions for tax purposes, module 2 2006, p. 3.

[76] Simonato 2011, p. 223.

[77] Simonato 2011, p. 223.

alternatively, that the participants in FCInet each generate a set of filters, each of which referring to persons suspected of a specific type of crime: one filter for money laundering suspects, one for corruption suspects, one for fraud suspects, etc. Suppose further that these filters are upon receipt cross-matched to all persons in the receiving participant's database. In that case, when a match occurs, the receiving participant knows that the person in his database with regard to whom the match occurred may be a suspect of a specific crime in the sending participant's state, for instance money laundering. Therefore, this approach enhances and increases the information that is exchanged between the participants. Of course it is also possible that the filters relating to a specific type of crime will only be cross-matched to persons in the database of the receiving participant which are associated with the same type of offence. This second approach does limit the number of hits, but it does not influence the nature of the transmitted information: the information is enhanced to the same extent as when it is cross-matched to all persons.

Thirdly, spontaneous exchange of information takes place from one party to another. It is thus not a multilateral process, but a bilateral, albeit that the flow of information is one-way only. The design of FCInet is such that the filters can be sent by each participant to some or all of the other participants individually. This happens at regular intervals, and preferably in a frequent manner (for instance, on a daily or weekly basis). When a participant receives a new filter from another participant, the previously received filter becomes obsolete and should be deleted. This procedure guarantees that each participant can make use at any given time of fairly recent information coming from the other participants. There is thus no central database that contains all the information available to the participants. However, the design of the network has a comparable effect of providing all participants with recently updated information at all times.

Fourthly, the spontaneously exchanged information should be potentially relevant to the receiving party. What is clear is that the mere fact that the sending party hopes the information will be usable for the receiving party does not make it information that is potentially relevant to the receiving party. But it is also not the case that information only becomes potentially relevant when the sending party legitimately believes that it will have a decisive role in an investigation, or that it will be used in evidence in a trial. Somewhere in between these extremes, the information changes from not even potentially relevant to definitely relevant. In the context of FCInet, a key aspect of the design is the fact that the receiving party can extract only those pieces of information out of the filter which is provided by the sending party if the receiving party already has that information about a person, event or other topic. Depending on the exact design of the filter, the information can be more or less specific. For example, the filter can contain data of a person who is, as a suspect or otherwise, involved in an investigation under the supervision of the sending party. Since the person is also known to the receiving organisation, there is most probably a need for usable information with regard to that person by the receiving party. Information about a specific suspect can be used for purposes of arrest, freezing of assets, exchange of evidence, or to take the investigation further. It can therefore be held that the information conveyed by the filter after a match is in principle potentially relevant to the receiving party. Information that will probably not have a relevance to the receiving participant will not be disclosed if the matching procedure is properly designed.

However, it depends on the information that the receiving organisation uses to match the filter with to decide whether the received (and matched) information in the filter is actually relevant. This is especially the case if the database of the receiving party that is used to cross-match a received filter includes persons, events or topics with regard to whom the receiving party does not have an immediate need for additional information. For instance, if convicted persons remain in the database even when their sentences have been completely executed, then there is no potential relevance for the receiving party to be informed of that person by the sending party. This is of course much less true in the reverse direction: information about already convicted persons may very well be relevant in an ongoing investigation, for instance for the purpose of taking recidivism into account

in sentencing. The database out of which the filters are generated may therefore contain data on persons which are no longer the subject of an ongoing investigation supervised by the sending party. If the character of spontaneous exchange of information is to be retained, the design of the databases that are used in generating the filters by the sending party and in cross-matching the received filters by the receiving party must have different inclusion conditions. The filters may be filled with data on persons known to the sending party, whereas the receiving party may only cross-match the filters to a database filled with data relating to persons with regard to whom additional information is of potential relevance.

Fifthly, spontaneous exchange of information takes place without a previous request by the receiving party. This aspect differentiates this type of international cooperation from the more standard types of mutual legal assistance, where a request from a party forms the incentive for the sending party to supply the information. The design of FCInet clearly incorporates this aspect. The participants in FCInet send each other the filters they generate without having to be requested to do so. FCInet's design does not seem to include a procedure by which a participant can request another participant to send an updated filter (or a filter generated in accordance to specific wishes). If FCInet would incorporate such a procedure, the nature of the international cooperation would change: such a specific request and the processing of it would be characterised as a form of mutual legal assistance based upon request.

The fact that an organisation participating in FCInet agreed to supply information does not change the spontaneous character of the exchange. The agreement to spontaneously supply information that could be relevant for the receiving organisation should not be regarded as a request for information, since that would mean it is impossible to make international agreements about the spontaneous supply of information. Instead those international agreements should be regarded as a framework within which the supply of information without a direct request is regulated. The fact that such frameworks are quite common is illustrated by the existence of provisions for the spontaneous exchange of information in several international instruments on cooperation in criminal and administrative matters, such as the Convention on Mutual Administrative Assistance in Tax Matters, the EU Directive on administrative cooperation in the field of taxation, the second protocol to the European Convention on Mutual Assistance in Criminal Matters, the Convention Implementing the Schengen Agreement, the 2000 EU Convention on Mutual Legal Assistance and the Swedish Framework Decision.

Sixthly, spontaneous exchange is no automatic exchange. According to the website of the OECD the automatic exchange of tax information is "the systematic and periodic transmission of tax information by countries to the residence country concerning various categories of income, such as dividends, interest, gross proceeds, royalties, salaries, pensions, etc".[78] In Article 3(9) of Directive 2011/16/EU on administrative cooperation in the field of taxation 'automatic exchange' is defined as "the systematic communication of predefined information to another Member State, without prior request, at pre-established regular intervals." The same definition can be found in Article 2(l) Council Regulation 904/2010 on administrative cooperation and combating fraud in the field of value added tax.

The exchange of information via FCInet can very likely not be characterised as a form of systematic communication of predefined information, without prior request, at pre-established regular intervals. As long as FCInet leaves considerable scope for deciding on the specific modes of information exchange, the timing and the inclusion of certain categories of data, the exchange will not come within the category of automatic exchange and the rules on spontaneous exchange of information will apply.

—

[78] 'Exchange of information', oecd.org, online last visited 12 August 2021.

4.3.2 Alternative view on foreseeable relevance

The standpoint mentioned above, that the method for exchange of information that is employed in the exchange of filters within FCInet can be classified as the spontaneous exchange of information, is not shared across the board. There is also an alternative view, which differs in the interpretation of the necessary requirement of foreseeable relevance. This is the position that the research team received from the Canadian participating organisation. This alternative view holds that, in order for the exchange of filters to be classified as spontaneous exchange of information, the sending organisation must have a strong basis to support that all the information in the filter has a foreseeable relevance to the receiving organisation before the sending organisation shares the filter. This view has two dimensions: this foreseeable relevance must exist with respect to each and every piece of information that is included in the filter, and this foreseeable relevance must exist with respect to the specific country for which the filter is created.

For this view, support is proposedly found in the Revised Explanatory Report to the Convention on Mutual Administrative Assistance in Tax Matters[79], in particular the explanation with regard to Article 7 of the Convention. This Explanatory Report characterises spontaneous exchange of information as occurring "when one of the Parties, having obtained information which it assumes will be of interest to another Party, passes on this information without the latter having asked for it."[80] There is some further support to this view in the Model Manual on Exchange of Information for Tax Purposes,[81] which refers to 'information that is foreseeably relevant to a foreign competent authority'.

The research team has discussed the merits of this alternative view and has not endorsed it, while acknowledging it, however, as a possible standpoint. The main reasons for this are the fact the foreseeable relevance as a criterion for the spontaneous exchange of information seems to have as its main function the prevention of fishing expeditions, disclosing the personal data of involved persons in an unwarranted manner. This function seems to be adequately attained by the design of FCInet, since it only discloses information to the receiving participant regarding persons that are already known to that participant. However, it remains important for FCInet if it wants to avoid the risk of engaging in fishing expeditions that is makes a careful selection of the personal data that are included in the filters, namely that it only should include data on persons with regard to whom there is a sufficient reason to disclose any data.

4.3.3 More information: information on request

The receiving organisation can use the received filter to check whether persons, events or other topics in its database are present in the filter. If there is a match it is likely that the sending organisation has more information about this person, event or topic. After a match the receiving organisation has to decide if it needs any additional information the sending organisation probably has. The match may be ignored, but if it is deemed necessary to gain additional information because of an ongoing financial investigation, the receiving organisation can ask the sending organisation for this information. This situation can be legally described as the exchange of information on request. According to the OECD "exchange of information on request describes a situation where one competent authority asks for particular information from another competent authority."[82] After the match the initiative to take action shifts, but the direction in which the information flows remains largely the same. The receiving organisation becomes the requesting organisation and the sending organisation becomes

—

[79] Revised Explanatory Report to the Convention on Mutual Administrative Assistance in Tax Matters as Amemded by Protocol, https://www.oecd.org/ctp/exchange-of-tax-information/Explanatory_Report_ENG_%2015_04_2010.pdf.

[80] Paragraph 1 of the explanations on Article 7 of the Convention.

[81] OECD 2021.

[82] OECD Manual on the implementation of exchange of information provisions for tax purposes, module 1 2006, p. 2.

the requested organisation. The information, however, is going mainly from the sending/requested organisation to the receiving/requesting organisation, except for the fact that the sending/requested organisation gets the information that the receiving/requesting organisation has information about a person, event or other topic that the sending/requested organisation has also information about.

It is possible to divide the request for information into two substages. In the first substage the receiving organisation can ask the sending organisation whether the match is genuine and the sending organisation truly has information about a person, event or other topic. As mentioned in chapter 2 it is possible that the match is a false positive, and therefore it is possible that after a match the sending organisation does not in reality have any information about the person, event or other topic in question. Although such a verification request is simple - and possibly easily integrated in the FCInet technical infrastructure - it still has to be regarded as information on request, because with this question one authority asks another authority for specific information. The second substage is then that the requesting organisation, after a confirmation of the match, can send a follow-up request for additional information the requested organisation has about the person, event or topic in question.

A request for information must be done by a competent authority. The request can only be done to another competent authority. Whether the participants of FCInet are competent authorities depends on the national distribution of competences and the available international frameworks. The procedures that need to be followed depend on the domain the information is exchanged in, and subsequently on the international and national rules regarding the exchange of information on request within this domain.

4.4 The domain in which the information is exchanged

4.4.1 Scope and domains

In choosing to use FCInet, participating organisations wish to exchange information that is relevant for financial and/or criminal investigations. From the beginning of FCInet, various organisations with different tasks and different responsibilities have participated. The scope of FCInet is therefore not entirely clear, and is not restricted to criminal investigations, or a particular type of criminal offences, since it also clearly includes matters of taxation. This creates confusion over the scope and goals of FCInet and makes it difficult to define its material reach and, accordingly, the applicable national and international legal frameworks.

Finding the commonalities in the participating organisations can create some clarity as to the scope of FCInet. These commonalities can be found in the answered questionnaires. All participating organisations are public, governmental organisations. This means that only public law provisions are relevant for the exchange of information through FCInet. All participating organisations are tax authorities or are somehow connected to tax authorities. All participating organisations are willing to exchange information. The sources of the information that is to be shared can differ. Most organisations primarily possess information to be used for the administration or enforcement of their domestic laws concerning taxes.[83] Other organisations (also) have gathered the information during the investigation regarding some or all sorts of financial and economic offences such as tax fraud, subsidy fraud, customs fraud, insider trading, bankruptcy fraud and money laundering.

All participating organisations wish to use the information exchanged within FCInet for investigation purposes. The goal of these investigations can differ. Most organisations want to use the information for the purpose of the administration or enforcement of their domestic laws concerning taxes. Other organisations (also) want to use the information for the purpose of the investigation of some or all sorts of financial and economic offences

—

[83] Using the words of Article 4 Convention on Mutual Assistence in Tax Matters and Article 3 of EU-Directive 2011/16/EU on administrative cooperation in the field of taxation.

such as tax fraud, subsidy fraud, custom fraud, insider trading, bankruptcy fraud and money laundering.

4.4.2 Cross-domain exchange of information

Broadly speaking, within FCInet information is exchanged to be used for financial investigations by public authorities. It is common that the domain of public law is divided into two separate domains: administrative law and criminal law. When information is gathered and/or used for the purpose of the administration or enforcement of their domestic laws concerning taxes, the information is in the administrative law domain (and more specifically in the tax domain). When information is gathered and/or used for the purpose of the investigation and prosecution of criminal offences the information is in the criminal law domain. However, the subdomain of criminal tax matters breaches this dichotomy between administrative and criminal law. On one hand, the enforcement of tax laws can be seen as part of the tax domain. On the other hand, the investigation of criminal offences is clearly part of the criminal law domain. It is therefore necessary to treat the domain of criminal tax matters as a field of law sui generis.

When two organisations exchange information, a distinction can be made between the purpose for which this information was gathered by the sending organisation and the purpose for which the receiving organisation wants to use the information. When the information is gathered and subsequently used for the same purpose, the information stays within the same legal domain. When the information is gathered and subsequently used for different purposes, the information crosses domains.

The starting point of national and international provisions regarding the exchange of information from one organisation to another, is that the information stays within the same domain. The cross-domain exchange of information is an exception, surrounded with additional provisions that act as safeguard against the unchecked use of information by the government. Especially data protection regulations contain purpose limitation provisions that prevent the unlimited re-use of gathered information for other purposes than it was gathered for. But international agreements regarding cooperation usually are also focused on the exchange of information to be used for a specific purpose. Only as an exemption can the cross-domain use of information sometimes be allowed. The possibilities for the cross-domain use of information are often lopsided. Regularly, information gathered for taxation purposes can be used in criminal investigations but not vice versa. Even then, in the context of the international exchange of information the crossing of domains often requires a case specific assessment and authorisation.

The field of criminal tax matters comprises an exemption to the rule that the cross-domain use of information is not allowed. Especially the Convention on Mutual Administrative Assistance in Tax Matters allows the exchange of all information regarding tax matters, including criminal tax matters. The Convention places no limitations on the use of information gathered for the administration of taxes for the purpose of the criminal enforcement of tax laws. Although less likely, the use of information gathered for criminal tax matters seems also to be allowed. Nevertheless, because the criminal enforcement of tax laws should be regarded as the investigation or prosecution of criminal offences, another data protection regime is applicable - at least within the European Union. The consequence of this is that criminal tax matters fall partly under the regime of administrative law provisions and partly under the regime of criminal law provisions.

4.5 Conclusion

The general international and EU legal framework within which FCInet operates gives the participants much freedom to operate. It does give them some obligations to cooperate and sets some limits, however. Particularly the EU framework could change notably in the future, if an EU Police Cooperation Code will be adopted. In that case, much of the information exchange between EU law enforcement authorities will be regulated in that Code.

The exchange of information via FCInet comprises two stages. In the first stage filters are sent by the sending organisation to the receiving organisation. This can be regarded as the spontaneous supply of information, because the filter is supplied from one organisation to another, the filter contains information which can be deemed relevant for the receiving organisation after a hit, the filter is sent without a prior request and information conveyed is not predefined information that is systematically shared. In the second stage the receiving organisation can decide to request additional information. This can be a verification of the match, as well as additional information about the subject. These can be regarded as an exchange of information on request. The receiving organisation becomes, for purposes of the additional exchange of information, the requesting organisation and the sending organisation becomes the requested organisation.

The information exchanged via FCInet can regard two legal domains: administrative (tax) law and criminal law. The starting point is that legal information stays within a given domain. The further use of information for other purposes then it was acquired for is only allowed as an exception. Therefore, a standardised cross-domain exchange of filters between international partners is not possible or very difficult to implement at least. Exception to this is the domain of criminal tax law. It seems possible to exchange tax information gathered for the administration of taxes to be used in criminal investigations and prosecutions of criminal tax offences in other states.

5 Exchange of Information in Tax Matters

5.1 Introduction

Several participating organisations want to use FCInet to exchange information for the purpose of the administration or enforcement of their domestic laws concerning taxes. This chapter is about the international and national legal framework for the exchange of information regarding taxes. In the second paragraph the international framework will be described. All states in which the participating organisations reside are signatory to the Convention on Mutual Administrative Assistance in Tax Matters. The main focus will therefore be on this Convention. In addition to this, attention will be given to some European Union legislation, since this is relevant for all participating organisations in EU member states. Some data protection topics will be discussed in the third paragraph. In the fourth paragraph some remarks about application of the international legal instruments within the national legal order will be made.

5.2 Convention on Mutual Administrative Assistance in Tax Matters

The Convention on Mutual Administrative Assistance in Tax Matters was developed by the OECD and the Council of Europe in a joint effort. The Convention was developed in 1988, entered into force in 1995 and was amended by a Protocol, entering into force in 2011. The Convention, in its amended form, has entered into force for Australia, Belgium, Canada, Denmark, Finland, Iceland, the Netherlands, Norway, Sweden, and the United Kingdom. The United States has signed the protocol, but it has not yet entered into force. Therefore, for the United States the original version of the Convention still applies, and the relevant differences will be mentioned. Obligations in this treaty in principle only apply to tax authorities.

The Convention applies to most kinds of taxes, except custom duties (Article 2). This includes income, profit and wealth taxes, but also property taxes and value added taxes. The object of the Convention is the administrative assistance between States in tax matters (Article 1). According to the Commentary on Article 1 of the Convention "such assistance comprises all mutual assistance activities in tax matters which can be carried out by the public authorities, including the judicial authorities".[84] Assistance can comprise the exchange of information (Article 1(2)(a)). This includes the exchange of information in criminal tax matters.[85] In the original version of the Convention it was provided that information under this Convention could only be used as evidence in a criminal court if prior authorisation was given by the supplying party (Article 4(2) old). This is no longer necessary, except for the United States. Therefore, as far as it concerns criminal tax matters there is no strict separation between the administrative law and criminal law.

As a general rule, all signatories agree to exchange any information that is foreseeably relevant for the administration or enforcement of their domestic laws concerning the taxes covered by the Convention (Article 4(1)).[86] The scope of this article is wide and "is intended to provide for exchange of information in tax matters to the widest possible extent".[87] Nevertheless, 'fishing expeditions' or requesting information that is unlikely to be relevant fall not under the scope of this Convention.

It is important to note that Article 4 is worded not as a competence, but as an obligation. Therefore the competent authorities are obliged to share all foreseeable relevant tax information with each other. There are five main methods of exchanging information.[88] For the exchange of information via FCInet two of them are relevant. In stage 1, filters are spontaneously and without request sent by the sending organisation:

—

[84] Commentary on the provisions of the Convention, p. 35 (under 9).

[85] Commentary on the provisions of the Convention, p. 35 (under 10).

[86] In paragraph 4.3 some additional remarks about the foreseeable relevance of tax information will be made.

[87] Commentary on the provisions of the Convention, p. 45 (under 50).

[88] Commentary on the provisions of the Convention, p. 45-46 (under 51).

this is the spontaneous supply of information. In stage 2, the receiving organisation can - after a match - request additional information. This is the exchange of information on request.

Concerning the spontaneous supply of information - such as the spontaneous supply of filters via FCInet - the Convention includes a provision on the spontaneous exchange of information between the Parties to the Convention (Article 7(1)). The provision reads:

> A Party shall, without prior request, forward to another Party information of which it has knowledge in the following circumstances:
> a) the first-mentioned Party has grounds for supposing that there may be a loss of tax in the other Party;
> b) a person liable to tax obtains a reduction in or an exemption from tax in the first-mentioned Party which would give rise to an increase in tax or to liability to tax in the other Party;
> c) business dealings between a person liable to tax in a Party and a person liable to tax in another Party are conducted through one or more countries in such a way that a saving in tax may result in one or the other Party or in both;
> d) a Party has grounds for supposing that a saving of tax may result from artificial transfers of profits within groups of enterprises;
> e) information forwarded to the first-mentioned Party by the other Party has enabled information to be obtained which may be relevant in assessing liability to tax in the latter Party.

Article 7 of the Convention provides a legal basis for the spontaneous exchange of information between tax authorities. It therefore also provides a legal basis for the supply of filters to the participating organisations via FCInet. Especially the first circumstance - the possibility of loss of tax - does give much room for the exchange of information. This circumstance requires grounds for the supposition that the information can be relevant in the assessment of the receiving party whether there may be loss of tax.[89] These grounds need to be present before the information is conveyed. This, however, does not mean that the grounds need to be present at the moment the filter is built and sent via FCInet. Since information within the FCInet system is only conveyed when there is a match, the match provides the grounds for the supposition that the conveyed information is relevant. Only after a match occurs, the organisation that receives the filter also receives any information. It could be seen as one of the advantages of the FCInet system that it in fact renders superfluous the prior assessment of the potential relevance of any information for a foreign partner.

Article 5 of the Convention covers the supply of information on request. In stage 2 of the exchange of information the receiving organisation may - if he wishes so - react to the match by requesting additional information from the sending organisation. This additional information can be the verification whether the person, company or other topic that matched is indeed known to the sending organisation and (if so) can also include the request to provide all or some of the information it has regarding the person, company or other topic. According to Article 5(1) "at the request of the applicant State, the requested State shall provide the applicant State with any information (...) which concerns particular persons or transactions."[90] If the requested information is not directly available, the requested State shall "take all relevant measures to provide the applicant State with the information requested" (Article 5(2). For the FCInet system this seems to be less relevant, since the match already indicates that the sending (and requested) organisation does have some information about a person, company or other relevant topic. The requested organisation shall respond as soon as possible to this

—

[89] In paragraph 5.5.3 some additional remarks about the foreseeable relevance of tax information will be made.

[90] Some exceptions to this obligation can be found in Article 21 of the Convention.

request (Article 20). Therefore, the Convention also provides a basis for the exchange of information on request to the participating organisations via FCInet.

5.3 European Union instruments

5.3.1 Introduction

The Convention on Mutual Administrative Assistance in Tax Matters gives a full and sufficient basis for the spontaneous supply of filters regarding tax matters and for the exchange of information about tax matters on request. This is the primary basis organisations participating in FCInet can use. For the sake of completeness, some EU instruments will be discussed in the following. These instruments are only relevant for participating organisation residing in EU member states. Starting point is that all EU member states have implemented these instruments into their legal order, and the rules in these instruments are therefore als applicable to the tax authorities in these EU member states. Since these instruments have only a secondary value for FCInet, no further application of the rules will be made.

5.3.2 Council Directive on Administrative Cooperation in Taxation Matters

Council Directive 2011/16/EU on administrative cooperation in the field of taxation applies to all possible forms of tax within EU Member States, including taxes of the lower administrative levels of government, with the exception that Value Added Tax and customs duties are not included in its scope, as well as excise duties and social security duties (Article 2). As a Directive, it needs transposition in national law of the EU Member States to be usable by the national authorities. The Directive allows the spontaneous exchange of information (Articles 9-10) and the exchange of information on request (Article 5). It defines spontaneous exchange as 'the non-systematic communication, at any moment and without prior request, of information to another Member State' (Article 3(10)).

Spontaneous exchange of information is possible for information falling within the scope of the Directive, when it 'is foreseeably relevant to the administration and enforcement of the domestic laws of the Member States concerning the taxes' within that scope (Article 1(1) in combination with Article 9). The exchange shall take place between the competent authorities of two EU Member States, under the same circumstances as in the OECD Convention on Mutual Administrative Assistance in Tax Matters (Article 9(1)(a)-(e)). Since these circumstances are identical to the circumstances which are enumerated in Article 7 of the Convention on Mutual Administrative Assistance in Tax Matters, the Directive can be seen as a close incorporation of that Convention in the legal order of the EU. When one of these circumstances applies, there is an obligation for the Member State concerned to exchange the information, for the wording of the Directive is clearly imperative. Also, Article 10(1) requires the competent authority to which information is available under one of these circumstances, to exchange this information with the other Member State within a month after it became available. In addition to this obligatory spontaneous exchange of information, the Directive also gives a competence (not an obligation) for the competent authorities to exchange 'any information of which they are aware and which may be useful to the competent authorities of the other Member States' (Article 9(2)). After either the obligatory or the non-obligatory exchange has taken place, the receiving authority is under an obligation to confirm the receipt of the information (Article 10(2)).

On request, information will be provided to the requesting authority if this information is foreseeably relevant to the administration and enforcement of the domestic laws of the Member States concerning the taxes (Article 1(1) in combination with Article 5). If need be, the requested authority should perform additional administrative enquiries to obtain the requested information (Article 6). The requested information should be provided as soon as possible, and in case the requested authority already possesses the information this should be done within two months after the

receipt of the request (Article 7(1)). The requested authority should also confirm the receipt of the request.

5.3.3 Council Regulation on Cooperation in Matters of Value Added Tax

Council Regulation (EU) 904/2010 on administrative cooperation and combating fraud in the field of Value Added Tax lays down rules for the cooperation between EU Member States in their application of VAT laws. As a regulation, it does not need transposition in national law and is directly applicable by all national authorities tasked with the cooperation in VAT matters. It does not affect Member States' mutual legal assistance in criminal matters (Article 1(3)). The regulation is restricted to three types of information, all relating to its central subject-matter: 1) any information that may help to effect a correct assessment of VAT; 2) any information that may help to monitor the correct application of VAT, particularly on intra-Community transactions; and 3) any information that may help to combat VAT fraud.

The Regulation contains provisions about the exchange of information of request (Article 7-9). It also includes two separate schemes for 'exchange of information without request': automatic exchange (Article 14) and spontaneous exchange (Article 15). Article 13 contains some general provisions applicable to both schemes. The scheme for spontaneous exchange of information, according to Regulation (EU) 904/2010, is of a subsidiary nature with respect to the automatic exchange of information: it applies to any information which has not been exchanged automatically but which the sending competent authority considers to be possibly useful to the receiving competent authority. This information must also satisfy the general conditions for exchange of information without request. Firstly, the information must fall within one of the categories named in Article 1 of the Regulation. Secondly, one of the following cases must apply: a) taxation is deemed to take place in the receiving Member State and the information that is sent is necessary for the effectiveness of the receiving Member State's control system, b) there are grounds to believe that a breach of VAT rules has been committed or is likely to have been committed in the receiving Member State, or c) there is a risk of tax loss in the receiving Member State. Under these conditions, the spontaneous exchange of information on VAT matters is allowed under the Regulation.

In the Implementing Regulation it is provided that all information communicated pursuant Regulation (EU) 904/2010 shall be transmitted as far as possible only by electronic means through the CCN/CSI network, with a few renounceable exceptions (Article 6).[91] This provision could complicate the feasibility of a new network, separate from the CCN/CSI network but for the same purposes of exchanging information on VAT. On the other hand, it seems questionable whether such an Implementing Regulation could prohibit the use of other electronic systems, especially when the exchange of information is based on other international instruments (such as the OECD Convention).

In 2012, Regulation (EU) 904/2010 introduced the mechanism of 'feedback' in the exchange of information (Article 16). This possibility of feedback specifically applies to spontaneous exchange of information. According to the Regulation, the sending competent authority may request the receiving competent authority to provide feedback on the information. The Regulation does not contain further specifications as to what counts as 'feedback', but mostly this will relate to the usability of the information exchanged for the receiving competent authority. According to the Commission Report on the application of Regulation (EU) 904/2010, this possibility of giving feedback

—

[91] The European Commission adopted Commission Implementing Regulation (EU) 79/2012 laying down detailed rules for implementing certain provisions of Council Regulation (EU) No 904/2010 concerning administrative cooperation and combating fraud in the field of value added tax.

improves the application of VAT rules and encourages a greater level of spontaneous exchange of information.[92]

5.3.4 Convention on Mutual Assistance between Customs Administrations

The Convention drawn up on the basis of Article K.3 of the Treaty on European Union on Mutual Assistance and Cooperation between Customs Administrations was concluded in the framework of the former third pillar of the EU. This so-called 'Naples II' Convention replaces the 1967 Naples Convention, which provided a basis for information exchange between customs administrations. The Convention provides a legal basis for operational cooperation in cross-border criminal matters, enabling enforcement authorities in the EU Member States to cooperate in the fight against drug trafficking, arms smuggling and other forms of cross-border crime and fraud with goods. The purpose of the Convention is to strengthen the legal basis for customs cooperation in criminal matters between EU Member Staten. In addition, Naples II is used for the exchange of information for administrative and criminal purposes in the field of customs enforcement.

The Convention includes provisions on mutual assistance in Articles 8-18. In principle, the request for assistance and the replies are exchanged between the central authorities designated by each Member State's customs administration. Article 10 concerns the exchange of information on request and Article 17 concerns spontaneous exchange of information. Assistance on its own initiative must be granted within the scope of the powers of the authority providing this assistance, which is defined in national law (Article 15). The authorities are mutually obliged to send each other 'all relevant information concerning planned or committed infringements'. This could among others include personal data of subjects, as is envisaged in FCInet, when it concerns customs infringements or suspicions thereof.[93] There are also specific data protection provisions in the Convention (Article 25).

5.4 Data protection

When personal data is transferred to a third state from a European Union member state (or other state in which the GDPR and LED) are applicable), Chapter V of the GDPR should be complied with. For criminal tax matters Chapter V of the LED is relevant. According to Article 45 GDPR "a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country (…) or the international organisation in question ensures an adequate level of protection" (see also Article 36 LED). At the moment the Commission has taken an adequacy decision on the United Kingdom for both the GDPR and the LED.[94] However, for most non-EU Member States (in which the GDPR and LED are not applicable) the Commission has not taken adequacy decisions; not under the GDPR and not under the LED. Therefore, there are no adequacy decisions for Australia, Canada (as far as relevant) and the United States.

In the absence of an adequacy decision, personal data may nevertheless be transferred to a third country if there are appropriate safeguards in place. Such appropriate safeguards may be provided for by a legally binding and enforceable instrument between public authorities (Article 46(1) and (2)(a) GDPR and Article 37(1)(a) LED). The OECD Convention on Mutual Administrative Assistance in Tax Matters can be regarded as such a legally binding instrument. Whether the Convention indeed provides appropriate safeguards for the protection of personal data has to be decided by the participating organisations of the EU member states. In their considerations, other international and national provisions regarding the protection of

—

[92] Report from the Commission to the Council and the European Parliament on the application of Council Regulation (EU) no 904/2010 concerning administrative cooperation and combating fraud in the field of value added tax, COM(2014) 71, p. 7-8.

[93] See the Handbook for the Naples II Convention, Council doc. No. 13615/05, p. 15.

[94] 'Adequacy decisions', ec.europa.eu (online last visited 12 August 2021).

data in the non-EU receiving organisations should also be taken into account. Although the need for a decision about the data protection level is evident, the obligation in the Convention to share relevant tax information with other signatories presumes a charitable judgement. It is contradictory to promise to share information on certain conditions, and after the fact demand additional conditions. Therefore the position can be defended that the OECD Convention should indeed be regarded as a legally binding instrument that provides appropriate safeguards. In that case, this Convention can be used by EU Member States to exchange personal data about tax matters and criminal tax matters with third countries, without requiring any further authorisation of a supervisory data protection authority or informing this supervisory authority.

Article 22 of the Convention contains some provisions regarding the protection of personal data. Firstly under (1) the general principle is set out: "any information obtained by a Party under this Convention shall be treated as secret and protected in the same manner as information obtained under the domestic law of that Party and, to the extent needed to ensure the necessary level of protection of personal data". Under (2) the principle of purpose limitation can be found. Only "persons or authorities concerned with the assessment, collection or recovery of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, taxes of that Party, or the oversight of the above" are allowed to use the information received. This information may in principle only be used for these purposes. Given this provision, it is possible to use information gathered for the purposes of administrative tax matters for the investigation and prosecution of criminal tax offences, and vice versa. In addition, tax information may be used for other purposes when this is allowed under the law of the supplying state and the competent authority of the supplying state authorises such use (Article 22(4) Convention). Also the transmission of received information to a third party can be allowed by the competent authority of the supplying party.

5.5 Application of international legal instruments on national level

5.5.1 Implementation of international conventions

Whether international legal instruments apply directly in the state of the signatory depends on national law provisions. In some states international legal instruments are directly applicable. In other states international legal instruments have to be converted into national legislation. A middle course is that national legislation allows certain types of action when there is an explicit legal provision or international agreement. According to the questionnaires in the states of all organisations that wish to participate in FCInet the OECD Convention on Mutual Administrative Assistance in Tax Matters is directly applicable, is implemented in national legislation or provides the required international agreement. Therefore, in all states there is a national legal basis for the spontaneous exchange of tax information via FCInet.

5.5.2 Competent authorities

International obligations and competences can only be executed on behalf of a state if an organisation is competent to do so. The assignment of competences to certain persons or organisations is a matter of national policy. Based on the answers in the questionnaires most organisations that wish to participate in FCInet are a competent authority for the exchange of information regarding tax matters. In some states - especially Belgium and Norway - only certain sections of the tax organisation seem to be allowed to share certain kinds of information. Whether this is a problem remains to be seen. It primarily seems a practical matter to ensure that the right persons within the national organisation that wish to participate in FCInet get the (delegated) authority to spontaneously exchange information with FCInet partners.

5.5.3 Foreseeable relevance

Article 4 of the OECD Convention on Mutual Administrative Assistance in Tax Matters only allows the exchange of information that is foreseeably relevant for the

administration or enforcement of their domestic laws concerning taxes. The question arises when information is foreseeably relevant. In chapter 4 it is explained that the FCInet system helps with the determination of whether a particular piece of information is foreseeably relevant. Because information in a filter is only conveyed when there is a match, information about persons, events or other topics in the filter the receiving organisation has no knowledge about will not be disclosed.

However, there still remains the question which kind of information in general can be qualified as foreseeably relevant for the administration or enforcement of domestic tax law. There has to be a general understanding about which information is relevant between the participating organisations of FCInet - or at least between the two organisations that send and receive a filter. Is it for example relevant that the sending and receiving tax organisation know the same person? If so, does it matter whether the last moment of registered contact was more than five years ago or twenty years ago? If knowing the same person is not enough, what kind of information does need to be added in general? Should for example only filters be sent that contain information about persons who are registered as possibly fraudulent? And if so, may the receiving organisation match this filter with a database of all persons it knows, or only with persons regarding who there are indications of possible tax avoidance or fraud?

The text of the Convention on Mutual Administrative Assistance in Tax Matters seems to offer a broad definition of relevance, because all information that can help the administration or enforcement of domestic tax laws is deemed relevant. It could therefore be argued that all information about persons, companies, bank accounts, etcetera that one tax authority has is foreseeable relevant for another tax authority if that authority has the same person, company, bank account, etcetera registered. After all, when two tax authorities have information on the same person, company, bank account, etcetera it can be relevant to compare the information to see if there are inexplicable differences and to discover whether a person or company is paying double taxes or evades taxation. It is however also possible that this view, that all information that is known to two tax authorities in different states is foreseeably relevant, is seen as too broad.

When there are divergent views between the participants to FCInet about the categories of information that can in general be deemed foreseeably relevant for the administration or enforcement of domestic tax laws by the receiving tax organisation, it is advisable to come to a clear understanding about this topic. This understanding should be about the information a filter can be based on: which persons, companies, bank accounts, events, topics and other kinds of information can be used to create a filter. This understanding should also be about the information the filter can be used on: which persons, companies, bank accounts, events, topics and other kinds of information can be used to check whether there is a match. It is advisable to have a general understanding between all participants to FCInet on the issue of the topics on which information can be exchanged, so that filters can be compared to find matches. Although it is possible to make bilateral arrangements that apply solely between the organisation that sends and the organisation that receives the filter, when more organisations use FCInet it quickly becomes very complex to have different bilateral sets of rules about information that can be added to a filter or used to match with a filter depending on the partner in question.

5.5.4 Purpose limitation

The principle of purpose limitation holds that in principle information can only be used for the goals it was collected and processed for. In other words, information that is collected and processed for the purpose of the administration or enforcement of domestic tax laws should only be used for the administration or enforcement of tax laws. This information can in principle not be used for other purposes, such as the investigation and prosecution of criminal offences (other than criminal tax offences). An exemption to this principle can be found in Article 22(4) of the OECD Convention on Mutual Administrative Assistance in Tax Matters. The receiving organisations may use tax information for other purposes when the laws of the state of the supplying organisation allow for this use and the supplying organisation authorises such use. These

conditions confirm that the use of tax information for other purposes is indeed the exception. The conclusion can therefore be drawn that it is not possible for the cross-border exchange of filters, in which filters based on administrative (and criminal) tax information is used against a database with information about criminal investigations regarding non-tax (financial) criminal offences, such as money laundering or bankruptcy fraud.

5.6 Conclusion

There is an international legal basis for the exchange of information about taxes via FCInet. This basis can best be found in Article 4, 5 and 7 of the OECD Convention on Mutual Administrative Assistance in Tax Matters. All FCInet participants are signatory to (at least a version of) this convention, and in all states the convention is part of the national law. In addition EU Member States also can apply several EU instruments, though the Council Directive on Administrative Cooperation in Taxation Matters can be seen as an implementation of the OECD Convention into the European Union system of law. All participating organisations can be seen as competent authority - or at least contain a division that is competent.

The main question that still needs to be answered by the FCInet participants is how they understand the concept of foreseeable relevance regarding the information the outgoing filters are based on and incoming filters are used against. The OECD Convention seems to offer room for a broad explanation of foreseeable relevance, but participants may want to limit the information that can be shared. To enable a proportionate and balanced exchange of equivalent filters it is therefore advisable to come to a general understanding of the sort of information a filter can be based on and used against.

6 Exchange of Information in Criminal Matters

6.1 Introduction

A relatively small number of FCInet participants wish to use it for the exchange of information for the purpose of detecting and investigating criminal offences. There are some FCInet participants who have indicated that they wish to use FCInet to exchange information on criminal tax offences. To the extent criminal offences actually involve tax offences (e.g. tax evasion, filing of false returns, etc.), information on these can be exchanged through the instruments for administrative or legal assistance in matters of taxation. This is for instance the case with Iceland, Canada, Australia and the United States. The participating authorities from these countries all indicate that the acts classified as criminal offences that they have included in the FCInet system data all concern tax offences, for which information can be exchanged on the basis of laws and regulations in matters of taxation. Therefore, this chapter does not include those participating authorities and the conditions for the exchange of information by them. For more information on the requirements applicable to that kind of information exchange, please refer to the preceding chapter.

Further, this chapter pays more attention to the spontaneous exchange of information than to exchange of information on request. The reason for this is that the exchange of information on request in the context of FCInet is legally much less difficult to classify than the spontaneous exchange of information. Nevertheless, the text below will indicate some legal basis for the exchange of information on request following a match as a result of FCInet operations.

For criminal offences that cannot be classified as tax offences, other international legal bases are available. This chapter gives an overview of those international instruments as well as an overview of national laws of the participating FCInet authorities that wish to use FCInet for exchanging information in criminal matters beyond tax offences. The countries for which this applies are the Netherlands, the United Kingdom and Sweden. In paragraph 6.2, a relevant international legal instrument will be presented: the 1959 Council of Europe Convention on Mutual Legal Assistance in Criminal Matters. In paragraph 6.3, a number of EU legal instruments will be discussed. While not all participants in FCInet are EU member states, the three countries to which this chapter applies are bound by this legislation either because they are member states of the European Union, or, in the case of the United Kingdom, have elected to keep applying European Union law by adopting the post-Brexit Trade and Cooperation Agreement.[95] Paragraph 6.4 will give an overview of the application of these international legal instruments by FCInet participants on the national level.

6.2 International legal instruments for cooperation in criminal matters

6.2.1 The Convention on Mutual Legal Assistance in Criminal Matters

Very important for criminal law cooperation in Europe is the 1959 European Convention on Mutual Assistance in Criminal Matters, concluded within the framework of the Council of Europe.[96] The Convention only pertains to criminal offences, for which a person can be sentenced by the criminal courts of the parties to the Convention. Cooperation in administrative matters is therefore not possible on the basis of the

—

[95] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, Brussels, 30 December 2020.

[96] To be found on the website of the Treaty Office under reference ETS No. 030. See http://www.coe.int/en/web/conventions.

convention. In 1978, an additional protocol was concluded,[97] followed in 2002 by a second additional protocol.[98]

For countries that ratified the additional protocols to the convention, the modified Article 1 of the Convention applies. This article obliges the parties to the convention to 'promptly to afford each other, in accordance with the provisions of this Convention, the widest measure of mutual assistance in proceedings in respect of offences the punishment of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Party'. This article implies an obligation on the sides of the parties to mutually assist each other in criminal proceedings. The Convention therefore does not only contain competences and procedures to be used, but additionally obliges the parties to use them. This first Article also seems to imply a legal basis for the exchange of information on request, as there is otherwise no specific legal basis for that mode of cooperation in the Convention. These are simply covered by the generic term 'request for mutual assistance' and are defined with regard to the applicable procedure, for instance in Article 14 and 15 of the Convention. Another reading of this Convention, however, would be that it simply does not cover the exchange of information on request. In that view, such an exchange simply goes without a specific regulation on the international level, which would be acceptable because an exchange of information causes very little interference with fundamental rights of the persons involved. Also, many countries are reluctant to promise that they will share information in case it would appear that such information is preferably not disclosed to authorities in other countries. Both arguments could explain why Conventions such as the 1959 Council of Europe MLA Convention do not contain specific provisions on the exchange of information on request.[99]

Because of the fact that the collaboration within FCInet also covers offences relating to taxation, it is relevant to address the grounds of refusal that are dedicated to tax matters. Article 2 of the Convention contains such a ground of refusal. However, the additional protocol removed this ground of refusal in its Article 1. Therefore the participants in FCInet that have ratified the additional protocol cannot refuse mutual legal assistance in matters of taxation.

While the Convention was initially concluded only with the aim of facilitating judicial cooperation and not police cooperation,[100] it contains provisions for information exchange in its second additional protocol. Importantly, this protocol enables the spontaneous exchange of information between the parties to the convention. Article 11 of this protocol ('Spontaneous information') states:

'1. Without prejudice to their own investigations or proceedings, the competent authorities of a Party may, without prior request, forward to the competent authorities of another Party information obtained within the framework of their own investigations, when they consider that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings, or might lead to a request by that Party under the Convention or its Protocols.

2. The providing Party may, pursuant to its national law, impose conditions on the use of such information by the receiving Party.

3. The receiving Party shall be bound by those conditions.

4. However, any Contracting State may, at any time, by means of a declaration addressed to the Secretary General of the Council of Europe, declare that it reserves the right not to be bound by the conditions imposed by the providing Party under paragraph 2 above, unless it receives prior notice of the nature of the information to be provided and agrees to its transmission.'

—

[97] To be found on the website of the Treaty Office under reference ETS No. 099. See http://www.coe.int/en/web/conventions.

[98] To be found on the website of the Treaty Office under reference ETS No. 182. See http://www.coe.int/en/web/conventions.

[99] Bassiouni 2008, p. 19-20.

[100] Fijnaut, Spapens & Van Daele 2005, p. 155-156.

The use of the term 'competent authorities' implies that it is up to the parties to the convention to define the authorities which are competent to carry out this type of mutual assistance. The fact that a certain authority may be designated as a competent authority does not empower that authority to freely exchange any information without the need to use the proper channels, however. Article 4 of the second additional protocol changed Article 15 of the Convention in such a way that paragraph 1 of Article 15 now states: 'Requests for mutual assistance, as well as spontaneous information, shall be addressed in writing by the Ministry of Justice of the requesting Party to the Ministry of Justice of the requested Party and shall be returned through the same channels. However, they may be forwarded directly by the judicial authorities of the requesting Party to the judicial authorities of the requested Party and returned through the same channels.' The judicial authorities that are named in this paragraph include prosecutors, but not investigators.[101]

This leads to the conclusion that the competent authorities may directly and spontaneously forward information to another competent authority, but that information must also be forwarded by judicial authorities to the judicial authorities of another party to the convention, and addressed by the Ministry of Justice to the Ministry of Justice of the other party to the convention. Such a cumbersome procedure may however be abolished by other agreements (Article 15 as amended by the second protocol, paragraph 10). Absent these further agreements, it is hardly imaginable how this multi-level system of spontaneous exchange of information could ever be used in the context of FCInet. FCInet's design seems ill-equipped to include judicial authorities and Ministries of Justice in each exchange of filters. Therefore the Convention cannot realistically serve as a legal basis for the type of cooperation envisaged.

The second additional protocol to the Convention includes provisions on data protection (Article 26). These provisions apply with regard to personal data that is transferred as a result of the execution of a request. These provisions are not applicable in case of the spontaneous exchange of information, but they do apply to the exchange of information on request, following a math during FCInet operations. If these operations would be based on this international legal basis, they therefore should comply with the requirements of Article 26 of the second protocol to the Convention.

6.2.2 The EU-UK Trade and Cooperation Agreement

As the United Kingdom left the European Union on 1 February 2020, a transition phase began that ended on 31 December 2020. During this transition period, most of European Union law remained in force, enabling the authorities within the United Kingdom to continue their usual cooperation with authorities in the member states of the European Union. Shortly before the transition period ended, the United Kingdom and the European Union agreed on a Trade and Cooperation Agreement[102] that would form the legal basis of their relationship and would enable the authorities from the United Kingdom and the member states of the European Union to cooperate on a new basis, with some notable changes, but without having to resort to using legal instruments of an older or more generic nature.

Article 563 of the Trade and Cooperation Agreement contains provisions on 'Cooperation on Operational Information'. These provisions have as an objective (as stated in Article 563(1)) to 'ensure that the competent authorities of the United Kingdom and of the Member States are able to, subject to the conditions of their domestic law and

—

[101] That is at least the case for the Netherlands (Declaration to the Convention, dated 13 February 1969) and the United Kingdom, which does not include the HMRC in this category (Declaration to the second Additional Protocol, dated 7 February 2013). Belgium probably defined the term 'judicial authority' as including only the Federal Prosecutors (Declaration to the second additional protocol, 11 March 2013).

[102] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, Brussels, 30 December 2020.

within the scope of their powers, and to the extent that this is not provided for in other Titles of this Part, assist each other through the provision of relevant information'. Further, Article 563(1) refers to four different purposes for which the authorities may want to provide information: a) the prevention, investigation, detection or prosecution of criminal offences, b) the execution of criminal penalties, c) safeguarding against, and the prevention of, threats to public safety, and d) the prevention and combating of money laundering and the financing of terrorism. Article 563(2) defines as 'competent authority' 'a domestic police, customs or other authority that is competent under domestic law to undertake activities for the purposes set out in paragraph 1'.

Article 563(3) gives a legal basis for an exchange of information on request as well as for a spontaneous exchange of information between the competent authorities of the United Kingdom and the member states of the European Union. It stipulates that the conditions of national law applying to the competent authorities in question, and the scope of their powers, remain applicable to their activities. Article 563(4) further stipulates that, if the relevant domestic laws require the information to be exchanged through judicial authorities, the competent authorities must comply with those requirements. Absent these requirements, the exchange of information may proceed through any appropriate communication channel (Article 563(9)). Any information may be exchanged, also information that has come within the possession of the competent authorities from other sources, as long as onward transfer is permitted in the framework under which it was initially obtained (Article 563(8)). There are also provisions regarding urgent procedures (Article 563(5)), the use of information in evidence (Article 563(6)) and conditions that can be attached to the use of the information that is exchanged (Article 563(7)).

This Agreement offers the most likely legal basis for an exchange of information in the criminal law domain between authorities in the United Kingdom on the one hand and authorities in the European Union on the other hand. It covers both the spontaneous exchange of information and the exchange of information on request. If this Agreement is to be used for FCInet, the participating organisations in the UK and the EU should be designated as competent authorities. This seems to be covered by the definition in Article 563(2) TCA.

6.3 European Union instruments

6.3.1 The Convention Implementing the Schengen Agreement

The Convention Implementing the Schengen Agreement (CISA) contains several provisions that are relevant to the exchange of information, both spontaneous and on request. Together with other instruments, based on CISA, it is called the *Schengen acquis*, which was incorporated into the EU framework in 1999 and has consequently become EU legislation.[103]

This Convention can be of limited value for FCInet, as its role in regulating the exchange of information between EU Member States has been abolished with the entering into force of Framework Decision 2006/960/JHA.[104] Article 12(1) of this Framework Decision states: 'The provisions of Article 39(1), (2) and (3) and of Article 46 of the Convention Implementing the Schengen Agreement (1), in as far as they relate to exchange of information and intelligence for the purpose of conducting criminal investigations or criminal intelligence operations as provided for by this Framework Decision, shall be replaced by the provisions of this Framework Decision.' The type of collaboration which is envisaged by FCInet clearly falls within the category of exchange of information or intelligence which is carried out for purposes of investigating criminal offences, or gathering criminal intelligence. Therefore, Article 39 CISA no longer applies to the exchange of information on request between the member states of the EU and

—

[103] This status is nowadays effectuated by Protocol No. 19 to the TFEU, on the Schengen Acquis Integrated into the Framework of the European Union.

[104] The so-called 'Swedish Framework Decision, which is elaborated upon later in this report.

Article 46 CISA no longer applies to the spontaneous exchange of information, and both cannot form a legal basis for the cooperation within FCInet. However, Articles 39 and 46 CISA have been an important provision in the past, and have been the subject of legal research as well. Therefore, these have been important for the understanding of the exchange of information in criminal matters. Rather than ignoring the Convention altogether, we will here present some elements of the discussion.

Article 39 CISA contains general provisions on police cooperation. However, the Convention does not define the term 'police authorities' that is mentioned in this article. That being the case, the Convention stipulates that the authorities shall, in compliance with national law and within their powers, 'assist each other for the purposes of preventing and detecting criminal offences, in so far as national law does not stipulate that the request has to be made and channelled via the judicial authorities and provided that the request or the implementation thereof does not involve the application of measures of constraint by the requested Contracting Party' (Article 39(1)). This clearly includes a legal basis for the exchange of information on request, all the more because Article 39(2) refers to 'written information provided by the requested Contracting Party', and provides that this information may not be used in evidence unless there is a separate consent for that. This indicates that Article 39(1) provides for a method of exchanging information on request without this information necessarily having evidentiary purposes.

Article 46 CISA provides a basis for the spontaneous exchange of information. It states:

'1. In specific cases, each Contracting Party may, in compliance with its national law and without being so requested, send the Contracting Party concerned any information which may be important in helping it combat future crime and prevent offences against or threats to public policy and public security.

2. Information shall be exchanged, without prejudice to the arrangements for cooperation in border areas referred to in Article 39(4), via a central body to be designated. In particularly urgent cases, the exchange of information within the meaning of this Article may take place directly between the police authorities concerned, unless national provisions stipulate otherwise. The central body shall be informed of this as soon as possible.'

The general purpose of this article is 'to facilitate the exchange of typical police information, such as intelligence, results of investigative measures and suspect's antecedents'.[105] The fact that there is an explicit basis in the CISA for this purpose is said to originate in the balancing of two interests. On the one hand, the character of the data would stand in the way of exchanging the data in a completely informal procedure, while on the other hand ascertaining this type of information would be very difficult if a formal request for information would have to be issued.[106]

It is important to note that the CISA leaves it to the parties to the convention to define a central body for purposes of spontaneous exchange of information. There are derogations possible for cooperation in border areas, as well as for particularly urgent cases. The Parties may decide that the exchange of information in these cases does not have to pass through a central authority. The central bodies defined for executing the CISA are mostly defined in the national fact sheets.[107]

Articles 39 and 46 CISA do not contain any limitation on the origins of the data that is exchanged. They appear to leave that to national law.[108] However, there is a list of purposes for which data may be exchanged: to prevent future crime, and to prevent offences against or threats to public order and security. It is not a condition that the information which is exchanged is necessary for the attainment of these purposes, but it should be helpful. This list does not include the investigation of criminal offences. This

—

[105] Joubert and Bevers 1996, p. 449.

[106] Joubert and Bevers 1996, p. 449.

[107] Joubert and Bevers 1996, p. 454.

[108] Joubert and Bevers 1996, p. 451-452.

shows that the Convention views this type of international cooperation as mostly aiming at the maintenance of public order and public security, rather than as helpful for investigative purposes.

The Convention also does not contain an exact definition of 'criminal matters', which is the term in its title. Therefore the question whether a proceeding is a 'criminal matter' is left to the parties. It can be held that as long as the proceedings in which the cooperation takes place involve a criminal charge within the meaning of Article 6 ECHR, the cooperation can be viewed as taking place with regard to 'criminal matters'.[109] This could include some proceedings which, according to national law, are labelled as administrative proceedings, but only if they comply with the criterion of a 'criminal charge' according to Article 6 of the European Convention on Human Rights (ECHR). Therefore, fiscal proceedings could also come into view, as these often end in imposing a tax surcharge. Such is for instance the case in Belgium, where the BBI can impose a tax surcharge of up to 200% of the indebted taxes,[110] or a penalty of 6.250 Euros.[111] The imposition of tax surcharges, even when it concerns 10% of indebted taxes, has been considered by the European Court of Human Rights to amount to a criminal charge. The fact that the Court also held that in such cases the requirements of Article 6 ECHR may apply to a lower extent, does not warrant the conclusion that there is no criminal charge.[112]

Article 129 CISA contains specific rules on the protection of data which is transferred for the exchange of information in criminal investigations. There are some additional obligations when it concerns information which is exchanged spontaneously. The data may only be used by the receiving party for the purposes that the sending party indicated, and according to the conditions the sending party attached to the cooperation. Furthermore, the data may be communicated to police forces and authorities only, and not to other authorities without the prior authorisation of the sending party. Lastly, the receiving party must inform the sending party of the uses to which the data has been put and of the results of that use.

While the CISA has been replaced by Framework Decision 2006/960/JHA, we can learn some important lessons from the literature. It has been said that regulating the spontaneous exchange of information is important because the character of the data does not allow for a completely informal procedure, while at the same time ascertaining these data would be very difficult if more elaborate procedures would have to be used. Slightly different ideas exist with respect to the exchange of information on request: while the sending country has full control over the information that is sent spontaneously, it does not have full control over information that is sent on request once it promises to assist other countries in the fullest possible manner when so requested. However, the text of Article 39 CISA shows little reluctance. The terms 'police authorities' and 'criminal matters' need not be very restrictive. Therefore, the Convention may also allow cooperation with administrative authorities, but only when their activities can be viewed as amounting to a criminal charge. However, this is subject to the possibilities afforded by the Parties to the Convention in their national law and in their designations of certain bodies as competent authorities. These aspects will most probably also be relevant for the spontaneous exchange of information that is carried out on the basis of other conventions and EU legal instruments.

6.3.2 The EU Convention on Mutual Assistance in Criminal Matters

The EU concluded in the year 2000, within the framework of the so-called Third Pillar, a Convention on Mutual Assistance in Criminal Matters between the Member

—

[109] Klip and Vervaele 2001, p. 37.

[110] Article 444 Wetboek van de Inkomstenbelastingen (WIB) 92 in combination with Article 225 to 229 KB/WIB 92.

[111] Article 445 WIB 92.

[112] ECtHR 23 November 2006, App.No. 73053/01 (Jussila).

States of the European Union.[113] This Convention was followed by a Protocol in 2001.[114] The Protocol to the Convention enables mutual cooperation on financial transactions. This protocol does however not contain any provisions for spontaneous exchange of information.

The 2000 Convention supplements and facilitates the application of the European Convention on Mutual Assistance in Criminal Matters and the associated protocols, insofar as it does not repeal parts of this Convention. It will, in its turn, in most aspects be superseded by the Directive on the European Investigation Order.

Article 6 of the Convention contains a provision on the exchange of information on request, which can be deemed to be included in the term 'requests for mutual assistance' mentioned in Article 6(1). These requests can be made directly between the judicial authorities that are territorially competent and the results can be returned through the same channel. This provision clearly refers to 'judicial authorities', which apparently excludes authorities that are not deemed 'judicial', such as police authorities. This is in contrast to the spontaneous exchange of information (see below), which is enabled between 'competent authorities'.

There is a further requirement in Article 6(1) that the exchange of information in this way is capable of leaving a written record, and that the exchange must be done in such a way that the receiving party is able to establish authenticity. The fact that such direct communication is possible does not rule out, however, that a central authority may be used in a particular case (Article 6(2)). The United Kingdom and Ireland have an opt-out of this possibility for direct communication, and the other Member States may apply reciprocity in these matters (Article 6(3)). There is another exception to the rule of direct communications, and that is that some notices of information from judicial records are not to be directly exchanged (Article 6(8(b))). Apart from these exceptions, Article 6 of the 2000 EU MLA Convention appears to give a solid foundation for the exchange of information on request between the judicial authorities of the Member States.

Article 7 of the Convention contains a provision on spontaneous exchange of information. Information provided spontaneously, without prior request of legal assistance, may be subject to conditions, such as a limitation on the purposes of its use. The sending authority may, on the basis of its national law, set limits to the use of the information by the receiving authority, which, according to the Convention, is bound to these conditions (Article 7(1) and 7(2)). A further condition, set by Article 7, is that the information that is sent to the receiving authority must fall within that authority's competences as regards handling the case the information relates to or imposing punishment for that case.

This article enables the authorities of the parties to the Convention to not only exchange information regarding criminal offences. It also enables mutual assistance in proceedings brought by the administrative authorities for acts that are punishable under the law of the receiving or the sending authority's state, or both. There is however a further condition: it must be the case that the decision in these administrative proceedings may give rise to proceedings before a court having jurisdiction in particular in criminal matters (Article 7(1) in combination with Article 3(1)).

However, using this Convention is difficult because of a reason which was already mentioned. The Convention designates the possible authorities that can make use of the spontaneous exchange of information as 'competent authorities'. This contrasts with the use, in other places, of the term 'judicial authorities'. While judicial authorities mostly do not include investigators, 'competent authorities' could potentially include investigative services. The Member States are under an obligation to formally designate the competent authorities (Article 24 of the Convention includes an obligation to specify the competent

—

[113] Council act 2000/C 197/01.

[114] Council act 2001/C 326/01.

authorities for the Convention in general, and names some Convention provision for which specific designations are necessary).[115]

Article 23 contains some provisions on data protection that apply to information which is exchanged using the Convention. It holds that the data may be used in the proceedings to which the Convention applies, i.e. criminal investigations and prosecutions (Article 23(1)(a)). Additionally, the data may be used in judicial and administrative procedures that are directly related to criminal investigations and prosecutions (Article 23(1)(b)), to prevent immediate and serious threats to public security (Article 23(1)(c)) and for any other purpose, but only with the prior consent of the sending Member State or the consent of the data subject (Article 23(1)(d)). Any conditions that have been attached to spontaneously exchanged information have precedence over these general data protection rules (Article 23(4)). These rules may be applicable when the exchange of information is based upon this instrument. However, they probably add little to the provisions of the Law Enforcement Directive.[116]

6.3.3 The EU Framework Decision on simplifying exchange of information

The prime legal basis for spontaneous exchange of information in criminal matters within the EU is the 2006 Framework Decision on simplifying the exchange of information. This is sometimes called the 'Swedish Framework Decision' because it was Sweden that took the initiative for the instrument.[117] Its scope is limited to criminal investigations and criminal intelligence. It therefore does not include administrative proceedings.

The purpose of the Framework Decision is to simplify and accelerate the exchange of information between EU law enforcement authorities. It obliges the Member States to designate the competent law enforcement authorities, and to notify the EU of their designations.

As mentioned above, the Framework Decision abolished the corresponding provision on spontaneous exchange of information in the Convention Implementing the Schengen Agreement (Article 12(1) of the Framework Decision). Next to that, the Framework Decision requires Member States to communicate to the Council and the Commission before 19 December 2006 any existing agreements and arrangements of a bilateral and multilateral nature which allow the Framework Decision's objectives to be extended and which simplify or facilitate the procedures for exchanging information (Article 12(3) and (6)). Potentially, this option could have been used to enable certain Member State authorities to use spontaneous exchange of information on the basis of previous instrument while they cannot use the Framework Decision.

Article 2(d) defines information and/or intelligence as any type of information which is held by law enforcement authorities or any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures, in accordance with Article 1(5). As the data used in the FCInet pilot project only concerns data which already is available to the authorities, this condition is met.

Article 7 provides for spontaneous exchange of information. It states:

'1. Without prejudice to Article 10, the competent law enforcement authorities shall, without any prior request being necessary, provide to the competent law enforcement authorities of other Member States concerned information and intelligence in cases where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of offences referred to in Article 2(2) of Framework Decision 2002/584/JHA. The modalities of such spontaneous exchange shall be regulated by the national law of the Member States providing the information.

—

[115] The declarations can be found on the website of the European Judicial Network (https://www.ejn-crimjust.europa.eu/ejn/).

[116] Directive (EU) 2016/680.

[117] Council Framework Decision 2006/9600/JHA.

2. The provision of information and intelligence shall be limited to what is deemed relevant and necessary for the successful detection, prevention or investigation of the crime or criminal activity in question.'

This article contains an obligation to share information, because of its wording: the authorities 'shall' provide each other with information. This spontaneous exchange of information is subjected to the criterion that there should be factual reasons to believe that the information could assist in detecting, preventing or investigating crimes. Therefore, the receiving authority must be able to use the information in ongoing procedures, or to use them in a more general preventive sense. FCInet complies with this condition, as the technology used automatically reveals only the fact that a person is known to the sending authority when that person is also involved in proceedings directed by the receiving authority, and nothing else. The chance that such information is useful in the ongoing procedures in the receiving country is quite high.

Article 5 provides an express basis for the exchange of information on request. It reads: '1. Information and intelligence may be requested for the purpose of detection, prevention or investigation of an offence where there are factual reasons to believe that relevant information and intelligence is available in another Member State. The request shall set out those factual reasons and explain the purpose for which the information and intelligence is sought and the connection between the purpose and the person who is the subject of the information and intelligence.

2. The requesting competent law enforcement authority shall refrain from requesting more information or intelligence or setting narrower time frames than necessary for the purpose of the request.

3. Requests for information or intelligence shall contain at least the information set out in Annex B.'

Annex B to this Framework Decision includes a form in which the requesting and requested Member State should indicate, among other things, the name and details of the requested and requesting authorities, the applicable time limit, the purpose for which the information is to be used, and any reasons why the exchange of information was refused, if that is the case.

This provision very clearly enables the exchange of information on request in criminal investigations. A condition that applies is that such a request for information may be made when there are factual reasons to believe that there is relevant information in another Member State. Clearly, that condition would be complied with if a match occurs within FCInet: in such a case, there is a significant chance that the participating authority that sent the filter has relevant information available on the person with respect to whom the match occurred.

Importantly, this provision refers to the 'competent law enforcement authority'. The same counts for Article 7 that deals with the spontaneous request for information. This limits the possibilities to use the Framework Decision. This particular aspect will be addressed below.

The Framework Decision only applies with regard to the so-called 'list offences' enumerated in the Framework Decision on the European Arrest Warrant.[118] This could potentially be a limitation to FCInet. These are the offences:

- participation in a criminal organisation,
- terrorism,
- trafficking in human beings,
- sexual exploitation of children and child pornography,
- illicit trafficking in narcotic drugs and psychotropic substances,
- illicit trafficking in weapons, munitions and explosives,
- corruption,

—

[118] Council Framework Decision 2002/584/JHA.

- fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests,
- laundering of the proceeds of crime,
- counterfeiting currency, including of the euro,
- computer-related crime,
- environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
- facilitation of unauthorised entry and residence,
- murder, grievous bodily injury,
- illicit trade in human organs and tissue,
- kidnapping, illegal restraint and hostage-taking,
- racism and xenophobia,
- organised or armed robbery,
- illicit trafficking in cultural goods, including antiques and works of art,
- swindling,
- racketeering and extortion,
- counterfeiting and piracy of products,
- forgery of administrative documents and trafficking therein,
- forgery of means of payment,
- illicit trafficking in hormonal substances and other growth promoters,
- illicit trafficking in nuclear or radioactive materials,
- trafficking in stolen vehicles,
- rape,
- arson,
- crimes within the jurisdiction of the International Criminal Court,
- unlawful seizure of aircraft/ships,
- sabotage.

Thirdly, the exchange should be limited in the sense that only information is exchanged which is considered relevant or necessary for purposes of detecting, preventing or investigating offences. This condition is also met by FCInet, because the information that is exchanged is very limited in nature. On the basis of the filters that are exchanged, the receiving authority can only deduce one piece of information: that a certain person whom the authority already knows is involved in an ongoing investigation led by the sending authority. The design of the FCInet intentionally excludes the possibility that any other personal data than names and dates of birth are being sent, while, as described above, the names and dates of birth of people unknown to the recipient will remain encrypted. The Framework Decision leaves the exact methods for sharing information to be defined in national law.

Article 9 contains several rules regarding data protection. It includes the principle of purpose limitation: the competent law enforcement authorities, based on their national law, must ensure that the information is processed in a confidential manner. Article 10 contains some grounds based on which information or intelligence may be refused.

6.4 Application of international instruments on national level

6.4.1 Implementation of international conventions

The 1959 Council of Europe Convention and both of its protocols were ratified by and have entered into force for the Netherlands, Sweden and the United Kingdom. Article 11 of the second additional protocol enables the parties to the convention to declare themselves to be unbound by any conditions that the sending party may attach to the spontaneously sent information. The United Kingdom has availed itself of this option.[119]

—

[119] See the table of declarations and reservations on the Treaty Office website: http://www.coe.int/en/web/conventions, ETS No. 182.

The 2000 EU MLA Convention and its protocol have entered into force for the Netherlands and Sweden, and it previously applied to the United Kingdom.[120] The United Kingdom used a possibility to opt-in to a part of the Schengen acquis, including the Schengen Information System. It was granted this possibility, as a consequence of which it is also a party to the EU Convention on Mutual Legal Assistance and the Protocol thereto.[121] Later, after using its option to opt-out of all EU legislation in police and judicial cooperation matters, the Council of the EU granted the United Kingdom's request to partly opt back into that acquis, Article 46 of the CISA being on the list of relevant measures, which is the provision relating to spontaneous information exchange.[122] Currently, following Brexit, relations between the United Kingdom and the member states of the European Union are defined comprehensively in the Trade and Cooperation Agreement, Article 563 of which deals with 'Cooperation on Operational Information'.

Both Sweden and the Netherlands are bound by the Framework Decision on simplifying the exchange of information.[123] This 'Swedish Framework Decision' is limited to a number of offences, mentioned in the list annexed to the Framework Decision on the European Arrest Warrant. Many of these crimes fall within the areas of competence of the participants in FCInet. In Sweden, the Swedish Tax Agency, being responsible for taxes, bookkeeping fraud, money laundering, etc., would find most of its criminal enforcement activities falling under the 'fraud' category. The Dutch FIOD's responsibilities for investigating fraud, money laundering, organised crime and trafficking of drugs are covered by the list.

6.4.2 Competent authorities

The Netherlands did not declare any specific authority as a competent authority for the spontaneous exchange of information under the second additional protocol to the 1959 Council of Europe Convention, in its instrument of ratification.[124] This also counts for the United Kingdom[125] and Sweden[126]. This leads to the conclusion for these three countries that any national authority which is competent according to national law for the spontaneous exchange of information can be viewed as a competent authority under the second additional protocol. Nevertheless, the Council of Europe Convention, as amended by the Protocol, still keeps a cumbersome procedure in place for these competent authorities to work with, as defined in Article 15 of the Convention as amended by the Second Protocol. This procedure could however be simplified by later conventions or treaties.

The Fiches Belges indicate that the 2000 EU MLA Convention would pre-Brexit be the sole method for spontaneous exchange of information with the United Kingdom. According to this source, all information that it sent on the basis of the 2000 EU MLA Convention to Scotland should be sent to the International Co-operation Unit, Crown Office, Edinburgh. For tax offences committed in England and Wales, the HMRC is the central office. All other communication should be directed at the Central Authority International Criminality Unit of the Home Office.

As concerns the EU-UK Trade and Cooperation Agreement, so long as the relevant authorities are made competent in their national laws, and act within the scope of their powers, these authorities seem to be able to exchange information by using FCInet on the basis of the Trade and Cooperation Agreement. This Agreement now lays a clear

—

[120] The United Kingdom opted back in to this Convention after using its block opt-out: Consolidated version of Council Decision 2002/926/EC.

[121] Council Decision 2004/926/EC.

[122] See Council doc. No. 15398/14; Consolidated version of Council Decision 2000/365/EC.

[123] The United Kingdom opted back in to this Framework Decision after using its block opt-out: Commission decision 2014/858/EU.

[124] Deposited on 20 December 2010.

[125] Instrument of ratification deposited on 30 June 2010.

[126] Instrument of ratification deposited on 20 January 2014.

foundation for exchanging information on criminal investigations between the competent authorities of the United Kingdom and EU member states, both on a spontaneous basis and on the basis of requests.

A condition, set by Article 7 EU MLA Convention, is that the information that is sent to the receiving authority must fall within that authority's competences as regards handling the case the information relates to or imposing punishment for that case. This condition is satisfied easily for the Dutch and Swedish partners in FCInet, since they are involved in proceedings that are explicitly characterised as being criminal in nature. Therefore, the Convention could potentially be used for exchanging data between the partners in FCInet.

With regard to the competent authorities under the 2000 EU MLA Convention, the Netherlands deposited a declaration at the same time as the instrument of ratification,[127] declaring that the competent authorities for the Convention would be the same authorities as were competent for the Council of Europe Convention on Mutual Assistance in Criminal Matters and the Benelux Convention. The United Kingdom declared that the authorities to be regarded as 'competent authorities' for purposes of this Convention are the same authorities which are competent for the Council of Europe Convention on Mutual Assistance in Criminal Matters.[128] An identical declaration was made by Sweden.[129] As described above in relation to the second additional protocol to the Council of Europe Convention on Mutual Assistance in Criminal Matters, the authorities which are made competent by national law for the spontaneous exchange of information can also be viewed as competent authorities for Article 11 of the second additional protocol. The consequence of this is that the cumbersome procedure which was still present in the Council of Europe Convention is abolished, and that the competent authorities are able to directly exchange information between themselves on the basis of the 2000 EU Convention.

When it comes to competent authorities under the Framework Decision on simplifying the exchange of information, the Netherlands designated the National Police Services Agency of the Netherlands Police (*Korps Landelijke Politiediensten*).[130] The FIOD (*Fiscale Inlichtingen- en Opsporingsdienst*) is therefore not a competent authority for purposes of this Framework Decision. The same counts for the Swedish Tax Agency. While this Agency is a partner in FCInet, is has not been designated as a competent authority under this Framework Decision. Therefore, it is unable to use this as a basis under any exchange of information. However, this Agency might be able to exchange information through Europol and Interpol. This state of affairs could be changed if the relevant governments would designate the FCInet partners as a competent law enforcement authority under the Framework Decision. Alternatively, if the EU were to adopt a new Police Cooperation Code, new decision will have to be made on which authorities will be competent to use it, which may induce the relevant governments to opt for designating additional authorities under the new Code.

6.4.3 Foreseeable relevance

In criminal matters, the spontaneous exchange of information is not defined in a single manner. The international legal instruments differ.

Article 11 of the second additional protocol to the 1959 Council of Europe Convention on mutual assistance in criminal matters stipulates that the competent authorities may forward to other competent authorities any information that is obtained in their investigations 'when they consider that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings, or might lead to a request by that Party under the Convention or its Protocols'.

—

[127] Notified on 2 April 2004.

[128] Declaration deposited on 14 December 2011.

[129] The Covention entered into force for Sweden on 5 October 2005.

[130] Council doc. No. 8677/08.

Article 7 of the 2000 EU MLA Convention declares that the competent authorities 'may exchange information, without a request to that effect, relating to criminal offences and the infringements of rules of law referred to in Article 3(1), the punishment or handling of which falls within the competence of the receiving authority at the time the information is provided'.

Article 7 of the Framework Decision on simplifying the exchange of information enables the competent authorities to spontaneously exchange information in cases 'where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of offences referred to in Article 2(2) of Framework Decision 2002/584/JHA'.

None of these instruments directly use the term 'foreseeable relevance', as is used in the Convention on mutual assistance in matters of taxation. However, to some extent the provisions relate to that concept in some sense. Whereas the Framework Decision includes a condition that the information 'could assist' and the additional protocol to the Council of Europe Convention states that the information 'might assist' a competent authority in the receiving state, the definition of spontaneous exchange of information in the EU MLA Convention does not even include a condition that requires such a thing as foreseeable relevance.

In the national laws of the Netherlands, the United Kingdom and Sweden, there are provisions that enable the authorities, if they have been designated as competent authorities, to disclose or send information on criminal investigations to other authorities within or outside of the European Union. Swedish law even includes an obligation to exchange some investigative data, which seems to resemble the spirit behind the principle of availability which underlies the Swedish Framework Decision.

6.4.4 Data protection

National authorities within the EU are only allowed to exchange information outside the European Union under the condition that data protection laws in the relevant country offer appropriate safeguards. This is further specified in the requirement that either an adequacy decision is necessary, or a legally binding instrument that provides appropriate safeguards, or, in the absence of this, an assessment of the controller of all circumstances surrounding the transfer of personal data with the conclusion that appropriate safeguards exist (Article 36-37 LED). As for FCInet, this means that transfer to the United Kingdom is allowed because of an adequacy decision. With respect to other FCInet participants outside the European Union, this requirements is fulfilled for criminal matters because the exchange of information with these countries only consists of the exchange of criminal tax information, which falls within the scope of the Convention on the Exchange of Information in Matters of Taxation. This means that for these exchanges, this Convention can be seen as a relevant legally binding instrument. Whether this instruments provides appropriate safeguards has to be decided by the national authorities. Seeing that the Conventions contains the obligation to share relevant criminal tax information, a charitable judgement of the safeguards seems sound – as already discussed in par. 5.4. Perhaps these appropriate safeguards can also be found in other instruments, such as the Council of Europe Convention 108+. On another note, it is a matter of interpretation whether the LED requires an internationally binding instrument, laying down obligations of relevant international parties, or whether the LED requires a binding instrument in national law, protecting personal data within a jurisdiction. The participating authorities are under an obligation to decide how to interpret this requirement and on the basis of that interpretation decide whether it is the case that appropriate safeguards exist.

There are some restrictions on the exchange of information, whether it is spontaneous or on request, that take place in FCInet with respect to criminal offences. Some of those restrictions apply to the further use of information that is received. HMRC reports that national law prohibits the recipient of information that is disclosed under section 19 of the Anti-Terrorism, Crime and Security Act 2001 to disclose this information further, unless this is for a requisite purpose and it has been consented by

the HMRC. Dutch authorities are also bound by law to only spontaneously exchange information to other EU authorities under the condition that it can only be processed for the purposes it is supplied for, and that the information should be deleted if that purpose is achieved. This principle of purpose limitation also is laid down in some of the applicable international legal instruments. Article 26 of the second protocol to the Council of Europe Convention on Mutual Assistance in Criminal Matters includes requires the state parties to comply with quite detailed rules on purpose limitation. Some of these restrictions are subject to the possibility of being lifted by prior consent by the sending authority. Additionally, the Framework Decision on simplifying the exchange of information contains a comparable provision on purpose limitation in Article 8(3) of that instrument.

6.5 Conclusion

Only some FCInet participants desire to exchange information outside the scope of taxation matters, and are willing to use it for exchanging information on criminal offences involving for instance corruption, money laundering and fraud. In principle, there seem to be more than enough possibilities in international legal instruments for both the spontaneous exchange of information and for the exchange of information on request. The definition of spontaneous exchange of information does not lead to particular difficulties, with respect to FCInet, to classify its operations as such.

The possibly applicable international legal instruments require the authorities in FCInet to be designated as 'competent authorities' in order for them to be able to use these instruments as an international legal basis defining their mutual commitments. This designation as competent authorities is however not available for all FCInet participants that wish to use it for purposes of exchanging information in criminal matters. On the basis of their national laws, these organisations have apparently not received sufficient competences to be able to operate as competent authorities for purposes of these international instruments. This is therefore primarily a matter of national law and decisions made by national bureaucracies, defining the role of these organisations with respect to these instruments. In principle, the organisations participating in FCInet with the wish to use it for criminal matters seem to be very well placed for that in terms of their general mandate. The governments of the respective countries could decide to designate these FCInet participants as competent authorities, which would solve the issue.

A minor issue might be that the national laws of some FCInet participants may require, now or in the future, that particular channels, such as Single Points of Contact, are used in case of international exchange of information. If this is the case, FCInet might choose to operate through these channels or under the supervision of relevant authorities that perform oversight over the use of these channels.

This being the case however, a further question is: how important is the fact that the participating authorities are not designated as a competent authority under this Framework Decision? As the Swedish Tax Agency indicates, it is not a requirement per se to have an international legal basis for being able to exchange information, but it is common to have one which is usually also implemented in national law. The unavailability of an international legal basis may therefore be partly an obstacle for FCInet operations, particularly if it is the wish to operate solely in case an international legal basis exists. If it exists, which seems to be the case with respect to a number of bilateral relations, FCInet can be used to exchange information on criminal matters.

7 Conclusions and Discussion

7.1 Introduction

In the conclusion of this report the main findings of the research project about the legal questions surrounding the setup of FCInet are laid down. The aim of this research is to check whether it is legally possible and feasible to spontaneously exchange filters containing pseudonymised personal data of people involved in financial crimes or irregularities, and to perform follow-up exchanges of information in case a match occurs. This exchange is envisaged between a number of participating authorities operating in different parts of the world. The main research question in this research project was: 'Which competences, duties and restrictions in national and international law apply to the exchange and matching of data as foreseen in FCInet?' This main research question is divided into four subquestions, which were dealt with in the previous chapters.

This conclusion is divided into three parts. These parts do not necessarily correspond to a certain subquestion and/or chapter, but contain a synthesis of the relevant research findings. In the first part, two essential legal starting points about FCInet are set forth and explained: the exchange of information involves personal data and the initial exchange is spontaneous in character. In the second part, some technical recommendations are presented to make sure that the operation in FCInet conforms to the demands of data protection regulations. In the third part, some legal recommendations are given. These legal recommendations focus on the competences, duties and restrictions to the exchange and matching of personal data as foreseen in FCInet.

7.2 Legal starting points

7.2.1 The exchange of information involves personal data

The first legal starting point is that the information exchanged in FCInet should be regarded as personal data; more specifically as a pseudonymised version of personal data. Therefore, the relevant national and international data protection regulations are applicable to the exchange of the personal data within FCInet. There is some difference in view about this. In one view, the filters that are exchanged always contain personal data. In another view, if FCInet operations lead to a match, then the filter in question becomes personal data with retroactive effect. In both cases, if a match occurs, the relevant filter is to be classified as personal data.

The starting point that the exchange of information concerns personal data has to be emphasised, because this triggers the applicability of data protection laws and regulations. The ma³tch process framework, which is used by FCInet, entails that the sending party is autonomous in selecting the personal data to fill the filters with, and in deciding the precision with which the filters are filled. The receiving party is served with filters containing inaccessible information on persons whose identity remains unknown to the recipient, unless the person to whom they relate is already known to the recipient. In that case the information in the filter can be accessed. The labelling of FCInet's method as 'anonymous' is intended to convey that the occurrence of a match by the receiving authority is not disclosed to the sending authority. It would be incorrect to state that the exchange of information as used by FCInet would involve only anonymous data, which would wrongfully create the impression that data protection rules do not apply. That conclusion would create a substantially different regulatory environment for FCInet compared to the regulations which would apply if the data being exchanged retained their status as personal data. Personal data is, according to the relevant data protection regulations, any information relating to an identified or identifiable natural person. This includes evidently data such as the name and date of birth of a person. Within FCInet this personal data is processed and transformed into a filter. This filter can be seen as containing (personal) data rendered unusable for a motivated intruder. Because the data in the filter cannot be reversed to an identifiable natural person without any additional

information, the data in the filter is protected against reasonable extracting attempts of unwanted intruders. However, irreversibility in itself is not enough for data to be regarded as anonymous.

Within the context of FCInet, the received filters can lead to the gaining of information regarding persons by the receiving participant, such as the identification of certain natural persons. The goal of FCInet is to check whether certain persons whose personal data is collected in the course of a financial investigation by a foreign authority are also known by the receiving national organisation. Comparing the information in the received filter with the information in the database of the receiving organisation can result in a match. A match means that the receiving organisation gets new information about a person: it knows for example that it is likely that a certain person is subject to investigations in a foreign country. Therefore, the data that is exchanged is to be regarded as personal data. Data is only truly anonymous when it is not possible to connect it directly or indirectly to an identifiable natural person. Within FCInet, it is clearly possible to receive information regarding certain natural persons. Were this not the case, the whole exchange of filters would be pointless.

Because the personal data is encrypted, the filter can be regarded as containing pseudonymised data. Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. This applies to FCInet, since the additional information to identify natural persons can only be generated within the context of FCInet and only if the receiving organisation knows the same natural person as the sending organisation does.

7.2.2 The supply of information is spontaneous

The second legal starting point is that the sending of filters by the sending organisation should be regarded as the spontaneous supply of information. The spontaneous supply of information is the provision of information to another contracting party that is foreseeably relevant to that other party and that has not been previously requested. In FCInet, the information that is sent is not directly requested for, but sent on the own initiative of the sending organisation.

The fact that in their mutual understanding, the partners to FCInet agreed to supply information does not change the spontaneous character of the exchange. The agreement to spontaneously supply information that could be relevant for the receiving organisation should not be regarded as a request for information, since that would mean it is impossible to make international agreements about the spontaneous supply of information. Instead those international agreements should be regarded as a framework within which the supply of information without a direct request is regulated. The fact that such frameworks are quite common is illustrated by the existence of provisions for the spontaneous exchange of information in several international instruments on cooperation in criminal and administrative matters, such as Convention on Mutual Administrative Assistance in Tax Matters, the second protocol to the European Convention on Mutual Assistance in Criminal Matters, the Convention Implementing the Schengen Agreement, the 2000 EU Convention on Mutual Legal Assistance, the Swedish Framework Decision and the EU Directive on administrative cooperation in the field of taxation.

The spontaneous character of the information supply has several consequences. Firstly, the supply is a one-way process in which information is only sent. There is an expectancy of reciprocity, but this is not necessary for the successful supply of information. Secondly, only information can be exchanged. In the case of FCInet, this information can consist of the fact that a certain person who is known by the receiving organisation is also known by the organisation that sent the filter. Thirdly, the spontaneous supply of information takes place from one organisation to another. This is a bilateral process, not a multilateral. Fourthly, the information sent should be possibly

relevant for the receiving organisation. This is guaranteed by the architecture of the FCInet software which provides that there only will be a match when a certain person is known by the sending as well as the receiving organisation. It is reasonable to presume that information about persons who are already known by the receiving organisation is possibly relevant for that organisation. Fifthly – as already mentioned – no request is needed for the spontaneous supply of information.

If a match occurs, and the FCInet participant that received the filter that led to the match requests for a validation of the match to the supplying FCInet participant, this is to be qualified as a request for information. There is a marked difference between such a request for validation and the initial sending of the filters: the request for validation is a bilateral exchange that involves a first step, the request, and a second step, the answer by the other party. This can therefore not be seen as a continuation of the spontaneous exchange of information, but must be qualified as a request for information.

This is even clearer when it comes to a request for additional information as a follow-up after a match occurs. If the receiving FCInet participant wants to gain more information with respect to a particular person whose data were involved in the match, this is surely to be seen as a request for information. There does not seem to be a clear lack of international and national legal bases for such requests of information, but it may be necessary to look into some requirements laid down on a lower, administrative level.

7.3 Technical recommendations

Data protection regulations stipulate that personal data can only be processed when it is – in short – acquired lawfully, sufficient to reach the goals it was collected for, relevant and not redundant. The technical architecture of FCInet can contribute to a use of personal data that is in accordance with the data protection regulations. In many regards the current design of FCInet does already contribute to this goal. Because of the encryption of the personal data the data is exchanged securely. And because there is only a match when both the sending and receiving organisation have the same information, the exchange of information is proportional, and restricted to what the receiving organisation needs to know. This can be seen as a form of 'privacy by design'. Nevertheless, there are some aspects of the FCInet system which could be improved.

A first recommendation is to draw up a protocol for the use of FCInet in which the data processing roles, rights and procedures are clearly defined. This protocol could be used by all partners of FCInet. Such a protocol prevents an unjustified use of FCInet. With a protocol, information rights, access rights and the right to rectification or erasure can be set forth. The architecture of FCInet must be such that there are procedures in place ensuring that these rights can be effectively exercised, and that the results of exercising these rights are implemented in practice.

A second recommendation is to limit the retention period of a filter to a certain period of time. Data protection regulations demand that personal data should be kept up to date. In addition, personal data should not be kept for a period longer than necessary to reach the goals for which the data was collected. These regulations are breached when personal data is kept for an unlimited amount of time. FCInet's design should prevent the use of old filters. A method for this could be to give each filter a time limit after which it self-destructs. This time limit could for instance be six months, because after six months much of the information in the filter will be outdated. While the exact time limit is not unimportant, it is perhaps more important that a reasoned decision about the time limit is made.

In addition to this time limit, it is also desirable to make sure that back-ups of old filters cannot be used to check for matches. In the system of FCInet, old filters are destroyed when new filters are created. However, receiving organisations are able to make back-ups and store those outside the FCInet program. When these old back-ups could be used to check for matches, it is possible that a match is based on obsolete information. A solution would be to prevent the use of a filter, before a check is done whether a new version of this filter is available.

7.4 Legal recommendations

7.4.1 Research findings

The competences, duties and restrictions that apply to the participants in FCInet when they spontaneously supply personal data, can be found in national and international laws and regulations. The competence to supply information to foreign partners is solely a matter of national law. Duties and restrictions can be found in national and international law. The starting point is that sovereign nations are free to decide if, and if so, under what conditions national organisation are allowed to spontaneously supply information with (organisations) in foreign nations. Whether a legal basis in an international law is necessary to enable the spontaneous supply of information depends on whether the national law of the participating organisations requires such a basis. In addition, international treaties about the exchange of information can limit the freedom of nations to freely decide on this topic.

Strikingly, most of FCInet operations seem to be able to be carried out under the Convention on Mutual Administrative Assistance in Tax Matters, for they involve matters of taxation of either an administrative or criminal law nature, and the FCInet participants involved are competent authorities under this convention.

National laws of the participating authorities mostly do not require a basis in international law for the spontaneous supply of information or a request for information. If national law does not require a treaty basis it is therefore not strictly necessary to identify an international instrument with provisions about the spontaneous supply of information. Nevertheless, a common international legal basis may clarify mutual commitments. In addition the current national provisions about the spontaneous supply of information are to a large extent based on international treaties. It is therefore advisable to take the international framework about the spontaneous supply of information into account.

Some international treaties create a duty for the signatories to spontaneously supply information. Among others, Article 7 of the EU Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (the Swedish Framework Decision) contains the obligation to share information in cases where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of criminal offences. Also several tax treaties create the obligation to spontaneously supply information that may lead to the rectification of a loss of tax in another state. These obligations can limit the freedom of nations to decide whether or not the spontaneous supply of information is desirable. With FCInet, the partner organisations comply with the international duties to share information which could assist in the investigation of criminal offences or tax fraud.

The scope of the national and international competences, duties and restrictions to share information by FCInet participants depends largely on the characteristics of the partner organisation. The partner organisations are quite divergent in nature. The Dutch FIOD is an organisation whose primary focus is the investigation of criminal offences. The British HRMC combines the duty to carry out criminal investigations with general duties lying within the fiscal domain and giving it the authority to collect taxes and manage the application of fiscal and customs provisions. The Swedish Tax Agency is quite similar to that, in combining a mandate to administer taxes with competences to investigate criminal offences, not completely restricted to tax offences. Some other organisations, such as the partner organisations in Iceland, Australia, Canada and the United States, do operate in the criminal law domain but solely in order to investigate criminal tax offences. The other partner organisations, the ones in Belgium, Norway, Denmark and Finland, are first and foremost a fiscal authority charged with upholding the laws on taxation in an administrative capacity. Although it is possible to argue that the imposition of tax surcharges as carried out by those organisations could be considered as amounting to a criminal charge, this does not mean that these organisations collect and processes information for the purpose of a criminal

investigation. Because the partner organisations of FCInet are active in different legal contexts, different sets of regulations are applicable. To some, regulations within the context of criminal law are applicable, while others fall under the regulations within the context of administrative and/or tax law.

Within the administrative law context there are some treaties and conventions that provide a basis for the spontaneous exchange of information and the exchange of information on request for the purpose of the levying of taxes. Most notable are the Convention on Mutual Administrative Assistance in Tax Matters. Within the European Union an additional basis is the EU Directive 2011/16/EU on administrative cooperation in the field of taxation. Another EU basis is the EU Regulation about the spontaneous supply of personal data with regard to certain tax categories: the Council Regulation (EU) 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax. These treaties could be used by administrative (tax) authorities.

Within the criminal law context there are also treaties and conventions that provide a basis for the spontaneous exchange of information and the exchange of information on request for the purpose of the investigation of criminal investigations. The main source is the Swedish Framework Decision. Article 7 makes it obligatory to spontaneously share information that could assist in the detection, prevention or investigation of offences about criminal offences listed in the Framework Decision on the European Arrest Warrant (the so-called list offences). Many of these crimes fall within the areas of competence of the participants in FCInet, although there are some crimes missing. In Article 5 the exchange of information on request is provided for. In addition to the Framework Decision, Article 7 of the 2000 EU Convention on Mutual Assistance in Criminal Matters can also provide a basis for the spontaneous supply of information relating to criminal offences by competent authorities, and Article 6 of that Convention can provide a basis for the exchange of information on request. The authorities competent under this Convention can include police organisations, but only for the spontaneous exchange of information. Whether national law grants them the competence to spontaneously share information is another matter to which national provisions apply. For the exchange of information on request, a judicial authority is needed. The application of this Convention is not limited to a certain list of offences. The exchange can be done by competent law enforcement agencies. Since not all FCInet participants that wish to share information within the criminal law sphere are designated as competent authorities, this merits attention. More or less the same applies to the exchange of information on request following a match. As regards this, it is much less problematic which legal framework applies as it is quite straightforward to classify FCInet operations as a particular form of international cooperation – much more so than it is to classify the initial exchange of a filter as a form of spontaneous exchange of information.

The legal context in which the partners of FCInet are active has also consequences on a national level. For FCInet participants that are regarded as a (special) criminal investigation service, all personal data collected and processed are regarded as criminal law or police data under national law. National laws on the processing of investigative data can provide a basis for the spontaneous supply of criminal law data to investigative authorities in EU Member States. It can be much more problematic to supply investigative data to purely administrative authorities. Conversely, national laws on the processing of administrative (tax) data may enable FCInet participants that are active in the administrative (tax) domain to exchange data with other FCInet partners in that domain, but may impose quite strict restrictions on the supply of data that is processed for administrative (tax) purposes to FCInet partners for the purposes of a criminal investigation. Also, international legal instruments very rarely provide for possibilities to share information in a 'cross-domain' fashion.

7.4.2 Recommendations

The main conclusion of the early stage of the research was that there seems to be no legal basis for the spontaneous supply of information between different legal domains,

i.e. between the criminal law domain and the administrative law domain. This finding is already acted upon by FCInet, but remains valid. Because of the purpose limitation provisions in almost all international and national (data protection) regulations, information can only be supplied if it is used for the purposes it was supplied for. This will either be a purpose of criminal investigations or administrative/tax purposes, but not both. As a consequence, in an early stage of this research it was recommended that FCInet should avoid the exchange of personal data between the FCInet participants active in the criminal law domain on the one hand and FCInet partners working in the administrative law domain on the other hand.

As a consequence of the endorsed recommendation in the preliminary report, FCInet is now split in two separate information exchange networks. One network focuses on the exchange of information for the purpose of criminal investigations, while another network focuses on the exchange of information for taxation purposes. These networks presumably still have the same technical architecture, which could be designed in such way that is only allowed to exchange information between participants who would be legally authorised to perform this exchange. A similar technical architecture could in the future allow the exchange of filters between certain participants of the two networks, if it would be established that such exchange would be allowed.

The second conclusion of the research is that – although mostly unnecessary – a common international legal basis could be desirable. Such a common legal basis could clarify the mutual commitments and it could also enable the exchange of information between two partners who are currently not competent to share this information. A long term solution would be the drawing up of an FCInet treaty. This treaty could provide a basis to exchange information across contexts. However, the drawing up of such a treaty could prove to be a real challenge, because of the nature of the information exchanged. A slightly more modest proposal is that a network of bilateral Memoranda of Understandings could be drawn up. For every set of two members of the network a Memorandum of Understanding could be made, detailing the information that could be exchanged and the foundations on which this exchange is made. With the help of these Memoranda of Understanding the possibilities to exchanges information between the context of criminal law and administrative (tax) law could also be outlined.

A third conclusion of this research is that there are already some international bases for the spontaneous supply of information within the criminal law context, but that none of these treaties fit completely. The most important basis is the Swedish Framework Decision. This instrument has the potential to be a sound foundation for the spontaneous supply of information and for the exchange of information following a match, but there are some obstacles that prevent an optimal use of the Swedish Framework Decision. The first obstacle is the fact that some FCInet participants in the criminal law domain are not designated as competent authority. As a consequence, the powers of the Swedish Framework Decision are not directly available. In itself this would not be a real obstruction if national regulations include the competence to spontaneously supply information. A second obstacle is the fact that only information about the so-called list facts can be exchanged. This means that information about certain categories of criminal offences, especially less serious criminal offences, cannot be exchanged. Other options for exchange include the EU Convention on Mutual Assistance in Criminal Matters, which includes a legal basis for the spontaneous exchange of information (Article 7) and for requests for information following a match (Article 6). Operations with the United Kingdom continue to be possible on the basis of Article 563 of the Trade and Cooperation Agreement.

The international legal framework for FCInet operation in the administrative (tax) domain is clear and coherent: the OECD/Council of Europe Convention on Mutual Administrative Assistance in Criminal Matters offers an international legal basis for both the spontaneous exchange of information (Article 7) and the exchange of information on request (Article 5). The national laws of the organisations participating in FCInet seem to provide an adequate basis for these organisations to use FCInet for purposes of exchanging administrative information on matters of taxation.

Annex 1: Matrix for the Tax Domain

This matrix shows options for spontaneous exchange of information (Spon), exchange of information on request (Request) in tax matters and exchange of information in custom matters, both spontaneous and on request (Cus). The matrix does not include criminal tax matters (Annex 2). The matrix offers a simplified summary of the results mentioned in the main report.

Receiving organisation / *Sending organisation*	Australia: Australian Taxation Office	Belgium: Special Tax Inspectorate	Canada: Canadian Revenue Agency	Denmark: Danish Tax Agency	Finland: Finnish Tax Administration
Australia: Australian Taxation Office		Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Belgium: Special Tax Inspectorate	Spon: 7 MAC Req: 5 MAC		Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII
Canada: Canada Revenue Agency	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC		Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Denmark: Danish Tax Agency	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon: 7 MAC Req: 5 MAC		Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII
Finland: Finnish Tax Administration	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	
Iceland: Directorate of Tax Inv.	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Netherlands: Fiscal Int. and Inv. Service					
Norway: Norwegian Tax Administration	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Sweden: Swedish Tax Agency	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII
UK: Her Majesty's Rev. and Customs	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
US: Internal Revenue Service[131]	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC

MAC = Convention on Mutual Administrative Assistance in Tax Matters
EU = Council Directive 2011/16/EU on administrative cooperation in the field of taxation
NII = Convention on Mutual Assistance and Cooperation between Customs Administrations (Naples II).

—

[131] Information can only be used in a criminal court after authorisation by the sending organisation.

Iceland: Directorate of Tax Investigations	Netherlands: Fiscal Intelligence and Investigation Service	Norway: Norwegian Tax Administration	Sweden: Swedish Tax Agency	United Kingdom: Her Majesty's Revenue and Customs	United States: Internal Revenue Service
Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC		Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon:7 MAC/9 EU Req: 5 MAC/5 EU Cus: 10/17 NII	Spon: 7 MAC Req: 5 MAC		Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC		Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	

Red = Supply of information is not possible
Light green = Supply of information is possible based on the MAC
Dark green = Supply of information is possible based on the MAC and EU law

Annex 2: Matrix for the Criminal Law Domain I - Tax

This matrix shows options for spontaneous exchange of information (Spon), exchange of information on request (Request) in criminal tax matters.

Receiving organisation / *Sending organisation*	Australia: Australian Taxation Office	Belgium: Special Tax Inspectorate	Canada: Canadian Revenue Agency	Denmark: Danish Tax Agency	Finland: Finnish Tax Administration
Australia: Australian Taxation Office		Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Belgium: Special Tax Inspectorate					
Canada: Canada Revenue Agency	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC		Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Denmark: Danish Tax Agency	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC		Spon:7 MAC Req: 5 MAC
Finland: Finnish Tax Administration	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	
Iceland: Directorate of Tax Inv.	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Netherlands: Fiscal Int. and Inv. Service	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC
Norway: Norwegian Tax Administration	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Sweden: Swedish Tax Agency	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC
UK: Her Majesty's Rev. and Customs	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
US: Internal Revenue Service[132]	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC

MAC = Convention on Mutual Administrative Assistance in Tax Matters
EU = Council Directive 2011/16/EU on administrative cooperation in the field of taxation

—

[132] Information can only be used in a criminal court after authorisation by the sending organisation.

Iceland: Directorate of Tax Investigations	Netherlands: Fiscal Intelligence and Investigation Service	Norway: Norwegian Tax Administration	Sweden: Swedish Tax Agency	United Kingdom: Her Majesty's Revenue and Customs	United States: Internal Revenue Service
Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC		Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC		Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon:7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC		Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC		Spon: 7 MAC Req: 5 MAC
Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	Spon: 7 MAC Req: 5 MAC	

Red = Supply of information is not possible
Light green = Supply of information is possible based on the MAC

Annex 3: Matrix for the Criminal Law Domain II – other offences

This matrix shows options for the spontaneous exchange of information (Spon) and for exchange of information on request (Request). It offers a simplified summary of the results mentioned in the main report. Criminal tax matters are included in the matrix in Annex 2.

<table>
<tr><td>Receiving organisation
Sending organisation</td><td colspan="2">Netherlands: Fiscal Intelligence and Investigation Service</td><td colspan="2">Sweden: Swedish Tax Agency</td><td colspan="2">United Kingdom: Her Majesty's Revenue and Customs</td></tr>
<tr><td rowspan="2">Netherlands: Fiscal Intelligence and Investigation Service</td><td colspan="2" rowspan="2"></td><td>Spon</td><td>Request</td><td>Spon</td><td>Request</td></tr>
<tr><td>Art. 7 FD (no competent authority) / Art. 7 EU MLA Conv.</td><td>Art. 5 FD (no competent authority) / Art. 6 EU MLA Conv.</td><td>Art. 563 TCA (possibly no competent authority)</td><td>Art. 563 TCA (possibly no competent authority)</td></tr>
<tr><td rowspan="2">Sweden: Swedish Tax Agency</td><td>Spon</td><td>Request</td><td colspan="2" rowspan="2"></td><td>Spon</td><td>Request</td></tr>
<tr><td>Art. 7 FD (no competent authority) / Art. 7 EU MLA Conv.</td><td>Art. 5 FD (no competent authority) / Art. 6 EU MLA Conv.</td><td>Art. 563 TCA (possibly no competent authority)</td><td>Art. 563 TCA (possibly no competent authority)</td></tr>
<tr><td rowspan="2">United Kingdom: Her Majesty's Revenue and Customs</td><td>Spon</td><td>Request</td><td>Spon</td><td>Request</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>Art. 563 TCA</td><td>Art. 563 TCA</td><td>Art. 563 TCA</td><td>Art. 563 TCA</td></tr>
</table>

FD = Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union
EU MLA Conv. = Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union
TCA = Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part

Orange = Supply of information is possible, but organisation is not a competent authority
Green = Supply is possible

Annex 4: Questionnaire

Introduction

This questionnaire is intended to gather information which can be used by the researchers to compose an overview of the legal framework for FCInet. It contains questions on the national and international legal rules that enable organisations to participate in FCInet, or that constrain them. The results from this questionnaire are processed by the research team of the University of Groningen, who have been contracted by the FCInet secretariat to conduct an analysis of the relevant legal framework. In order to fulfil this task, the research team depends on the cooperation of (potential) participants in the project. In this phase of the research, that includes organisations from Denmark, Sweden, Finland, Norway and Iceland. In a previous phase, the legal framework for the participating organisations from Belgium, the Netherlands, and the United Kingdom has already been analysed. Currently, there is additional research under way involving a study into the legal framework for the participating organisations from Australia, Canada and the United States. These three countries have responded to an identical questionnaire as this one.

Your organisation is kindly requested to fill in this questionnaire. As the research team is mostly unfamiliar with the national laws of the participating organisations, we are dependent on your kind and much valued cooperation. The answers provided in this questionnaire will be helpful for the research team in making a comprehensive overview of the possibilities and complications for the spontaneous exchange of personal data between organisations participating or willing to participate in FCInet and the handling of resulting requests for mutual legal assistance.

If anything is unclear, the research team is of course willing to provide further explanation. If the research team, in compiling the results, encounters information that remains ambiguous or incomplete, the participating organisation may be approached to provide further elaboration.

There are no limitations in the number of words that you use in framing your answers. You can use this document and write your answers below the (italicized) questions. There is no need to use Word's 'track changes' option.

If you have filled in this questionnaire, you are kindly requested to send the document to w.geelhoed@rug.nl.

Thank you very much for filling in this questionnaire!

A. Data protection regulations in general (international and national)

The data shared within the framework of FCInet should be regarded as (pseudonymised) personal data. Therefore the national and international data protection laws and regulations that are applicable to the (potential) FCInet participant contain the conditions for the exchange of personal data through FCInet.

1. Is the state signatory to an international (whether global or regional) treaty or agreement which contains binding personal data protection provisions? If so, which?

Note: Examples of binding data protection regulations are: The Council of Europe Data Protection Convention of 1981 (Convention 108), the European Union General Data

Protection Regulation (GDPR) (Regulation (EU) 2016/679), the European Union Directive on Data Protection in criminal matters (Directive (EU) 2016/680), the African Union Convention on Cyber-security and Personal Data Protection, the ECOWAS Supplementary Act A/SA.1/01/10 on data protection, or trade agreements like the Trans-Pacific Partnership Agreement (TPP).

2. For what purpose was the personal data that is exchanged through FCInet initially gathered?

Note: The purpose for which the personal data was gathered can influence which treaty or agreement is applicable. Within the EU, the Directive is applicable if the data was gathered for criminal purposes, while the GDPR is applicable if the data was gathered for other purposes (such as tax purposes).

B. Obligations in the applicable international data protection regime

3. Which obligations are laid down in the applicable international data protection regulations regarding the gathering and processing of personal data?

4. Which obligations are laid down in the applicable international data protection regulations regarding the preservation and storage of personal data?

5. Which obligations are laid down in the applicable international data protection regulations that limit the (further) processing of gathered data to specific purposes?

6. Which obligations are laid down in the applicable international data protection regulations regarding the rights of data subjects?

7. Which other obligations are laid down in the applicable international data protection regulations that could be relevant to FCInet and that have not been mentioned in questions 3-6?

C. Obligations in the national data protection regime

8. Which obligations are laid down in the applicable national data protection regulations regarding the gathering and processing of personal data?

9. Which obligations are laid down in the applicable national data protection regulations regarding the preservation and storage of personal data?

10. Which obligations are laid down in the applicable national data protection regulations that limit the (further) processing of gathered data to specific purposes?

11. Which obligations are laid down in the applicable national data protection regulations regarding the rights of data subjects?

12. Which other obligations are laid down in the applicable national data protection regulations that could be relevant to FCInet and that have not been mentioned in questions 8-11?

D. International legal bases for the spontaneous exchange of personal data in general

Within the framework of FCInet, personal data is spontaneously exchanged between the participating organisations. Therefore, an international legal basis for FCInet can be found in treaties that allow the spontaneous supply and receipt of personal data between organisations in different countries.

Not all countries require an international legal basis for the spontaneous supply or receipt of personal data. Without this requirement it is not strictly necessary to answer the questions about the international treaties that can serve as a legal basis for FCInet. Nevertheless, in order to clarify mutual commitments it can be desirable to find a common legal basis for the spontaneous exchange of personal data if the sending and receiving organisations are in different countries.

Additionally, because of purpose limitations that can prevent the exchange of information between the domains of criminal matters and tax matters, different treaty bases are relevant for the spontaneous exchange of information in criminal matters (questions 15-20) and in administrative(/tax) matters (questions 21-26)

13. Does your national law require an international legal basis for the spontaneous supply of personal data and/or receipt of spontaneously supplied personal data?

14. For what purpose was the personal data gathered that is to be exchanged?

E. The international legal framework for the spontaneous exchange of information in criminal matters

15. Is the state signatory to a multilateral treaty or framework that allows the spontaneous supply of personal data in criminal matters, whether as a general mode of cooperation or for specific purposes of cooperation? If so, which?

Note: Within the European context there are several examples of treaties that allow the spontaneous exchange of personal data for broad purposes. These treaties include: the Second Protocol to the 1959 Convention on Mutual Legal Assistance of the Council of Europe, the Convention Implementing the Schengen Agreement, the 2000 EU Convention on Mutual Assistance and the Framework Decision 2006/960/JHA (Swedish Framework Decision).

In addition there are some multilateral treaties that allow the spontaneous exchange of personal data for specific purposes. An example is the 2005 Convention on Proceeds of Crime and Financing of Terrorism of the Council of Europe which allows the spontaneous exchange of personal data for the purpose of the identification of instrumentalities and proceeds of crime.

16. For which goals is the exchange of personal data in criminal matters allowed, according to the international legal framework as indicated in the answer to question 15?

17. Is the exchange of personal data, as envisaged in FCInet, relevant to reach these goals?

18. Which authority is designated as 'competent authority' to exchange personal data in criminal matters in the context of the international legal framework as indicated in the answer to question 15?

19. For which criminal offences is the exchange of personal data allowed, according to the international legal framework as indicated in the answer to question 15?

20. Are there any other conditions in the international legal basis for the spontaneous exchange of information in criminal matters that have not been mentioned in the answers to questions 16-19?

F. The international legal framework for the spontaneous exchange of information in tax/administrative matters

21. Is the state signatory to a multilateral treaty or framework that allows or obliges the spontaneous supply of personal data in tax/administrative matters? If so, which?

Note: Examples – within the European context – are: the European Union Convention on Mutual Assistance and Cooperation between Customs Administrations (Naples II), the Council of Europe Convention on Mutual Administrative Assistance in Tax Matters, the European Union Council Regulation on Cooperation in Matters of Value Added Tax (Regulation (EU) 94/2010) and the European Union Council Directive on Administrative Cooperation in Tax Matters (Directive (EU) 2011/16). This Directive (EU) 2011/16 contains an obligation to spontaneously exchange information.

22. For which goals is the exchange of personal data in tax/administrative matters allowed, according to the international legal framework as indicated in the answer to question 21?

23. Is the exchange of personal data, as envisaged in FCInet, relevant to reach these goals?

24. Which authority is designated as 'competent authority' to exchange personal data in tax/administrative matters, in the context of the international legal framework as indicated in the answer to question 21?

25. For which administrative decisions or acts is the exchange of personal data allowed, according to the international legal framework as indicated in the answer to question 21?

26. Are there any other conditions in the international legal basis for the spontaneous exchange of information in tax/administrative matters that have not been mentioned in the answers to questions 22-25?

G. National legal basis for the spontaneous exchange of personal data

The rule of law requires that powers of state authorities are defined in national legal provisions. This includes the responsibilities and competences of national criminal law enforcement authorities and of tax/administrative authorities.

27. Is there a legal basis in your national law for the spontaneous exchange of personal data with foreign organisations? If so, please indicate which provisions are relevant.

Note: National regulations on spontaneous exchange of personal data with foreign organisations may overlap with (inter)national data protection regulations. Also, there may be different data protection regulations in the domain of criminal matters and the domain of tax matters or administrative matters in general. Finally, there may be differences between the rules on supplying and on receiving personal data. For these reasons, more detailed subquestions are provided below.

28. Is your national authority allowed to spontaneously supply personal data to other (foreign) organisations for the purpose of criminal investigations? If so, under what conditions?

29. To what (categories of) organisations can personal data in criminal matters be supplied?

30. For which goals is the supply of personal data in criminal matters allowed?

31. Is the supply of personal data, as envisaged in FCInet, relevant to reach these goals?

32. For which criminal offences is the supply of personal data allowed?

33. Is your national authority allowed to spontaneously receive personal data from other (foreign) organisations for the purpose of criminal investigations? If so, under what conditions?

34. From what (categories of) organisations can personal data in criminal matters be received?

35. For which goals is the receipt of personal data in criminal matters allowed?

36. Is the receipt of personal data, as envisaged in FCInet, relevant to reach these goals?

37. For which criminal offences is the receipt of personal data allowed?

38. Is your national authority allowed to spontaneously supply personal data to other (foreign) organisations for the purpose of tax or administrative oversight? If so, under what conditions?

39. To what (categories of) organisations can personal data in tax/administrative matters be supplied?

40. For which goals is the supply of personal data in tax/administrative matters allowed?

41. Is the supply of personal data, as envisaged in FCInet, relevant to reach these goals?

42. For which tax/administrative offences is the supply of personal data allowed?

43. Is your national authority allowed to spontaneously receive personal data from other (foreign) organisations for the purpose of tax or administrative oversight? If so, under what conditions?

44. From what (categories of) organisations can personal data in tax/administrative matters be received?

45. For which goals is the receipt of personal data in tax/administrative matters allowed?

46. Is the receipt of personal data, as envisaged in FCInet, relevant to reach these goals?

47. For which tax/administrative offences is the receipt of personal data allowed?

H. Legal bases for follow-up exchange of information (international and national)

When a participant finds a match, it may wish to inquire with the sending participant whether that participant has additional information on the person or subject with respect to whom the match occurred. The question is whether this is allowed under national and international law. In order to adequately decide on this, one must distinguish between exchange of information in criminal law matters and in administrative matters. Furthermore, in both contexts there can be differences between requesting for information on the one hand and supplying information on the other hand. Usually, requesting information is less regulated than supplying information. Lastly, in order to analyse the legal bases for exchange of information, we distinguish between three issues: whether there is a legal basis in national law, whether national law requires a basis in international law for exchanging information, and whether the national authority is a competent authority for using that international legal basis.

48. Does your national law offer a legal basis for sending a request for information to other (foreign) organisations in criminal law matters?

49. Is your national authority a competent authority for sending a request for information to other (foreign) organisations in criminal law matters?

50. Does your national law require a basis in international law for sending a request for information to other (foreign) organisations in criminal law matters?

51. What other conditions, according to your national law, are relevant for the sending of a request for information to other (foreign) organisations in criminal law matters?

52. Does your national law offer a basis for supplying information on the basis of a request by another (foreign) organisation in criminal law matters?

52. Is your national authority a competent authority for supplying information to other (foreign) organisations in criminal law matters?

54. Does your national law require a basis in international law for supplying information to other (foreign) organisations in criminal law matters?

55. What other conditions, according to your national law, are relevant for supplying information to other (foreign) organisations in criminal law matters?

56. Does your national law offer a legal basis for sending a request for information to other (foreign) organisations in tax/administrative matters?

57. Is your national authority a competent authority for sending a request for information to other (foreign) organisations in tax/administrative matters?

58. Does your national law require a basis in international law for sending a request for information to other (foreign) organisations in tax/administrative matters?

59. What other conditions, according to your national law, are relevant for the sending of a request for information to other (foreign) organisations in tax/administrative matters?

60. Does your national law offer a basis for supplying information on the basis of a request by another (foreign) organisation in tax/administrative matters?

61. Is your national authority a competent authority for supplying information to other (foreign) organisations in tax/administrative matters?

62. Does your national law require a basis in international law for supplying information to other (foreign) organisations in tax/administrative matters?

63. What other conditions, according to your national law, are relevant for supplying information to other (foreign) organisations in tax/administrative matters?

I. Prospects for further development of the legal framework

It may be the case that the current legal framework provides difficulties for organisations willing to participate in FCInet. These will probably be described in the answers to the questions posed above, but if you feel that you have not been able to describe these completely, you are invited to explain any problematic issues that remain.

64. What other issues provide legal difficulties for your organisation's participation in FCInet?

The research team is also requested to advise on the future development of the legal framework of FCInet, such as the framing of a new multilateral treaty, of bilateral memoranda of understanding, or anything else which may be of benefit in shaping the legal framework. It may be the case that you have particular preferences in that regard, or that certain options are, in your view, less preferable.

65. Which possible developments in the legal framework for FCInet would you find preferable? And which would you find less preferable?

J. Other comments

66. Are there any other comments you wish to make?

Annex 5: Country Reports

Australia

Member organization: The Australian Taxation Offices (ATO)

In which domain falls the information the organization wants to share spontaneously?

- The ATO wants to share information in both domains: TAX and CRIMINAL.

Domain TAX

1. What kind of information is to be shared?

– Data that has been collected by the ATO in its administrative function. This includes data from taxpayers and third parties for the purpose of making assessments of tax (income, VAT and so forth). Officers can also obtain evidence of criminal tax offences by way of the Search and Seizure Warrants where suspicion or evidence that a taxpayer has committed a tax related criminal offence exists. Thus, where the ATO has reasonable suspicion that information collected by way of its administrative function could relate to tax crime offences committed in another jurisdiction, the information will also be shared with the approval of the competent authority. Information obtained during Search and Seizure warrant executions are subject to other international treaties and domestic criminal (enforcement) bodies. In these cases information seized under the warrant relating to non- tax crimes will not be shared.

2. Is there a legal basis to share this information spontaneously?

a. In national law?

– The ATOs ability to exchange information is governed by the Taxation Administration Act 1935. Within Division 355 of this act, it is a criminal offence for a taxation officer to disclose ATO Protected Information under specific conditions.

Furthermore, the act limits the ATO's ability to exchange ATO Protected Information to countries with whom they have an international tax treaty (MMA, DTA or TIEA) which then provide a legal basis for the spontaneous exchange of information.

b. In international law?

– Under the Taxation Administrative act, the exchange of ATO Protected Information internationally has been explicitly limited to the use of Tax Treaties that Australia is signatory to. The three legal instruments under which an exchange of information is currently permitted in Australia are the Tax Information Exchange Agreements (TIEAS), Double Taxation Conventions (DTC/DTA) and the Convention on Mutual Administrative Assistance in Tax Matters (MAC).

Australia's DTCs and the MMA both provide a legal basis for the spontaneous exchange of information for criminal tax matters.

3. Under what conditions can the information be shared spontaneously?

a. Conditions in national law regarding international cooperation

– The ATO can only exchange information with other Revenue Authorities (incl. Criminal investigation arms) with whom Australia has a treaty or information exchange agreement.

Additionally, the ATO is allowed to receive and supply information, as all the agreements provide for reciprocity of exchange.

As long as the other foreign agency has a legal framework with Australia to share and exchange information directly, it is able to do so. Yet, usually these are limited to international revenue agencies or domestic law enforcement agencies. The ATO is allowed to exchange information as is relevant to carrying out the provisions of the

Agreement of the administration or enforcement of the domestic laws regarding taxes covered by the Agreement.

b. Conditions in international law regarding international cooperation

- Under Art. 4 of the MAC the parties shall exchange information that is foreseeably relevant for the administration or enforcement of their domestic laws concerning the taxes covered by the Convention. Furthermore, the various DTCs and DTAs that Australia is party to, contain specific rules on the exchange of information, generally in Art. 25 or Art. 27 respectively. However, nothing in these articles is contrary to the use of information for FCInet.

c. Conditions in national privacy law/ Conditions in international privacy laws

- Personal data collection is subject to the Privacy Act 1988 which contains the Australian Privacy Principles (APPs). The Office of the Australian Information Commissioner administers the APPs including investigations into their contravention. Moreover, all the treaties mentioned in q2(b) entered into Australian law including their confidentiality provision which require information exchanged to be treated as secret in the same manner as information obtained under domestic law. Similarly, any information exchanged by international partners becomes, by definition ATO Protected Information and is thus provided with all the safeguards of Division 355.
- All the information that will be exchanged with the ATO by international partners, including FCInet, becomes by definition ATO Protected Information and is then subject to all the domestic safeguards per the Taxation Administration Act and the APPs.

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences

- All of the relevant international agreements that Australia is signatory to contain provisions on the ATO's ability to further share data received under the treaties. In general, these provisions stipulate that the ATO will not further share information without the express approval of the original agency.

Moreover, the information received under the tax treaties can only be used for the purposes provided for in the treaty.

5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?

- The MAC as well as the DTCs that Australia is party to allow for sending request for information on tax and/or administrative matters. The Commissioner of Taxation (or an authorized representative) is the competent authority to carry out this task for both civil and criminal tax matters. Furthermore, the ATO may only send request for information relating to criminal tax matters to other revenue authorities with whom they have an exchange agreement for information with.

6. What is the procedure when the sending organization/ Country receives a request for follow-up information after a hit?

a. Procedure under national law

- The ATO may only supply information relating to tax and/or administrative matter to other revenue authorities with whom they have an exchange of information agreement.

b. Procedure under international law

– The MAA as well as the DTCs that Australia is party to allow for supplying information in relation to a request from another foreign organization for tax and/or administrative matters. The Commissioner of Taxation (or an authorized representative) is the competent authority to carry out this task for tax and/or administrative matters.

Domain CRIMINAL

1. What kind of information is to be shared?

- Only information related to tax crimes. The ATO does not have the authority to share information on non- tax criminal offences. (cf. q1 in domain TAX)

2. Is there a legal basis to share this information spontaneously?

a. In national law?

- The Taxation Administration Act 1953 limits the ATO's ability to exchange ATO Protected Information to countries with whom they have an international tax treaty (MAC, DTA or TIEA) which then provide a legal basis for the spontaneous exchange of information in criminal tax matters.

b. In international law?

- The DTCs and MAC that Australia is party to provide a legal basis for the exchange of information of personal data for criminal tax matters.

3. Under what conditions can the information be shared spontaneously?

a. Conditions in national law regarding informational cooperation

- The information can only be shared with other revenue agencies, including the criminal investigation arms, which Australia has an information exchange agreement with. The supply of ATO Protected Information must be for the purposes of criminal tax offences (such as VAT and Excise) as specified in the relevant treaties only. Similarly, the ATO may receive information on criminal investigations as long as it is for tax crime investigations only.
- The ATO is able to receive information from Australia's domestic Law Enforcement Agencies that has been shared with international agencies and relate to other criminal offences not relating to the administration of taxation. The ATO may receive this information for the purpose of protecting public finances of Australia by ensuring appropriate safeguards are in place. This type of exchange of information is governed by the Taxation Administration Act of 1953 as well as 'on- sharing' restrictions from partners of the ATO and any restrictions imposed by the originating jurisdiction.

b. Conditions in international law regarding international cooperation

- The tax treaties that Australia is party to allow information to be exchanged as is relevant for carrying out the provisions of the Agreement or the administration or enforcement of the domestic law regarding taxes covered by the agreement. Thus, the ATO may exchange information that has been collected in the exercise of its functions that may be evidence of a tax crime in the country that receives information. It is entirely up to the receiving country to determine which purpose the information exchanged in FCInet is utilized.
- The exchange of information under the tax treaties relates only to criminal tax offences. If the ATO comes into possession of information on non- tax crime offences, the information has to be disclosed to the Australian Criminal Intelligence Commission or the Australian Federal Police Agencies under their own treaties.

c. Conditions in national and international privacy laws

- Same as Domain TAX

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain?

- Same as Domain TAX

5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?

a. Procedure under national law

b. Procedure under international law

- The MAC and DTCs entered into by Australia allow for sending requests for information for civil and criminal tax purposes. Thus, the ATO is the competent authority

to send requests on criminal tax matters to other foreign competent authorities, with whom Australia has such an exchange agreement.

No other conditions apply if the information relates to criminal offences involving taxation to revenue systems covered by the treaty purposes.

6. What is the procedure when the sending organization/country receives a request for follow-up information after a hit?

a. Procedure under national law

– There is no need for a national legal basis to supply information, as it is covered by the relevant tax treaty.

b. Procedure under international law

- The MAC and DTCs entered into by Australia allow for supplying information in relation to a request of a foreign organization for civil and criminal tax purposes. This relates to criminal tax matters only.

Belgium

Member organization: BBI – Special Tax Inspectorate (*Bijzondere Belastinginspectie)*

In which domain falls the information the organization wants to share spontaneously?

Domain TAX

1. What kind of information is to be shared?
   - Any form of taxation information.
2. Is there a legal basis to share this information spontaneously?
   a. In national law?
      - Art. 9 of the EU Directive 2011/16/EU has been incorporated into Belgian law by Art. 338 of the *Wetboek van de Inkomstenbelastingen 1992* (WIB 1992).
   b. In international law?
      - There are several provisions that allow for the spontaneous exchange of information between the EU Member States and furthermore with third countries.
      - These include the 2011/16/EU Directive on administrative cooperation in the field of taxation and the Council Regulation 904/2010 on administrative cooperation and combating fraud in the field of value added tax. Furthermore, Belgium is signatory to the Treaty on Mutual Administrative Assistance in Tax Matters.
      - Lastly, Belgium and the USA entered into a bilateral agreement, the Double Taxation Treaty Belgium-US, which allows for the spontaneous exchange of information in Art. 25.
3. Under what conditions can the information be shared spontaneously?
   a. Conditions in national law regarding international cooperation
      National law does not require an international legal basis for sharing.
   b. Conditions in international law regarding international cooperation
      - Art. 7(1) of the Treaty on Mutual Administrative Assistance in Tax Matters places the condition of foreseeable relevance of the information on the authorities in question.
   c. Conditions in national privacy law/ Conditions in international privacy laws
      a. in international law: The Council of Europe Data Protection Convention of 1981 (Convention 108) and the European Union General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
      b. in national law:
      - W. 30/07/2018 zgn. Kaderwet http://www.ejustice.just.fgov.be/eli/wet/2018/07/30/2018040581/staatsblad
      - W. 03/08/20212 zgn. Privacywet Financiën, gewijzigd 05/09/2018 http://www.ejustice.just.fgov.be/eli/wet/2012/08/03/2012003257/justel

   The most important conditions: there must be a legal basis for processing, purpose limitation applies (although repurposing is possible) and processing must be kept to a minimum and within time limits. Data subjects have rights of information, inspection, rectification and erasure.

   For spontaneous exchange of information, foreseeable relevance is the most important criterion

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences
5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?

   This is explained in the document 'Handleiding Inkomstenbelastingen - Internationale uitwisseling van inlichtingen op verzoek'

   Essentially, the competent authority in Belgium can ask any information from an authority in another country within the provisions of a relevant international tax treaty and for the purposes of that treaty. There are standard forms, within the EU as well as outside of it.
6. What is the procedure when the sending organization/ Country receives a request for follow-up information after a hit?
   a. Procedure under national law and international law taken together

      This is explained in the document 'Handleiding Inkomstenbelastingen - Internationale uitwisseling van inlichtingen op verzoek'

      In these cases, there is communication between the authorities involved including statements of receipt, validity checks, possible refusal and status updates
   b. Procedure under international law

      see above

Domain CRIMINAL

1. What kind of information is to be shared?
2. Is there a legal basis to share this information spontaneously?
   a. In national law?
      - There is no legal basis for BBI officials to transfer information to a foreign prosecution service. It can only do so via the Belgian Public Prosecutor's Office (PPO) which has full access to the files of the BBI, while the BBI can only inform the PPO of facts that are punishable by criminal law according to the tax laws. If the Belgian PPO works on the file after Belgium has received information via taxation treaties, the PPO is still bound by the conditions that apply according to those treaties.
   b. In international law?
3. Under what conditions can the information be shared spontaneously?
   a. Conditions in national law regarding international cooperation
   b. Conditions in international law regarding international cooperation
   c. Conditions in national privacy law/ Conditions in international privacy laws
4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences
5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?
   a. Procedure under national law
   b. Procedure under international law
6. What is the procedure when the sending organization/ Country receives a request for follow-up information after a hit?

a. Procedure under national law

b. Procedure under international law

Canada

Member organization: The Canada Revenue Agency (CRA)

In which domain falls the information the organization wants to share spontaneously?
The CRA wants to share information in both domains. TAX and CRIMINAL

Domain TAX and CRIMINAL (the same provisions apply)

1. What kind of information is to be shared?
   - Tax information allowing for mutual administrative assistance in tax matters. The information further must relate to taxes stipulated in the Canadian Income Tax Act; for other tax information the CRA must ensure that the information relates to taxes that are permitted under all treaties or international agreements.

2. Is there a legal basis to share this information spontaneously?
   a. In national law?
      - The Canadian Income Tax Act (ITA) in subparagraph 241(4)(e)(xii) stipulates that an official may exchange tax information or allow access to such information solely based on a provision contained in a tax treaty with another country or in a listed international agreement. Furthermore, paragraph 8(2)(f) of the Canadian Privacy Act states that '(…) personal information under the control of a government institution may be disclosed under an agreement or arrangement between [the Canadian government and the foreign state's government] (…) for the purpose of administering or enforcing any law or carrying out a lawful investigation.' Moreover, the provision provides statutory authority for the CRA to participate in the exchange of information and release of information as long as it is consistent with the CRA's international commitments and within the existing legal framework under its tax treaties.

      Additionally, the relevant international instruments form part of the domestic law of Canada, after Parliament passes implementing legislation.

   b. In international law?
      - Canada is signatory to the Convention on Mutual Administrative Assistance in Tax Matters (MAC), as well as being part to tax treaties with 93 other jurisdiction which allow for the spontaneous exchange of information in criminal and civil tax matters.

      Moreover, Canada entered into 24 tax information exchange agreements (TIEA). All of these only allow for exchange of information on request, except for one.

      Canada is also signatory to the OECD Common Reporting Standard Multilateral Competent Authority Agreement (CRS MCAA) and the Multilateral Competent Authority Agreement on Exchange of Country- by-Country- Reports (CbC MCAA). The CRS MCAA is the international standard for tax administrations to automatically exchange financial account information approved by the OECD. The CbC MCAA similarly allows for the signatory states to automatically exchange country reports on global allocation of income, taxes paid, economic activity among tax jurisdiction in which multinational enterprises work.

3. Under what conditions can the information be shared spontaneously?
   a. Conditions in national law regarding international cooperation

- For both tax offences and tax (civil) administrative enforcement matters, subparagraph 24(4)(e)(xii) of the ITA provides statutory authority for the CRA to participate in the information exchange and release such information as long as the exchange is consistent with the CRA's international commitments and within the existing legal framework under its tax treaties, including the MAC. Most of the TIEAs only allow for exchange of information on request.

b. Conditions in international law regarding international cooperation

- Canada's bilateral tax treaties generally follow the OECD Model Tax Convention. Thus, the information exchanged by the CRA with other competent authorities of contracting States must be 'foreseeably relevant', 'necessary' or 'relevant' for carrying out the provisions of the treaties or to the administration or enforcement of the domestic laws concerning taxes to which the treaties apply. This applies to information exchanged under the bilateral tax treaties after 2005, the TIEAs as well as the MAC.

The competent authority under the bilateral treaties, TIEAs and the MAC is the Minister of National Revenue or the Minster's authorized representative(s).

The CRA may provide personal data to Canada's current treaty partners or to a foreign tax authority whom is also signatory to the MAC or the Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting (MLI) and for which either a Multilateral Competent Authority Agreement or a Bilateral Competent Authority Agreement exists between Canada and the foreign government.

Furthermore, the exchange of information either automatic, spontaneous or on request is allowed for all decision and acts related to carrying out the provision of the Treaties.

c. Conditions in national privacy law/ Conditions in international privacy laws

- Generally, information received under Canada's bilateral tax treaties must be treated as secret in the same manner as information obtained under the tax laws of the State and shall be disclosed only to persons or authorities who are involved in the assessment or collection, the administration and enforcement in respect of, or the determination of appeals in relation to the taxes to which the treaty applies.

- The bilateral and multilateral tax Conventions generally contain binding data safeguard provisions. Under the MAC, several conditions apply regarding secrecy of the information, such as Art. 22. Moreover, under the OECD instruments mentioned above in Q2(b) (the CRS MCAA and the CbC MCAA), all information that is exchanged under these agreements is subject to the confidentiality rules and safeguards provided in the MAC.

- Under the TIEAs, all information received thereunder must be treated as confidential. The confidentiality provisions of the TIEAs set out limited situations where disclosure of the relevant information is permitted.

- Within national law, the Federal Privacy Act stipulates the CRA's obligations with regard to the collection, retention and disposal of personal information. Under the Privacy Act and Privacy Regulations, the CRA retains the information used for administrative purposes for at least two years, or where a request for access has been received until such time as the individual has had the opportunity to exercise all his/ her rights under the Access to Information Act.

- Furthermore, Section 8 of the Canadian Charter of Rights and Freedoms protects the privacy interests and rights of individuals against unreasonable intrusion by the State. Additionally, under Section 7 of the same instrument, privacy can be protected under the liberty and security of the person.

- Moreover, Section 19 of the Access to Information Act the head of government must refuse to disclose any record requested under that Act that contains personal information, unless it is in accordance with Section 8 of the Privacy Act.

Additionally, any information that is obtained in confidence from a treaty partner under an exchange of information article is protected from disclosure under Section 19 of the Privacy Act, and Section 13 of the Access to Information Act. Section 44 of the Mutual Legal Assistance in Criminal Matters Act furthermore prohibits the sharing of records obtained to Canadian mutual legal assistance in criminal matters requests.

- Under the Canadian ITA, the disclosure of taxpayer information must be authorized under Section 241 which strictly controls the use, access and disclosure of said information.

Additionally, the Taxpayer Bill of Rights contains in Art. 3 the right to privacy and confidentiality. It enshrines the CRAs handling of information under the ITA, the Excise Tax Act and the Privacy Act.

8 Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences

- As per the applicable condition in national and international privacy laws (see Q3(c) above), information must be treated secretly and can only be disclosed to persons or authorities who are involved in the assessment or collection, the administration and enforcement in respect of, or the determination of appeals in relation to the taxes to which the treaty applies.
- The Privacy Act, Section 7 limits the use of, or further processing of, personal information collected by a government institution.

9 What is the procedure when the organization wants to ask for follow-up information or receives such a request after a hit?

a. Legal bases

- In relation to tax offences, the same domestic legal provision as for the exchange of spontaneous information constitutes the legal basis to request information. There is no additional law that offers a legal basis for sending a request for mutual legal assistance in criminal matters, since such requests are made through treaties or on the basis of reciprocity.

The competent authority to issue such a request for tax offences is the same as for the exchange of information (cf. q3(b)). Furthermore, the Minister of Justice is the competent authority to send a mutual legal assistance request in criminal matters.

For sending a request on tax information held by foreign tax authorities, the same domestic legal provisions as for the exchange of information apply, which require a basis in international law. This includes the Exchange of Information Article of Canada's tax treaties, Art. 5 of the MAC, Exchange of Information upon Request and Spontaneous Exchange of Information articles of the Tax Information Exchange Agreements. There is no additional national law offering a legal basis for sending a request for mutual legal assistance in criminal matters as such requests are made through treaties or on the basis of reciprocity.

b. Conditions for sending or receiving a request for information

- In accordance with all exchanges of information on request under the treaties, all reasonable efforts to obtain information domestically must have been exhausted before issuing a request for information on criminal matters to a treaty partner. The Canadian government must be satisfied that the information supplied will be safeguarded and that it will only be used in a

humane manner, for the administration of the foreign governments' administration of tax matters.

- Under paragraph 3(1) of the Avoiding Complicity in Mistreatment by Foreign Entities Act the CRA must abide by certain rules of engagement with foreign entities relating to disclosing or requesting information, spontaneous exchange of information included, in the special circumstance, pursuant to the Directions for Avoiding Complicity in Mistreatment by Foreign Entities. These circumstances relate to (1) disclosure of information and (2) request for information. Accordingly, (1) Canadian officials are under an obligation not to disclose information if there is a risk of mistreatment, unless they determine that the risk can be mitigated and appropriate measures taken. Furthermore, (2) if sending a request would result in a substantial risk of mistreatment of an individual, the Commissioner of the CRA must ensure that the CRA officials do not make such a request, unless the risk can be mitigated.
- The legal basis for supplying information is the same as the domestic legal provision for the exchange of spontaneous information. Additionally, the Mutual Legal Assistance in Criminal Matters Act (MLACMA) provides a basis to comply with qualifying requests made by foreign countries in criminal matters. The Canada Evidence Act allows for Canadian court orders for letters rogatory. Moreover, requests for tax information in criminal investigation or prosecution can be made either through a treaty or an administrative arrangement entered into under the MLACMA, or a bilateral agreement for mutual legal assistance in criminal matters to which Canada is party. The disclosure of taxpayer information is authorized under subparagraph 241(4)(e)(xiii) of the ITA.
- The sending of a request or receiving a request for further information in tax and/or administrative matters are governed by the same laws and rules as the exchange of spontaneous information above.

Denmark

Member Organization: The Danish Tax Agency (DTA)

In which domain falls the information the organization wants to share spontaneously?
The DTA wants to share information in one domain: TAX

Domain TAX
1. What kind of information is to be shared?
- Information which is foreseeably relevant to secure the correct assessment or collection concerning taxes of every kind and is exchanged according to an exchange agreement, bilateral or multilateral.

2. Is there a legal basis to share this information spontaneously?
a. In national law?
- The domestic legal basis for exchange of information in tax/administrative matters is contained in the Danish Tax Control Act §66. Consequently, the Customs and Tax Administration provides information to and receives information from the competent authorities in the Faroe Islands, Greenland and in a foreign jurisdiction in accordance with the provisions of relevant EU legislation (see next question), double taxation agreements and administratively concluded agreements on administrative assistance in tax matters between Denmark and the Faroe Islands, Greenland or the foreign jurisdiction in question (§66(1)-(3)). Moreover, any additional agreement or convention dealing with administrative assistance in tax matters which Denmark has acceded to are applicable to the Customs and Tax Administration (§66(4)).
- Furthermore, there is a general requirement for a legal basis for the transmission of personal data under the General Data Protection Regulation (GDPR) which is applicable to Denmark in its entirety. This includes that the processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, cf. Art. 6(1)(e) GDPR or a necessity for compliance with a legal obligation to which the controller is subject, cf. Art. 6(1)(c) GDPR.
Additionally, the basis for transmission of personal data may appear in sector-oriented national law in accordance with Art. 6(2) and 6(3) GDPR.

b. In international law?
- Yes. § 66 implements the EU Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC. Additionally, the EU Council Regulation No. 389/2012 of 2 May 2012 on administrative cooperation in the field of exercise duties and repealing Regulation (EC) No. 2073/2004 and the EU Council Regulation No. 904/2010 of 7 October 2012 on administrative cooperation and combating fraud in the field of value added tax are applicable.

3. Under what conditions can the information be shared spontaneously?
a. Conditions in national law regarding international cooperation?
- The competent authority (the Danish Tax authorities) shall exchange such information as is foreseeably relevant to secure the correct assessment or collection concerning taxes of every kind. Additionally, it may exchange information related to tax administration and compliance improvement, including risk analysis techniques, tax avoidance or evasion schemes. Regarding offences, the receipt of personal data is allowed only for offences concerning the assessment or collection of taxes by the exchange agreement.
- The Danish Tax authorities may receive and supply personal data from and to other countries' competent Tax authorities.

b. Conditions in international law regarding cooperation?

- The competent authorities (here the DTA) shall exchange such information as is foreseeably relevant to secure the correct assessment or collection concerning taxes of every kind. Moreover, the competent authority may exchange information related to tax administration and compliance improvement, including risk analysis techniques or tax avoidance evasion schemes.
- The information exchanged according to the international legal framework listed above may be disclosed to persons and authorities involved in the assessment or collection of taxes. Information may also be communicated to the taxpayer, his proxy or to the witnesses. This also means that information can be disclosed to governmental or judicial authorities tasked with deciding whether such information should be released to the taxpayer, his proxy or to the witnesses.
- The information received by a contracting State may be used by such persons or authorities only for the purposes mentioned. Furthermore, information whether taxpayer- specific or not, should not be disclosed to persons or authorities not mentioned, regardless of domestic disclosure laws such as freedom of information or other legislation that allows greater access to governmental documents.
- Information can furthermore be disclosed to oversight bodies. Such oversight bodies include authorities that supervise tax administration and the enforcement authorities as part of the general administration of the government of the contracting State. In their bilateral negotiations, however, contracting States may depart from this principle and agree to exclude the disclosure of information to such supervisory bodies.

c. Conditions in national privacy laws/ Conditions in international privacy laws?

- The DTA applies all provisions of the GDPR.

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, given an indication of relevant differences

- The DTA wants to share information about all kinds of taxes, as long as they fulfil the conditions listed in Q1., this question is not relevant.

5. What is the procedure when the receiving organisation wants to ask for follow-up information after a hit?

- The GDPR- team of the Danish Tax Agency's legal department is not aware of special legal bases in Danish or international law for this type of exchange of information apart from the above mentioned §66 of the Danish Tax Control Act and the general rules under the GDPR. Article 6 of the GDPR is important in this regard.

6. What is the procedure when the sending organization/ country receives a request for follow- up information after a hit?

a. Procedure under national law
b. Procedure under international law

Domain CRIMINAL – Not applicable to Denmark, as they do not wish to share information in this domain.

Finland

Member organization: The Finnish Tax Administration (FTA)

In which domain falls the information the organization wants to share spontaneously?

- The FTA wants to share information in one domain: TAX

Domain TAX

1. What kind of information is to be shared?

   The FTA wants to share information about all kinds of taxes. The FTA does not have criminal investigative rights, however, it gathers data related to criminal matters, such as criminal reports made by the FTA or business bans. This data is considered as tax data.

   The FTA may receive any information for tax purposes from any organization but does not conduct criminal investigations. Any suspected tax crimes will be reported to the police. Likewise, any information received on criminal matters will be supplied to the national criminal investigative authorities based on national legislation, unless it is supplied for taxation purposes.

2. Is there a legal basis to share this information spontaneously?
   a. In national law?

      The FTA may only disclose secret tax information (all information related to an identifiable taxpayer) when there is an explicit legal provision or international agreement, as enshrined in the Act on the Openness of Government Activities, Chapter 7, Section 30 'Granting access to secret information to the authority of foreign state or to an international institution'. Additionally, an authority may grant access to a secret official document to an authority of a foreign state or to an international institution, if an international agreement binding on Finland contains a provision on such co-operation between Finnish and foreign authorities, or there is a provision to this effect in an Act binding Finland and the Finnish authority in charge of the co-operation could under this Act have access to the document.

   b. In international law?

      Finland is signatory to the Convention on Mutual Assistance in Tax Matters (MAC), the EU Council Regulation on Cooperation in Matters of Value Added Tax (904/2010) and the EU Council Directive on Administrative Cooperation in Tax Matters (2011/16). Moreover, Finland is Party to several bilateral tax treaties (EIO). All these agreements have been implemented by national legislation.

3. Under what conditions can the information be shared spontaneously?
   a. Conditions in national law regarding international cooperation

      The FTA is only allowed to supply personal data to other foreign competent tax authorities under international agreements that allow EIO for tax purposes. Similarly, the FTA is allowed to receive personal data pursuant to international agreements only. The goal of the exchange must be for taxation purposes. Each agreement stipulates how received information may be used, and contains different conditions in the terms of each agreement.

   b. Conditions in international law regarding international cooperation

      The FTA is the competent authority to spontaneously share information with other (foreign) competent authorities on tax matters.

c. Conditions in national privacy laws/ Conditions in international privacy laws

The FTA applies all provisions of the General Data Protection Regulation (GDPR) without any reservations.

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences

The FTA wants to share information on all kinds of taxes.

As mentioned above, each agreement stipulates how received information may be used. Typically, received information may be additionally used for criminal taxation investigation. Moreover, with the permission of the competent authority who provided the information, it can be used for wider purposes.

5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?

For official requests to foreign authorities there needs to be an intentional legal basis (international agreement). Generally, there are no limitations on asking information from any organization in tax matters but if there is no legal basis, the FTA has no means to compel the production of information.

6. What is the procedure when the sending organization/ country receives a request for follow- up information after a hit?
   a. Procedure in national law

      Same as sending (see above).

   b. Procedure in international law

      Same as sending (see above).

Iceland

Member organization: The Directorate of Tax Investigations (DTI)

In which domain falls the information the organization wants to share spontaneously?
The DTI wants to share in both domains: TAX and CRIMINAL

Domain TAX

1. What kind of information is to be shared?
   - The DTI wants to share information gathered for the purpose of investigating violations of tax, such as tax evasion and fraud.
2. Is there a legal basis to share this information spontaneously?
   a. In national law?
      - The Icelandic Tax Administration may only exchange tax information spontaneously when there are explicit legal provisions or international agreements permitting such exchange. The national legal provision forming the legal basis for this type of information exchange is Art. 119 of the Income Tax Act No. 90/2003. It stipulates that the Icelandic government is permitted to enter into agreements with foreign governments of other countries on mutual tax concessions of foreign and Icelandic taxable entities that according to the current tax legislation of the countries are supposed to pay tax on the same tax base in both Iceland and abroad. Moreover, the government is allowed to negotiate with other countries on the mutual exchange of information concerning the collection of public dues.
   b. In international law?
      - Iceland is signatory to the Convention on Mutual Administrative Assistance in Tax Matters (MAC), as well as party to bilateral double taxation treaties and bilateral treaties for the exchange of information. The Icelandic Revenue and Customs (IRC) and the DTI are the competent authorities under this international framework.
3. Under what conditions can the information be shared spontaneously?
   a. Conditions in national law regarding international cooperation
      - The Icelandic authorities are only allowed to spontaneously supply or receive personal data if based on an international agreement that allows for such an exchange of information for tax purposes, and only to or from other (foreign) competent authorities. Furthermore, the supply of the data is only allowed for the purposes of the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to the taxes under investigation.
   b. Conditions in international law regarding international cooperation
      - The information which can be exchanged must be foreseeably relevant for the administration or enforcement of domestic law concerning covered taxes. Furthermore, the exchange of information must be stipulated by the conditions of the relevant international instrument and its use and disclosure must be governed by its terms.
   c. Conditions in national privacy laws/ Conditions in international privacy laws
      - The DTI applies all provisions of the General Data Protection Regulation (GDPR). Iceland has not made any reservations to the GDPR.
4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences
      - As stated above in q3(a), the supply of personal data is allowed for the purposes of the assessment or collection of, the enforcement or

prosecution in respect of, or the determination of appeals in relation to the taxes under investigation. The information may additionally be used for other purposes only with the express written consent of the competent authority of the jurisdiction providing the information.

5. What is the procedure when the receiving organisation wants to ask for follow-up information after a hit?
   - Under Art. 119 of the Income Tax Act No. 90/2003, the DTI, constituting the competent authority, is allowed to send and receive requests for the exchange of information in taxation cases under investigation based on international legal instruments in place. The conditions for issuing those requests are stipulated in the terms of each legal instrument.
6. What is the procedure when the sending organization/ country receives a request for follow- up information after a hit?
   a. Procedure under national law
      - The procedure is the same as for requesting information (see q5).
   b. Procedure under international law
      - The procedure is the same as for requesting information (see q5).

Domain CRIMINAL

1. What kind of information is to be shared?
   - The DTI wants to share information gathered for the purpose of investigating violations of tax law, such as tax evasion and tax fraud.
2. Is there a legal basis to share this information spontaneously?
   a. In national law?
      - Article 119 of the income Tax Act No. 90/2003 serves as a legal basis for the spontaneous exchange of information for tax purposes as stipulated above (*Domain TAX)*. Additionally, the DTI can send and receive requests for the exchange of information in cases under investigation, based on international legal instruments.
   b. In international law?
      - All of the international treaties that Iceland is signatory to where the DTI is a competent authority allow for spontaneous exchange of information for tax purposes and use of the exchanged information for criminal tax purposes. Notably, this includes the MAC.
3. Under what conditions can the information be shared spontaneously?
   a. Conditions in national law regarding international cooperation
      - The DTI gathers personal data in criminal matters (cf. q1). The information is subsequently disclosed to competent authorities involved in the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to the taxes under investigation. The supply of personal data is only allowed for the purpose of assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to the taxes under investigation. Additionally, the DTI can spontaneously receive information for the purpose of criminal investigations of suspicion of tax fraud and other violations of tax legislations for example from the police and the FIU.
   b. Conditions in international law regarding international cooperation
      -
   c. Conditions in national and international privacy laws
      - The DTI applies all provisions of the General Data Protection Regulation (GDPR). Iceland has not made any reservation to the latter.
4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences

- As stated above in q3(a), the supply of personal data is allowed for the purposes of the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to the taxes under investigation. The information may additionally be used for other purposes only with the express written consent of the competent authority of the jurisdiction providing the information.

5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?
   a. Procedure under national law
      - The DTI is the competent authority for sending a request, under Art. 119 of the Income Tax Act No. 90/2003. As stated above, domestic Icelandic legislation requires a basis in international instruments for sending such a request. Moreover, the terms of each of these legal (international) instruments set out the conditions for sending a request.
   b. Procedure under international law
6. What is the procedure when the sending organization/ country receives a request for follow- up information after a hit?
   a. Procedure under national law
      - The procedure for sending a request is the same as for receiving a request. (Cf. q5).
   b. Procedure under international law

The Netherlands

Member organization: FIOD

In which domain falls the information the organization wants to share spontaneously?

The FIOD wants to share information in both domains: TAX and CRIMINAL

Domain TAX

1. What kind of information is to be shared?

The FIOD wants to share information about all kinds of taxes.

2. Is there a legal basis to share this information spontaneously?

a. In national law?

Yes. Article 7 of the Wet op de internationale bijstandverlening bij de heffing van belastingen / International assistance with levying taxes code (WIB) contains a provision about the compulsory spontaneous supply of information (Article 7(1) WIB) and a provision about the voluntary spontaneous supply of information (Article 7(2) WIB). The difference between the compulsory and voluntary spontaneous supply of information is the receiving authority. If this authority is in an EU Member State, the spontaneous supply of information is compulsory. If the authority is in a non-EU Member State the spontaneous supply of information is voluntary.

b. In international law?

Yes. Article 7 WIB is an implementation of the EU Directive 2011/16/EU on administrative cooperation in the field of taxation and its predecessor Directive 77/799/EEC. In addition there are some EU Regulations about the compulsory automatic and spontaneous supply of personal data with regard to certain tax categories, such as value added tax (Council Regulation (EU) 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax) and excise duties (Council Regulation (EU) 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) 2073/2004). This includes the compulsory supply of information where an EU Member State has grounds to believe that a breach of value added taxes legislation has been committed or is likely to have been committed in the other EU Member State (Article 13(1)(b) Regulation (EU) 904/2010) and where there is a risk of fraud or a loss of excise duty in another EU Member State (Article 15(1)(c) Regulation (EU) 389/2012). Furthermore, the Netherlands are signatory to the Convention on Mutual Administrative Assistance in Tax Matters which provides in article 7 a basis for the spontaneous supply of information worldwide.

3. Under what conditions can the information be shared spontaneously?
a. Conditions in national law regarding international cooperation

- The FIOD/Belastingdienst should/can spontaneously supply information: a) when there is a suspicion that it is unjustified that a foreign authority grants a tax reduction, discharge, restitution or exemption or that it is unjustified that the foreign authority does not levy any tax, b) when in the Netherlands a tax reduction, discharge, restitution or exemption is given which can influence the levying of taxes by a foreign authority, c) when in the Netherlands acts are performed with the purpose to wholly or

partly prevent the levying of taxes by a foreign authority and d) when the supply of information is necessary according to the Minister of Finance (Article 7(1)(2) WIB).

- Spontaneous information supply should take place as soon as possible and at the latest within one month after the relevant information was received by the FIOD/Belastingdienst (Article 7a WIB).
- Information is supplied by the FIOD/Belastingdienst for the purpose of assisting foreign authorities with the levying of taxes (Article 1 WIB). The information can also be used by the foreign authority in judicial or administrative procedures which could lead to punishment because of the infringement of tax regulations (Article 17(1)(c) WIB). Furthermore the Minister of Finance can give permission to use the information for other purposes (Article 17(2) and 17(5) WIB). Among others, this seems to include criminal investigations. This permission will at the least be given when the information is used in the Netherlands for the same goals (Article 17(2) WIB).

b. Conditions in international law regarding international cooperation

- The FIOD/Belastingdienst is on behalf of the Dutch Minister of Finance the competent authority (Mandaatverlening internationale inlichtingenuitwisseling) to spontaneously share information with states and competent authorities worldwide.
- Within the European Union the most relevant provision is that the Dutch Minister of Finance may communicate, by spontaneous exchange, to the competent authorities of the other Member States any information of which they are aware and which may be useful to the competent authorities of the other Member States (Article 9(2) EU Directive 2011/16/EU).
- Within the European Union regarding value added tax and excise duties it is provided that the Dutch Minister of Finance may (or regarding VAT shall), by spontaneous exchange, forward to the competent authorities of the other Member States any relevant information that they are aware of and which they consider may be useful to those competent authorities (Article 15 Council Regulation (EU) 904/2010 and Article 16 Council Regulation (EU) 389/2012).
- The Netherlands are signatory to the Convention on Mutual Administrative Assistance in Tax Matters the following. The Dutch Minister of Finance may spontaneously supply information to other party's under the following conditions. A Party shall, without prior request, forward to another Party information of which it has knowledge in the following circumstances: a) the first-mentioned Party has grounds for supposing that there may be a loss of tax in the other Party; b) a person liable to tax obtains a reduction in or an exemption from tax in the first-mentioned Party which would give rise to an increase in tax or to liability to tax in the other Party; c) business dealings between a person liable to tax in a Party and a person liable to tax in another Party are conducted through one or more countries in such a way that a saving in tax may result in one or the other Party or in both; d) a Party has grounds for supposing that a saving of tax may result from artificial transfers of profits within groups of enterprises; e) information forwarded to the first-mentioned Party by the other Party has enabled information to be obtained which may be relevant in assessing liability to tax in the latter Party.

c. Conditions in national privacy laws / Conditions in international privacy laws

- The FIOD applies all provisions of the General Data Protection Regulation.

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences

The FIOD wants to share information about all kinds of taxes. Therefore this question is not relevant.

5. What is the procedure when the receiving organisation wants to ask for follow-up information after a hit?

- A request for information can be sent to the FIOD and Belastingdienst (Article 5 WIB / Mandaatverlening internationale inlichtingenuitwisseling).
- The request can only be done by a state with which the Netherlands has made arrangements regarding the mutual assistance in tax matters (Article 2(1)(d) WIB).

6. What is the procedure when the sending organisation/country receives a request for follow-up information after a hit?

a. Procedure under national law

- The FIOD/Belastingdienst will give the requested information if it is expected that the information is of interest to the administration and enforcement of national legislation regarding taxes in the requesting state.
- The FIOD/Belastingdienst will provide the information as soon as possible (Article 5a WIB). At the very latest the information will be provided six months after the request, or - if the FIOD/Belastingdienst already possesses the information - two months after the request. Within a week a confirmation of the received request will be sent to the requesting party.

b. Procedure under international law

- Within the European Union, at the request of the requesting authority, the FIOD/Belastingdienst (on behalf of the Dutch Minister of Finance) shall communicate to the requesting authority any information that it has in its possession or that it obtains as a result of administrative enquiries is foreseeably relevant to the administration and enforcement of the domestic laws of the Member States concerning the taxes (except for VAT and excise duties) (Article 1(1) and 5 EU Directive 2011/16/EU).
- This information will be provided as soon as possible (Article 7 EU Directive 2011/16/EU). At the very latest the information will be provided six months after the request, or - if the FIOD/Belastingdienst already possesses the information - two months after the request.
- Within the European Union, at the request of the requesting authority, the the FIOD/Belastingdienst (on behalf of the Dutch Minister of Finance) shall in principle communicate the information that may help to effect a correct assessment of VAT, monitor the correct application of VAT, particularly on intra-Community transactions, and combat VAT fraud, including any information relating to a specific case or cases (Article 1(1) and 7 Council Regulation (EU) 904/2010).
- Within the European Union, At the request of the requesting authority, the FIOD/Belastingdienst (on behalf of the Dutch Minister of Finance) shall communicate the information necessary to ensure the correct application of legislation on excise duties, including any information relating to a specific case or specific cases, in particular concerning movements of excise goods within the Union (Article 8(1) Council Regulation (EU) 389/2012).
- At the request of a Party to the Convention on Mutual Administrative Assistance in Tax Matters the FIOD/Belastingdienst (on behalf of the Dutch Minister of Finance) shall provide the applicant State with any information which concerns particular persons or transactions that is foreseeably relevant for the administration or enforcement of their domestic laws concerning the taxes covered by the Convention.

Domain CRIMINAL

1. What kind of information is to be shared?

The FIOD wants to share information with regard to the criminal facts they investigate. The FIOD has a broad array of duties relating to the criminal enforcement of the fiscal, financial and economic legal order. The FIOD is responsible for the criminal investigation of fraud with regard to the three main tasks of the Belastingdienst: all sorts of tax fraud (e.g. carousel fraud and concealed assets), subsidy fraud and custom fraud (duty fraud). The FIOD is also responsible for the criminal investigation of certain economic and financial offences on other policy areas, like insider trading, bankruptcy fraud and money laundering. And the FIOD plays a role in confiscating illegally obtained assets.

2. Is there a legal basis to share this information spontaneously?
a. In national law?

- Within the European Union: to persons or organisations in other EU Member States that are responsible for preventing and investigating criminal offences police data can be supplied under the same conditions as to police officers in the Netherlands as long as the supply of the police data is in the interest of the right functioning of the prevention or investigation of criminal offences (Article 15a Wet politiegegevens / Police data code (Wpg) and Article 5:3 Besluit politiegegevens / Police data regulation (Bpg)). This includes the spontaneous supply of information.
- Outside the European Union: to competent authorities outside the EU, it is possible to supply police data for the purpose of criminal enforcement of the legal order (Article 1(1) and 17a(1) Wpg and Article 5:1(1) Bpg). This includes the spontaneous supply of information.

b. In international law?

- Within the European Union: Competent law enforcement authorities shall, without any prior request being necessary, provide to the competent law enforcement authorities of other Member States concerned information and intelligence in cases where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of offences referred to in Article 2(2) of Framework Decision 2002/584/JHA (Article 7 Council Framework Decision 2006/9600/JHA). These offences include fraud and the laundering of the proceeds of crime.
- Outside the European Union: There are no relevant international or bilateral treaties that regulate the spontaneous exchange of information in criminal matters to which the Netherlands is signatory.

3. Under what conditions can the information be shared spontaneously?
a. Conditions in national law regarding international cooperation

- The Wpg en Bpg should be regarded as privacy laws. Strictly speaking, there is no national law regarding international cooperation in criminal matters that governs the spontaneous supply of information.
- Within the European Union: It is not totally clear whether the FIOD is by itself competent to spontaneously supply information to (competent) law enforcement authorities within the European Union. The formal regulations do not mention the obligation that information can only be supplied to EU authorities by a competent authority. Nevertheless, the (outdated) guidelines of the public prosecutor stipulate that all outgoing information should be done via mediation of a national coordinator.
- Outside the European Union: The supply of police data to non-EU countries must be done through mediation of a central authority (Article 5:1(2) Bpg). This is a national police unit: the LIRC (Landelijk Internationaal Rechtshulpcentrum / National International Centre for Mutual Legal Assistance). Mediation of the LIRC is not necessary when the supply of police data is in accordance with an agreement made with

foreign police authorities and this agreement is approved by the Minister of Justice (Article 5:1(2) Bpg).

b. Conditions in international law regarding international cooperation

- Within the European Union: according to Article 7(2) of the Council Framework Decision 2006/9600/JHA the provision of information and intelligence shall be limited to what is deemed relevant and necessary for the successful detection, prevention or investigation of the crime or criminal activity in question.
- Within the European Union: based on Article 7(2) of the Council Framework Decision 2006/9600/JHA information can only be shared regarding offences referred to in Article 2(2) of Framework Decision 2002/584/JHA.

c. Conditions in national and international privacy laws

- Police data may be supplied if this is necessary for the enforcement of the Dutch legal order (Article 17a(1) and 1(a) Wpg, and art. 3 and 4 Politiewet / Police act). According to Article 35(1)(a) and 1(1) Law Enforcement Directive 2016/680/EU (hereafter Directive) police data may be supplied if this is necessary for the investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
- Within the European Union: The supplier of information is allowed to set limiting conditions to the spontaneous supply of information to investigative authorities in EU Member States (Article 5:3(2) Bpg). This can be done if the supply of police data: harms essential national security interests, endangers the success of an ongoing investigation, is clearly disproportional or irrelevant, regards data about a criminal offence with a maximum prison sentence of one year or less, regards the publication of data for which the approval of a prosecutor is necessary and this approval is missing or regards data received from another nation which cannot passed over.
- Within the European Union: Information is supplied under the condition that it can only be processed for the purposes the information is supplied for (Article 5:3(4) Bpg)/Article 50 Directive). The information should be destroyed when this purpose is achieved (Article 5:3(5) Bpg).
- Outside the European Union: Police data can be supplied to a controller in a non-EU third country (art. 17a Wpg). The controller should be a competent authority (art. 3(8) Directive). According to the Directive the competent authority in non-EU third countries is any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (Article 3(7)(a) Directive). The Wpg has a slightly broader definition of competent authorities which also includes other public body's or entities entrusted with police tasks (art. 1(l) Wpg).
- Whether police data can be supplied to a controller in a non-EU third country depends on whether this foreign controller provides an adequate level of data protection. There is a multi-stage procedure to determine if a controller is eligible.
- The first stage is to determine whether the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation ensures an adequate level of protection (Article 36(1) Directive, art. 17a(1) Wpg). As of March 2021 the Commission has not made any adequacy decision based on article 36 of the Directive, although the United Kingdom has requested such a decision.
- The second stage is divided into two. Police data may be exchanged if either a) there is a legally binding instrument that provides appropriate safeguards with regard to the protection of personal data or b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards

exist with regard to the protection of personal data (Article 37(1)(a)&(b) Directive, Article 17a(2) Wpg). Legally binding instruments should contain provisions about the protection of personal data. There are no general data protection treaties regarding the exchange of police data between the Netherlands or the European Union and Australia, Canada or the United States. Police data may also be exchanged if the national controller comes to the conclusion that the foreign controller in a third country offers appropriate safeguards with regard to the protection of personal data. With regard to the exchange of filters within FCInet a finding of appropriate safeguards by the sending organisation (in an EU member state) could possibly be made if the receiving organisation (in a non-EU third country) has put in place enough safeguards. This could be the case if FCInet is designed and implemented in a way that provides the appropriate safeguards by design.

- The third stage of the procedure to decide whether the foreign controller provides an adequate level of data protection (art. 38(1) Directive, Article 17a(3) Wpg). Then in individual cases the exchange of information is possible. Because within FCInet the exchange of information is structural, this provision is not relevant.

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences

The FIOD has no duties with regard to the investigation of criminal offences in general. Whether information regarding these general criminal offences can be shared by the FIOD is questionable, especially in light of purpose limitation provisions.

5. What is the procedure when the receiving organisation wants to ask for follow-up information after a hit?
   a. Procedure under national law
   b. Procedure under international law

- The Dutch code of criminal procedure offers in Article 5.1.4 a legal basis for the supply of information to foreign countries after a request. A request for mutual legal assistance will in principle be granted, unless this will be contrary to a national legal provision or contrary to the public interest. No difference is made between requests for information from EU member states or non-EU third countries.
- The FIOD is a competent authority to supply information to other foreign organisations. In general, requests for mutual legal assistance will be decided upon by the prosecutor (Article 5.1.4(1) and 5.1.6 CCP). However, if a request is solely about information and no additional, special coercive investigation matters need to be applied, the request may be granted and executed by a criminal investigator (art. 5.1.7(1) CCP). The criminal investigator acts under supervision of the prosecutor. The prosecutor's office (Openbaar Ministerie) can govern the supply of information to foreign countries through general and specific instructions. At the moment there are no instructions about the request for information.
- Up to March 2021 there is a (out-of-date) general Instruction from the prosecutor's office about the assessment of incoming requests for information by criminal investigators. Information can only be sent through mediation of the LIRC. Only when the minister of Justice approves an agreement about the direct and unmediated exchange of information between the national and foreign authority, the involvement of the LIRC is not necessary.

6. What is the procedure when the sending organisation/country receives a request for follow-up information after a hit?
   a. Procedure under national law
   b. Procedure under international law

- The Dutch Code of criminal procedure offers in Article 5.1.2 a legal basis for sending requests for mutual legal assistance in general and requests for information in particular. The request must be done for the purpose of the investigation, prosecution or adjudication of criminal offences or the execution of criminal sentences (Article. 5.1.1(1) CCP). No difference is made between requests for information to EU member states or non-EU third countries.
- As a rule only prosecutors or judges are competent to send out a request for mutual legal assistance. However, requests for information are excluded from this rule. If a request is solely about getting information from foreign police authorities, the request may be done by a criminal investigator (Article 5.1.2(2) CCP). The criminal investigator may also send the request (Article 5.1.2(3) CCP). The actions of the police are supervised by the prosecutor. The prosecutor's office (Openbaar Ministerie) can govern the request for information by criminal investigators through general and specific instructions. At the moment there are no instructions about the request for information.
- Up to May 2021 there is an out-of-date general Instruction from the prosecutor's office about requests for information by criminal investigators based on the now obsolete provisions in the Dutch criminal procedure code about international cooperation (art. 552h CCP etc.). Under reference to art. 5:1(3) Besluit politiegegevens (old) the Instruction stated that all requests for information to foreign police authorities must be done through mediation of the LIRC (Landelijk Internationaal Rechtshulpcentrum / National International Centre for Mutal Legal Assistence). Only when the minister of Justice approves an agreement about the direct and unmediated exchange of information between the national and foreign authority, the involvement of the LIRC is not necessary.
- The two-tier FCInet information exchange – first a filter and when there is a hit, possibly a request for additional information – is similar to other forms of mutual legal assistance, like the comparison of DNA-profiles or fingerprint profiles. With the Prüm Treaty EU-member states agreed to give access to national databases with DNA- or fingerprint profiles to the national contact points of other member states. After a hit the supply of further available data and other information is governed by the national law about mutual legal assistance (art. 5 Prüm Treaty). The exchange of additional information about DNA or fingerprints should according to the aforementioned (obsolete) Instruction also be mediated by the LIRC.

Norway

Member organization: The Tax Administration

In which domain falls the information the organization wants to share spontaneously?

- The Tax Administration wants to share information in one domain: TAX

Domain TAX

1. What kind of information is to be shared?

The Norwegian Tax Administration wants to share information about all kinds of tax, as permissible under the international legal instruments.

2. Is there a legal basis to share this information spontaneously?

a. In national law?

The Tax Administration Act section §3-3-1 second ident states that information can be shared with other public authorities that may need it in their taxation or customs work and is complemented by the Double Taxation Act. This provision also comprises foreign taxation and custom authorities. There is however, no positive tax law provision specifically mentioning foreign organizations, i.e., international organizations, as far as the Tax Administration is aware. But the national legal provisions cover foreign authorities of public law. Additionally, there are different sector rules, such as the EEA Act which provide for cooperation with other bodies, i.e., the EFTA Surveillance Authority (ESA) and the EFTA Court providing a legal basis for exchanging tax information with these organizations or bodies of public international law.

b. In international law?

The legal basis must follow directly from national law as supranational treaties do not have direct effect usually before they have been incorporated into national law due to the duality principle of international law in Norwegian legal tradition. National law will in many instances contain explicit references to international treaties and rules which provide for the legal basis for spontaneous supply or exchange of information. In the absence of an international treaty or of specific provisions allowing the transfer of data to other countries, organizations and authorities, the exchange would not be permissible.

Norway is signatory to the Convention on Mutual Administrative Assistance in Tax Matters (MAC). The Convention obliges Parties to spontaneously exchange information in tax matters in addition to automatic exchanges and exchange on request. The first article of the Convention states that the assistance comprises all mutual assistance activities in tax matters that can be carried out by the public authorities, including the judicial authorities. Moreover, Art. 4 embodies the general obligation to exchange any information that is foreseeably relevant for the administration or enforcement of domestic laws concerning the taxes covered by the Convention.

Furthermore, Norway has entered into several agreements on the exchange of information in tax matters. The Nordic Convention on Administrative Assistance is the only agreement of a multilateral nature. Under Art. 11(2) of the Nordic Convention a Party should exchange information to another Party without notice, such as interests, dividends, salary, but also information gathered during the course of an investigation and that might be of interest to the other Party.

Additionally, all of the Double Taxation Treaties into which Norway has entered with other countries contain special provisions relating to the exchange of information.

Moreover, there is an agreement between the EU and Norway on administrative cooperation in the field of VAT. Since the exchange of information based on this agreement takes place in a communication network hosted by the EU, FCInet will not be relevant for this agreement.

3. Under what conditions can the information be shared spontaneously?

a. Conditions in national law regarding international cooperation

Only designated persons in the Ministry of Finance, the Directorate of taxes and a separate unit in the Tax Administration constitute a competent authority to exchange the personal data (both supply and receive). Additionally, there are designated persons who are competent authorities to exchange information within special areas of cooperation. Any other conditions that are found in international law are applicable in the national law of Norway as well.

b. Conditions in international law regarding international cooperation

As mentioned above, Art. 4 of the MAC contains the general obligation to exchange information. Notably, the scope of this article is wide and should assist the State Parties in combating international tax avoidance and evasion to the largest extent possible. However, Parties are not at liberty to engage in 'fishing expeditions or request information that is unlikely to be relevant to the tax affairs of a given person.

Furthermore, the Convention enshrines in Art. 22 strict rules on confidentiality. Under Art. 22(2) information that is obtained shall in any case be disclosed only to the competent authorities tasked with the assessment, collection or recovery of, the enforcement or criminal proceedings in respect of taxes or the oversight thereof.

Within the Nordic Convention, Art. 21 stipulates that information received through the Convention is governed by the receiving State's national legislation. Thus, the Nordic countries do not have a uniform regulation on confidentiality.

c. Conditions in national privacy laws/ Conditions in international privacy laws

All provisions of the General Data Protection Regulation are applicable to Norway and the competent Norwegian authorities. Additionally, special provisions in taxation law can provide for more detailed rules relating to access to documents and administrative information. Rights to file complaints on decisions and administrative acts performed by the tax administration also involve data subject rights.

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences.

The Norwegian Tax Administration wants to share information about all kinds of tax, as permissible under the international legal instruments. Therefore, this question is not relevant.

5. What is the procedure when the receiving organisation wants to ask for follow-up information after a hit?

A request for information will relate to a particular case and should include (not exhaustive list): the name of the tax payer, control period and the period of time the information is requested, taxes concerned, in comprehensive cases a summary and the main question of the case are required and a description of the case, including why there is a control of the taxpayer, facts, and why there is a need for the requested information. Moreover, there is a condition for all available resources to have been consulted before sending a request for information, which includes contacting the taxpayer (except in cases where it is necessary that the taxpayer does not know of the control).

The competent authorities under domestic law to send such a request are designated persons in the Ministry of Finance, the Directorate of taxes and a separate unit in the Tax Administration. Furthermore, there are designated persons who constitute competent authorities to exchange information within special areas of cooperation.

All requests send by the Norwegian authorities must have a legal basis either in Norwegian national law or in an international agreement with the receiving jurisdiction.

6. What is the procedure when the sending organization/ country receives a request for follow-up information after a hit?

a. Procedure under national law

The competent authorities for receiving a request are the same as for sending such a request (see above). Norwegian national law provides for a legal basis for supplying information on the basis of a request by another competent authority, pursuant to an international agreement with the sending jurisdiction.

b. Procedure under international law

The same as to national law.

Sweden

Member organization: The Swedish Tax Agency

In which domain falls the information the organization wants to share spontaneously?

- The Swedish Tax Agency wants to share information in both domains: TAX and CRIMINAL.

Domain TAX

1. What kind of information is to be shared?
   - Information for tax purposes.

2. Is there a legal basis to share this information spontaneously?
   a. In national law?
      - Sweden has a dualist system. Thus, all international treaties must be incorporated into domestic law in order to take effect. Commonly an international agreement is implemented into national law.

      The most relevant provision in Swedish national law stipulates that there is an obligation to exchange data, the purpose for what it should be exchanged and confidentiality together with provisions about what kind of information should be exchanged.

   b. In international law?
      – Theoretically, there is no need for an international legal basis if one exists in national law. However, this is uncommon and an international agreement will usually be incorporated into national law.

      Sweden is signatory to the Convention on Mutual Administrative Assistance in Tax Matter (MAC) and the Nordic Convention on Mutual Administrative Assistance in Tax Matters. Furthermore, the EU Council Regulation No. 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax, as well as the EU Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation are applicable to Sweden. Additionally, Sweden is signatory to bilateral tax treaties. All these international instruments have been implemented into national law or are directly applicable (see EU Regulations).

3. Under what conditions can the information be shared spontaneously?
   a. Conditions in national law regarding international cooperation
      - The Swedish Tax Agency is the designated competent authority to supply and receive information on tax/ administrative matters from other (foreign) competent Tax authorities. In general, the conditions for spontaneous exchange follow from each legal instrument, such as those mentioned in q2(b) above.
   b. Conditions in international law regarding international cooperation
      -

   c. Conditions in national privacy law/ Conditions in international privacy laws
      - The Swedish Tax Agency applies all provisions of the General Data Protection Regulation (GDPR).

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences

- Generally, the exchanged information can be used for tax purposes. If used for other purposes, the main rule is that the sending country must give its permission to use the information for other purposes. Not every agreement covers all taxes, depending on the terms of the agreement.

5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?
   - Under the international legal instruments listed in q2(b), the Swedish Tax Agency is competent to request information from other tax authorities appointed as competent authorities for the purpose of exchange of information on taxes.
6. What is the procedure when the sending organization/ Country receives a request for follow-up information after a hit?
   a. Procedure under national law
   - The procedure and conditions for requesting information are the same as for applying.
   b. Procedure under international law
   -

Domain CRIMINAL

1. What kind of information is to be shared?
- The Swedish Tax Agency wants to share information for the purposes of the prevention, investigation, detection or prosecution of criminal offences related to economic crime and for carrying out intelligence in the field of economic crime. The criminal offences for which the supply of personal data is allowed are related to economic crime such as tax fraud, bookkeeping fraud, money laundering etc.

2. Is there a legal basis to share this information spontaneously?
   a. In national law?
- Within Swedish law, there is a provision according to which there is an obligation to exchange data, an obligation to specify the purpose for the exchange of the data and confidentiality. Additionally, there are other provisions on which specific information should be exchanged.

   b. In international law?
- The Swedish Tax Agency can only exchange with foreign authorities within the framework of regulated EU cooperation, relying on EU Regulation 2016/794 of the European Parliament and the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. The Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union is also applicable to Sweden, however, the Swedish Tax Agency is not the competent authority for criminal matters under it.
- As long as there exists a national legal basis for the exchange, an international one is not necessarily required. However, it is common that an international agreement on the exchange is implemented into national law. Usually. The international agreement will already stipulate the purpose for the exchange of data, as well as the terms for the use of said data.

3. Under what conditions can the information be shared spontaneously?
   a. Conditions in national law regarding internal cooperation

- The Swedish Tax Agency is allowed to supply personal data in criminal matters to other authorities appointed as the competent authorities for the exchange of information in criminal matters, for example in cooperation within Europol. The criminal offences for which the supply of data is allowed must be related to economic crimes such as tax fraud, bookkeeping fraud, money laundering etc.
- Considering the receipt of personal data for criminal investigations, the conditions are the same as mentioned in the previous paragraph on the supply of such data. Additionally, under the principle of free consideration of evidence applicable in Swedish procedural law, the parties to a trial may invoke all evidence that they can obtain (so- called 'free presentation of evidence') and furthermore, the principle stipulates that the value of the evidence is examined freely by the court (free evaluation of evidence).
-

b. Conditions in international law regarding international cooperation

- The Swedish Tax Agency can only exchange with foreign authorities within the framework of regulated EU cooperation.

As mentioned in Q2(b), the Swedish Tax Agency has not been appointed as the competent authority for criminal matters under the Framework Decision 2006/960/JHA. It is however engaged in cooperation through the Police in Europol and Interpol.

c. Conditions in national and international privacy laws

- The General Data Protection Regulation (GDPR) is applicable to Sweden, as well as the EU Directive 2016/680, which has been implemented through the Criminal Data Act (SFS 2018:1177).

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences

5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?
   a. Procedure under national law

- Swedish domestic law offers a legal basis for requesting information from other organizations in criminal law. Since the Swedish Tax Agency has not been appointed as a competent authority for criminal matters yet, requests for information that are send to other organizations concerning criminal law matters are sent by the Police or by the Economic Crime Authority who are appointed as competent authorities in this matter.
- Moreover, the domestic Swedish law requires a basis in international law for sending such a request in criminal matters.
- In order to send such a request, there needs to be suspicion of a serious crime that carries with it a certain degree of sanctioning.

   b. Procedure under international law

-

6. What is the procedure when the sending organization/ country receives a request for follow- up information after a hit?
   a. Procedure under national law

- Swedish national law contains a legal basis for supplying information in criminal matters and it requires a basis in international law for supplying said information. As stated above, the Swedish Tax Agency is not the appointed competent authority for criminal matters, however it is engaged in certain cooperation where the supply of such information is possible.

   b. Procedure under international law

-

United Kingdom

Member organization: Her Majesty's Revenue and Customs (HMRC)

In which domain falls the information the organization wants to share spontaneously?
The HRMC want to share information in both domains: TAX and CRIMINAL

Domain TAX

1. What kind of information is to be shared?
- Various information on taxes, such as income tax and value added tax. However, the HRMC is not responsible for all taxes which consequently are not to be shared, such as council taxes for which local (tax) authorities are responsible. Furthermore, some taxes in Wales and Scotland are under the authority of the Welsh Revenue Authority and Revenue Scotland, and thus not to be shared under FCInet either.

2. Is there a legal basis to share this information spontaneously?
a. In national law?
- See below the national laws implementing international arrangements.
b. In international law?
- The UK is signatory to the Organization for Economic Co-Operation and Development's Convention on Mutual Assistance in Tax Matters and has entered into several tax treaties and arrangements that include the exchange of information.
- In order for the international arrangements to work and fall into co-called disclosure gateways (see Q3(c)), the UK has introduced domestic legislation imposing obligations on the financial sector. Thus, there are four different regimes implemented by national legislation governing automatic exchange of financial account information.
- Firstly, the UK and the US signed an agreement to implement the United States Foreign Account Tax Compliance Act (FATCA) aimed at reducing tax evasion, in the UK; the "The UK-US Agreement to Improve International Tax Compliance and to Implement FATCA" (the US IGA). The US IGA is in force under the Tax Compliance Regulations 2015 (SI 2015/878).
- Secondly, there is the Common Reporting Standard (CRS) developed by the OECD allowing for exchange of information on financial accounts which is implemented by the International Tax Compliance Regulations 2015.
- In order to incorporate the CRS in the EU, the EU Directive on Administrative Cooperation in Tax Matters (DAC) was adopted, making automatic exchange of financial account information among EU Member States mandatory. This is implemented in the UK by the International Tax Compliance Regulations 2015.
- Additionally, the UK has obligations on exchange of information under the Crown Dependencies and Gibraltar Regulations (CDOT).
- The legal basis for sharing UK customs information and its scope depends on several factors, such as the type of information to be shared. Within the EU, disclosure in civil matters is governed by Regulation 515/97. The Customs Information (CIS) Council Decision concerns a database to that end, whose provisions are applicable to the HMRC.
- The scope of exchange of the UK and third countries depends on the EU's exercise of its external competence under Art. 216(1) TFEU. The EU has exercised its full external competence on customs information in the civil sphere and thus us governed by the EU Mutual Assistance Agreements (MAA).
3. Under what conditions can the information be shared spontaneously?
a. Conditions in national law regarding international cooperation

b. Conditions in international law regarding international cooperation

c. Conditions in national privacy law/ Conditions in international privacy laws

- The HMRC is subject to a statutory duty of confidentiality under section 18(1) of the Commissioners for Revenue and Customs Act 2005. Thus, any information obtained within the HMRC's function is confidential and undisclosable unless a statutory exception applies ('disclosure gateway') as listed in section 18(2) of the Act. Additionally, further disclosure gateways can be created by other Acts, as stated in section 18(3) of the Act. The HMRC's approach to disclosures is in accordance with the Information Disclosure Guidance (IDG) by the UK government.
- Section 18(2)(a) of the Commissioners for Revenue and Customs Act 2005 regulates the disclosure to other tax authorities. Accordingly, the HMRC may disclose information to other tax authorities if it is for the purpose of a function of the HMRC, including the management of taxes.
- Where personal data of individuals is involved in the disclosure, the Data Protection Act 1998 (DPA) implementing the 1995 EU Data Protection Directive (Directive 95/46/EC) must additionally be complied with. The DPA includes exceptions which allow data controllers to make derogations from it. For the HMRC's purpose the exemption for personal data processed relating to crime and taxation is among the most relevant, set out in Part 4 and Schedule 7 of the DPA.

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences

5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?

a. Procedure under national law

- English domestic law offers a legal basis for sending such a request for information and the HMRC is the competent authority for it. Furthermore, a basis international law is required for sending a request.
- The concept of reasonable foreseeability constitutes an additional condition for sending a request.

b. Procedure under international law

6. What is the procedure when the sending organization/ Country receives a request for follow-up information after a hit?

a. Procedure under national law

- The national laws offering a legal basis for supplying such information are Council Directive 2011/16/EU on Administrative Cooperation in the Field of Taxation, implemented by the European Administrative Co-operation (Taxation) Regulations 2012 SI 2012/3062 and the Convention on Mutual Administrative Assistance in Tax Matters (Council of Europe and OECD). The national law further requires such a basis in international law for supplying information.
- The HMRC is the competent authority to supply information. Similar to requesting information, the concept of reasonable foreseeability poses an additional condition for sending information.

b. Procedure under international law

Domain CRIMINAL

1. What kind of information is to be shared?

- HMRC officers have a range of criminal powers and may conduct criminal investigations into offences relating to matters in respect of which HMRC has functions. These include statutory offences of fraudulent tax evasion, false accounting, fraud and money laundering. However, the HMRC does not prosecute such offences.

Thus, the information that may be shared, depending on the legal possibility to disclose information in criminal matters must relate to the HMRC's functions.

2. Is there a legal basis to share this information spontaneously?
a. In national law?

- In relation to disclosures to law enforcement agencies and prosecutors, the most significant disclosure gateway (see explanation Domain TAX, Q3(c)) is found in section 19 of the Anti-terrorism, Crime and Security Act 2001, permitting the HMRC to disclose to any person for the purpose of a criminal investigation, criminal prosecution, or for the making of the decision to initiate an investigation or prosecution (s19(2)). This gateway is not limited to disclosure made to law enforcement officials and related to investigations made in the UK or abroad.
- A further statutory gateway allowing the HMRC to disclose information to the National Crime Agency (NCA) is enshrined in section 7 of the Crime and Courts Act 2013, if the disclosure is for the purpose of the exercise of any NCA function. Similarly, section 7 and schedule 7 of the Crime and Courts Act 2013 allow NCA officers to disclose information to others including the HMRC.
- Moreover, under the Crime (International Co-operation) Act 2003 (CICA) section 19 the HMRC must transmit lawfully gathered evidence if so requested by foreign officials under EU Mutual Assistance conventions (see Q2(b)). Thus, if read in conjunction with section 18(3) of the Commissioners for Revenue and Customs Act 2005, it creates another statutory exception to the duty of confidentiality of the HMRC.

b. In international law?

- The EU's Forth Anti-Money Laundering Directive is implemented in the UK by Regulation 52 and 50 of the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017. In combination with section 18(3) of the Commissioner for Revenue and Customs Act 2005 (mentioned above) the HMRC may disclose information relevant to the supervisory functions to other law enforcement agencies of bodies with this task under the EU Directive.
- Furthermore, there are several legal instruments under which the HMRC can share information relating to criminal matters with foreign authorities. These include the 1959 European Convention on Mutual Assistance and its protocols, the EU Convention on Mutual Assistance and its Protocols (the Conventions) or by way of a European Investigation Order (EIO).
- The EU Directive 2014/41/EU was opted into by the UK and implemented into domestic law with the Criminal Justice (European Investigation Order) Regulations 2017.
- Moreover, the UK shares information with other EU Member States under the EU Framework Decision (The Swedish Initiative) and the Convention on mutual assistance and cooperation between customs and administrations. This is possible under section 19 of the Anti-Terrorism, Crime and Security Act 2001.
- The legal basis for sharing UK customs information and its scope depends on several factors, such as the type of information to be shared. Within the EU, customs information is shared under the Naples II Treaty for disclosure in criminal matters. The Customs Information (CIS) Council Decision concerns a database to that end, whose provisions are applicable to the HMRC.
- Contrary to the civil sphere, the UK has retained some competences to act in criminal customs matters (see Domain TAX above, Q2(b)). Where the UK has competence, information sharing is based on various international agreements, such as ones under the UN or the World Customs Organization.

3. Under what conditions can the information be shared spontaneously?
a. Conditions in national law regarding international cooperation

- Under section 19(3) of the Anti-terrorism, Crime and Security Act 2001, the disclosure must be proportionate and comply with the requirements of the Data Protection Act 1998.

b. Conditions in international law regarding international cooperation

c. Conditions in national privacy law/ Conditions in international privacy laws
- Same as in Domain TAX.

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences
- If disclosures are made under section 19 of the Anti-terrorism, Crime and Security Act 2001, the recipient of the disclosure is under a statutory prohibition from further disclosing the information, unless the further disclosure is for a requisite purpose and has been consented by the HMRC (see s19(5)).
- Where a disclosure is made under Regulation 52 and 50 of the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017, regulation 52(2) prohibits the recipient from further disclosing the information, unless certain conditions are fulfilled.

5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?
a. Procedure under national law
- The legal basis for sending a request for information in criminal matters is found in the Crime (International Co-operation) Act 2003 and the European Investigation Order Directive (Consolidating the EU Convention on Mutual Assistance in Criminal Matters 2000). Additionally, the UK Tax Administration can rely on the Tax Treaty Conventions to obtain information in criminal investigations.
- The HMRC is the competent national authority to send a request. Furthermore, a basis in international law is required for sending a request for information.
- Importantly, consent of the defence is crucial for material to constitute evidence within a court. Additionally, the concept of proportionality constitutes another condition under national law relevant to sending such a request.

b. Procedure under international law

6. What is the procedure when the sending organization/ Country receives a request for follow-up information after a hit?
- Same answer as question 5.
- Additionally, if a request is made under the EU's mutual assistance conventions (specified in Q2(b)), the HMRC is obliged under section 19 of the CICA to gather and transmit evidence that has been requested.
- Furthermore, if the request is made under a European Investigation Order (EIO), the HMRC is required to transmit the material to the issuing authority by regulation 31 of the Criminal Justice Regulations 2017.

United States of America

Member organization: The Internal Revenue Service (IRS)

In which domain falls the information the organization wants to share spontaneously?
The IRS wants to share information in both domains: *TAX* and *CRIMINAL*.

Domain TAX

1. What kind of information is to be shared?
   - Tax payer data or other kinds of tax- related data, collected for tax administrative purposes including civil income tax examinations as supplied by taxpayers and other parties, such as employers and financial institutions.

2. Is there a legal basis to share this information spontaneously?
   a. In national law?
   - 26 U.S.C. § 6103(k)(4) concerns tax returns and return information and provides that tax information may be exchanged with other foreign countries under an income tax treaty or other agreement for the provision of tax information to the foreign authority. The applicable exchange instrument (i.e. a tax convention or TIEA) governs whether tax information can be exchanged via a specific mode of exchange, such as spontaneous exchange. 26 U.S.C. § 6103(k)(4) and the relevant instrument permit disclosure of information if various requirements are met.

   b. In international law?
   - The United States is party to several bilateral tax treaties and tax information exchange agreements (TIEAs). Additionally, the United States is signatory to the 1998 OECD/CoE Convention on Mutual Administrative Assistance in Tax Matters (MAC), which in Art. 7 provides for the spontaneous exchange of information.

3. Under what conditions can the information be shared spontaneously?
   a. Conditions in national law regarding international cooperation
   - Under 26 U.S.C. § 6103(k)(4), the disclosure of information is permitted if various requirements are met: 'The (…) information may be disclosed to a competent authority of a foreign government which has an income tax or gift and estate tax convention, or other convention or bilateral agreement relating to the exchange of tax information with the United States but only to the extent provided in, and subject to the terms and conditions of such convention to bilateral agreement.' Usually, these conventions and agreements require the foreign government to have made a request for the information prior to the exchange, unless spontaneous exchange is provided for.
   - The provision does not provide for disclosure to foreign non- governmental organizations.
   - Disclosure of information under 26 U.S.C. § 6103(k)(4) (i.e. to competent authorities pursuant to a tax convention) may be made for the purposes provided for, and subject to the terms of, a tax convention or other exchange agreement.
   - The IRS is the competent authority to supply personal data for tax/ administrative oversight. Under 26 U.S.C. § 6103(k)(4), the agreements and conventions govern the extent to which personal data may be shared with other competent tax authorities (i.e., what is foreseeably relevant for tax administration/enforcement).

-
- There are no specific conditions for the receipt of personal data by the IRS in tax matters. Additionally, there are no restrictions as to the categories of organizations from which such data may be received. The purpose for the receipt of tax matters is for the compliance with the terms of the relevant tax convention or other exchange agreement.
- Information received under the income tax conventions or tax exchange agreements may be used for all federal income tax offences.

b. Conditions in international law regarding international cooperation
- The 'competent authority' to exchange personal data under the international legal framework is the Secretary of the Treasury, who has delegated its authority to certain members of the Large Business & International division in the IRS.
- The exchange of personal data is allowed for tax determinations, tax enforcement and the collections of taxes by the convention (MAC).
- Usually, the conventions and agreements require the foreign government to have made a request for the information prior to the exchange, unless spontaneous exchange is provided for. Additionally, under the conventions and agreements, the data must be 'foreseeably reasonable' both to the administration and enforcement of the domestic laws of the other government and must relate to the types of taxes covered by the instrument. Thus, the supply of personal data in tax matters may not be made where there is no potential relevance to the administration or enforcement of laws (no 'fishing expeditions').

c. Conditions in national privacy law/ Conditions in international privacy laws
- Generally, data subjects do not have enforceable rights with respect to data protection under US tax treaties and TIEAs, as well as the MAC.
- The Privacy Act of 1974, 5 U.S.C. § 552a applies to US residents and citizens of certain foreign countries or regional economic organizations. Moreover, the Judicial Redress Act enables a 'covered person' to bring a suit in the same manner, and to the same extent, as an 'individual' (i.e., a US citizen or permanent resident alien) may bring and obtain with respect to:
  (1) intentional or willful disclosure of a covered record under 5 U.S.C. § 552a(g)(1)(D)
  (2) improper refusal to grant access to or amendment of a covered record under 5 U.S.C. § 552a(g)(1)(A) and (B).

  Furthermore, under the Judicial Redress Act, a 'covered person' means a natural person (other than an 'individual' as defined by the Privacy Act) who is a citizen of a covered country. A 'covered country' is a country or regional economic integration organization, or member country thereof, that has been designated by the Attorney General to have met certain protections outlined in Section 2(d)(1) of said Act.
- Moreover, the US Internal Revenue Code (26 U.S.C.) includes statutes that lay down obligations regarding the gathering and processing of tax-specific data, including tax-related personal data. Accordingly, under 26 U.S.C. § 6103, unless otherwise provided by title 26, officers and employees of the US, including the IRS agents, must keep all tax returns and return information confidential. Other Title 26 provisions contain penalties for unauthorized inspection of such information.
- Additionally, the above mentioned restrictions under 26 U.S.C. § 6103 to the disclosure of information apply.

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences
   - Under the TIEAs and the MAC, protections apply on sharing and further disseminating tax data (not just personal data). Under these agreements, information may be used only for the stated reasons in the request and the information must be maintained as confidential by the recipient authority and disclosed only to those persons involved in the assessment, collection or recovery of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, taxes of that recipient Party.

5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?
   a. Procedure under national law
   b. Procedure under international law
   - Generally, US domestic law requires a treaty as a legal basis for requesting information. Furthermore, if the request contains confidential tax information, a treaty or other agreement should be the basis for the request so that the confidentiality of the request and the response can be maintained pursuant to the confidentiality requirements of such treaty or other agreement.

6. What is the procedure when the sending organization/ Country receives a request for follow-up information after a hit?
   a. Procedure under national law
   b. Procedure under international law
   - For supplying information, the IRS is the competent authority. Furthermore, 26 U.S.C. § 6103(k)(4) permits the supply of tax information pursuant to an income tax treaty or other relevant agreement for the exchange of tax information. The requesting organization must be a party to that treaty or agreement.
   - Consistent with the treaty instrument, the information supplied must be relevant or 'foreseeably relevant' to the request and related to a tax covered thereunder. Under some treaties, national law is relevant to determine what information could be supplied subject to confidentiality and disclosure laws.

Domain CRIMINAL

1. What kind of information is to be shared?
   - Taxpayer data that is used for the investigation of tax crimes and other crimes related to tax administration, as well as data gathered specifically for criminal investigations.

2. Is there a legal basis to share this information spontaneously?
   a. In national law?
   - Under 26 U.S.C. § 6103(k)(6) the disclosure of information is permitted for investigative purposes to the extent necessary to obtain information relating to such investigations, provided that (1) the disclosure concerns a tax-related matter, such as civil or criminal tax investigation, and (2) the requested information is not otherwise reasonably available.

   b. In international law?
   - The United States us not signatory to any multilateral treaties allowing specifically for the spontaneous supply of tax- related information in

criminal matters. Nonetheless, it is party to other multilateral relationships, such as the Egmont Group.

- Established in 1995, the Egmont Group is an international network seeking to improve interaction among financial intelligence units (FIUs) in the area of communications, information sharing and training coordination. Its goal is to provide a forum for national FIUs worldwide to improve support to their respective governments in the fight against money laundering, terrorist financing and other financial crimes. To be able to join the Egmont Group, an FIU must be a centralized unit within a nation or jurisdiction to detect criminal financial activity and secure adherence to laws against financial crimes. The Egmont Group now comprises more than 150 FIUs. It is evolving towards a structure of independent units who work closely together to strengthen their own countries' anti- money laundering/ counter- terrorism financing (AML/CFT) regimes, as well as the global effort of economic resistance to money launderers and terrorist financiers.

3. Under what conditions can the information be shared spontaneously?
   a. Conditions in national law regarding international cooperation

- There is not specific US law restricting the disclosure of personal data to foreign organizations. Yet, several federal and state laws governing, regulating and restricting the disclosure of sector- specific data exist, such Federal Rule of Criminal Procedure 6(e), which prohibits the disclosure of any information or records that would reveal what transpired during a grand jury investigation. Similarly, 26 U.S.C. § 6103 provides for restrictions and limitations on the supply of information, as mentioned in the *TAX* domain part.
- Spontaneous exchange of information under 26 U.S.C. § 6103 (k)(6) may be authorized only for criminal investigations undertaken by the IRS. Conversely, spontaneous exchange of information under 26 U.S.C. § 6103 (k)(4) may be authorized as provided for by a specific treaty or other exchange instrument, without regard to the geographical location of the criminal investigation taking place.
- Except for protected information under Rule 6(e) (see above), the US may disclose (supply) limited information to domestic law enforcement during an investigation into a criminal violation of the Internal Revenue Code, as long as it is in connection with audits, criminal investigations or collection, in order to obtain information not otherwise reasonably available, as provided for under 26 C.F.R. § 301.6103(k)(6)-1. Under 26 U.S.C. § 6103(k)(4) the disclosure of tax returns and return information in response to a criminal investigation undertaken by a non- US jurisdiction may be permitted, subject to the terms of the applicable exchange instrument.
- Disclosure of information under 26 U.S.C. § 6103(k)(6) (i.e. to certain officers and employers for investigation purposes) must be made for the purpose of enforcing internal revenue laws.
- Typically, under 26 U.S.C. § 6103(k)(4), tax information exchange is limited to matters covered by the treaty or convention, which is typically the investigation or prosecution of tax crimes. Under 26 U.S.C. § 6103(k)(6) the disclosure of information must be in connection to an audit, collection activity or civil or criminal tax investigations or any other offence under the internal revenue laws of the US. Information that is not a return or return information is not subject to these confidentiality restrictions on disclosure.
- The IRS is, additionally, allowed to receive personal data in criminal investigations. It needs to determine the origin of the information and confirm that the public policy or other circumstances would not limit the scope of intended use. As an example, the IRS would not typically supply information directly obtained from taxpayers to other US government

agencies for the use in criminal investigations to avoid implicating the right against self- incrimination. Similarly, receiving taxpayer information from a foreign organization may implicate these considerations as well.
- The receipt of data is allowed for all federal tax crimes under internal revenue laws, as well as crimes related to federal tax crimes.

b. Conditions in international law regarding international cooperation
-
c. Conditions in national privacy law/ Conditions in international privacy laws
- Same as above in the *TAX* domain.

4. Are the answers given also applicable for other information (which is not to be shared in first instance) in this domain? If not, give an indication of relevant differences
   - Data received in the context of investigating and prosecuting certain tax offences may be used for certain related matters controlled by statutes that are not part of the Internal Revenue Code, such as money laundering and drug or terrorism fighting.
   - Also see Q4 on the *TAX* domain.

5. What is the procedure when the receiving organization wants to ask for follow-up information after a hit?

a. Procedure under national law
b. Procedure under international law
   - Generally, US national law requires a treaty partner to send a request for information. There are no other conditions under national law for sending a request for information in criminal matters.

6. What is the procedure when the sending organization/ Country receives a request for follow-up information after a hit?

a. Procedure under national law
b. Procedure under international law
   - To supply information on even the existence of a tax examination or criminal tax investigation, the IRS needs a basis to provide information to another person or country. Under 26 U.S.C. § 6103(k)(4) the IRS may supply tax information pursuant to an international convention or agreement. Moreover, under 26 U.S.C. § 6103(k)(6) allows the IRS officer to make an ‘investigative disclosure’ that is appropriate and helpful in obtaining information to perform official duties related to an examination, investigation, or other enforcement activity under the internal revenue laws.
   - Additionally, subject to the treaty instrument the information supplied must be relevant or ‘foreseeably relevant’ (tax treaty term) to the request and must relate to a covered tax.

Annex 5: List of Consulted Officials and Experts

Bruce Paynter	Australian Taxation Office
Rebecca Moore	Australian Taxation Office
Bert Bouwen	Belgium – Special Tax Inspectorate
Amy Garson	Canada Revenue Agency
Heather Hemphill	Canada Revenue Agency
Freya Hvass	Danish Tax Agency
Henning Hoffmann	Danish Tax Agency
Udo Kroon	FCInet Secretariat
Harry Krüter	FCInet secretariat
Gonnie de Graaf-van Dijk	FCInet secretariat
Jules Anthonia	FCInet secretariat
Jarkko Mäki	Finnish Tax Administration
Lisa Yoder	Iceland – Directorate of Tax Investigations
Harald Koppe	NL – Ministry of Justice and Security/FIU.net
Margot Oenema	NL – Fiscal Intelligence and Investigation Service
Garincha Pattinaja	NL – Fiscal Intelligence and Investigation Service
Susan Kloppenborg	NL – Fiscal Intelligence and Investigation Service
Mark Brons	NL – Fiscal Intelligence and Investigation Service
Lisette Vos	NL –Prosecutor, Public Prosecutor's Office
Jaime Espantaleón	Norwegian Tax Administration
Hans Petter Tetmo	Norwegian Tax Administration
Marie Mattson Vangekrantz	Swedish Tax Agency
Anette Bergvall	Swedish Tax Agency
Petra Wagner	Swedish Tax Agency
Mike Hainey	UK – Her Majesty's Customs and Excise
Christopher Draycott	UK – Her Majesty's Customs and Excise
Jeanne Mifsud-Bonnici	University of Groningen
Catherine Jasserand-Breeman	University of Groningen
Cleve Lisecki	US – Internal Revenue Service
Katia Fano	US – Internal Revenue Service
Erick Bell	US – Internal Revenue Service

References

Balboni & Macenaite 2013
Balboni, P, Macenaite, M, 'Privacy by design and anonymisation techniques in action: Case study of Ma³tch technology', *Computer law & Security Review* 2013, p. 330-340.

Bassiouni 2008
M.C. Bassiouni, *International Criminal Law, Volume II: Multilateral and Bilateral Enforcement Mechanisms*, Leiden: Martinus Nijhoff 2008.

Belastingdienst 2013
Belastingdienst, 'Verwerkingen van persoonsgegevens door de Belastingdienst en de FIOD', August 2013.

Belastingdienst/FIOD 2014
Belastingdienst/FIOD, 'FIOD. Aansprekend opsporen', April 2014

Bertoni 2021
E. Bertoni, 'Convention 108 and the GDPR: Trends and perspectives in Latin America', *Computer Law & Security Review* (40) 2021, nr. 105516.

De Busser & Vermeulen 2010
E. de Busser & G. Vermeulen, 'Towards a coherent EU policy on outgoing data transfers for use in criminal matters? The adequacy requirement and the framework decision on data protection in criminal matters. A transatlantic exercise in adequacy', in: *EU and International Crime Control. Topical Issues*, Antwerpen: Maklu 2010.

EU Agency for Fundamental Rights 2018
EU Agency for Fundamental Rights, *Handbook on European data protection law*, Luxembourg: Publications Office of the European Union 2018.

Eurojust News 2016
Eurojust News, 'Conflicts of Jurisdiction', 2016/14.

European Law Institute Special Report 2017
European Law Institute Special Report 'Prevention and Settlement of Conflicts of Exercise of Jurisdiction in Criminal Law', 2017.

Fijnaut, Spapens & Van Daele 2005
Fijnaut, C., Spapens, T., Daele, D., *De Strafrechtelijke rechtshulp verlening van Nederland aan de Lidstaten van de Europese Unie: De politieke discussie, het juridische kader, de landelijke organisatie en de feitelijke werking*, Zeist: Uitgeverij Kerckebosch 2005.

Geelhoed, Hoving, Lindenberg & Renshof 2018
W. Geelhoed, R.A. Hoving, K. Lindenberg & A.D. Renshof, *FCInet: Legal Context and Data Protection*, Groningen: University of Groningen 2018.

Hirsch Balin 2016
Hirsch Ballin, M.F.H., 'III.11.3.4 Onregelmatigheden bij spontane rechtshulp', in: Melai,A.L./Klip, A.H., (red.), *WvSv/IISS* (online, updated 30 August 2016).

Information Commissioner's Office 2012
Information Commissioner's Office, *Anonymisation: managing data protection risk code of practice*, Wilmslow: ICO 2012.

Joubert and Bevers 1996
Joubert, C., Bevers, H., *Schengen Investigated: A Comparative Interpretation of the Schengen Provisions on International Police Cooperation in the Light of the European Convention on Human Rights*, Antwerp: Kluwer Law International, 1996.

Klip and Vervaele 2001
Klip, A.H., Vervaele, J.A.E., 'Supranationale normen voor administratieve en strafrechtelijke samenwerking', in: Vervaele, J.A.E., (red.), *Administratieve en strafrechtelijke samenwerking inzake fraudebestrijding tussen justitiële en bestuurlijke instanties van de EU-lidstaten*, Den Haag: WODC 2001, p. 7-53.

Kroon 2013
Kroon, U., 'Ma³tch: Privacy AND Knowledge: 'Dynamic Networked Collective Intelligence", in: *2013 IEEE International Conference on Big Data*, Los Alamitos: IEEE Computer society, p. 23-31.

Landelijk Informatie en Expertise Centrum 2014
Landelijk Informatie en Expertise Centrum, 'Convenant ten behoeve van Bestuurlijke en Geintegreerde Aanpak Georganiseerde Criminaliteit, Bestrijding Handhavingsknelpunten en Bevordering Integriteitsbeoordelingen', September 2014.

Nunzi 2007
A. Nunzi, 'Exchange of Information and Intelligence among Law Enforcement Authorities. A European Union Perspective', *Revue internationale de droit penal* 2007, p. 143-151.

Organisation for Economic Co-operation and Development 2006
Organisation for Economic Co-operation and Development, *Manual on the Implementation of Exchange of Information Provisions for Tax Purposes*, Approved by the OECD Committee on Fiscal Affairs on 23 January 2006.

Organisation for Economic Co-operation and Development 2021
Organisation for Economic Co-operation and Development, *Model Manual on Exchange of Information for Tax Purposes*, 2021.

Rijksoverheid 2013
Rijksoverheid, *Convenant ICOV,* 2013.

Roosendaal 2013
Roosendaal, A., *Digital Personae and Profiles in Law. Protecting Individuals' Rights in Online Contexts* (diss. Tilburg), Oisterwijk: Wolf Legal Publishers 2013.

Simonato 2011
M. Simonato, 'The 'Spontaneous Exchange of Information' between European Judicial Authorities from the Italian Perspective', *New Journal of European Criminal Law* 2011, p. 220-229.

Vermeulen et al. 2005
G. Vermeulen et al., *Availability of law enforcement information in the European Union. Between mutual recognition and equivalent right of access*, Antwerp: Maklu 2005.

Digital sources

Europol 2017

Financial intelligence unites – FIU.net. (n.d.). retrieved 15 June 2017, from https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net.

Wikipedia 2017

Wikipedia, *Rainbow table,* 31 August 2017, retrieved 26 June 2017, from https://en.wikipedia.org/wiki/Rainbow_table.

Conventions

Agreement between the Government of the Kingdom of Belgium and the Government of the Federal Republic of Germany on cooperation between police authorities and customs services in the border regions. Brussels, 27 Mar 2000 (I-39265).

Agreement between the Government of the Kingdom of Belgium and the Government of the French Republic concerning cross-border police and customs matters (with exchange of letters of 10 June 2002), Tournai, 5 March 2000 (I-46562).

Benelux Convention on Cooperation in Administrative and Criminal Matters, 's-Gravenhage, 29 March 1969.

Benelux Convention on Extradition and Legal Assistance in Criminal Matters, Brussels, 27 June 1962.

Convention on Cybercrime, Budapest, 23 November 2001.

Convention on Mutual Administrative Assistance in Tax Matters, Strasbourg, 27 May 2010.

- Protocol amending the Convention on Mutual Administrative Assistance in Tax Matters, Paris, 27 May 2010.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981.

- Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8 November 2001.

Council of Europe Convention on Action against Trafficking in Human Beings, Warsaw, 16 May 2005.

Council of Europe Convention on Laundering, Search, Seizure and confiscation of the Proceeds from Crime and on the Financing of Terrorism, Warsaw, 22 October 2014.

Council of Europe Convention on the Prevention of Terrorism, Warsaw 16 May 2005.

Council of Europe Criminal Law Convention on Corruption, Strasbourg 27 January 1999.

European Convention on Human Rights, Rome, 4 November 1950.

European Convention on Mutual Assistance in Criminal Matters, Strasbourg 20 April 1959.

- Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Strasbourg 17 March 1978.

- Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Strasbourg 8 November 2001.

Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, Brussels, 30 December 2020.

European Union documents

Treaty on European Union

Treaty on European Union, Maastricht, 7 February 1992, Trb. 1992, 74.

Charter of Fundamental Rights of the European Union

Charter of Fundamental Right of the European Union (*OJ* 2000, C 364/1)

Treaty on the Functioning of the European Union

Treaty on the Functioning of the European Union, Rome, 25 March 1957, Trb. 1957,91.

- Protocol (No 19) on the Schengen acquis integrated into the framework of the European Union (*OJ* 2012, C 326/1).

Convention Implementing the Schengen Agreement

The Convention Implementing the Schengen Agreement and the Schengen acquis, Schengen 19 June 1990, Trb. 1990, 145.

Commission Decision 2014/858/EU

Commission decision 2014/858/EU of 1 December 2014 on the notification by the United Kingdom of Great Britain and Northern Ireland of its wish to participate in acts of the Union in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Treaty of Lisbon and which are not part of the Schengen acquis (*OJ* 2014, L 345/6).

Convention on Cooperation between customs administrations

Convention drawn up on the basis of article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations, Brussel, 18 December 1997, Trb. 1998, 174.

EU Convention on Mutual Assistance in Criminal Matters

Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, Luxembourg 29 May 2000, Trb. 2000, 96.

- Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, Luxembourg 16 October 2001, Trb. 2001, 187

Consolidated version of Council Decision 2000/365/EC

Consolidated version of Council Decision 2000/365/EC of 29 may 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis (*OJ* 2014, C 430/1).

Consolidated version of Council Decision 2002/926/EC

Consolidated version of Council Decision 2002/926/EC of 22 December 2004 on the putting into effect of parts of the Schengen *acquis* by the United Kingdom of Great Britain and Northern Ireland (*OJ* 2014, C 430/2).

Council act 2000/C 197/01
Council act 2000/C 197/01 of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (*OJ* 2000, C 197/1).

Council act 2001/C 326/01
Council act 2001/C 326/01 of 16 October 2001 establishing, in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (*OJ* 2001, C 326/1).

Council Decision 2000/642/JHA
Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (OJ 2000, L 271/4).

Council Decision 2004/926/EC
Council decision 2004/926/EC of 22 December 2004 on the putting into effect of parts of the Schengen acquis by the United Kingdom of Great Britain and Northern Ireland (*OJ* 2004, L 395/70).

Council Decision 2008/615/JHA
Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, recital 18 (*OJ* 2008, L 210/1).

Council Directive 2011/16/EU
Council Directive 2011/16/EU of 15 February 2011on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC (*OJ* 2001, L 64/1).

Council Framework Decision 2002/584/JHA
Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision (*OJ* 2002, L 190/1).

Council Framework Decision 2006/9600/JHA
Council Framework Decision 2006/9600/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (*OJ* 2006, L 386/89).

Council Framework Decision 2008/977/JHA
Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (*OJ* 2008, L 350/60).

Council Regulation (EU) 904/2010
Council Regulation (EU) 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax (*OJ* 2010, L 268/1).

Council Regulation (EU) 389/2012
Council Regulation (EU) 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) No 2073/2004 (*OJ* 2012, L 121/1).

Directive 2014/41/EU
Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (*OJ* 2014, L 130/1).

Directive (EU) 2015/849
Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (*OJ* 2015, L 141/73).

Directive (EU) 2016/680
Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (*OJ* 2016, L 119/89).

Regulation (EU) 2016/679
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (*OJ* 2016, L 119/1).

Commission Communication 2017
Communication from the Commission to the European Parliament and the Council *Exchanging and Protecting Personal Data in a Globalised World*, COM(2017) 7.

Case law

European Court of Human Rights
ECtHR 23 November 2006, App.No. 73053/01 (*Jussila*).

ECtHR 17 December 1996, nr. 19187/91, ECLI:NL:XX:1996:ZB6862, NJ 1997, 699 (*Saunders v. UK,)*

Court of Justice of the European Union
Court of Justice of the European Union, 26 February 2013, C-617/10, ECLI:EU:C:2013:105 (*Akerberg Fransson*).

Court of Justice of the European Union, 14 November 2013, C-60/12, ECLI:EU:C:2013:733 (*Balaz*).

Court of Justice of the European Union, 8 September 2015, C-105/14, ECLI:EU:C:2015:555 (*Taricco*).

Netherlands
Supreme Court of the Netherlands 16 November 1999, ECLI:NL:HR:1999:ZD1451, NJ 2000, 214

Supreme Court of the Netherlands 21 January 2006, ECLI:NL:HR:2006:AU3446, NJ 2006, 365.

Supreme Court of the Netherlands 14 November 2006, ECLI:NL:HR:2006:AX7471, NJ 2007, 179.

Supreme Court of the Netherlands 12 July 2013, ECLI:NL:HR:2013:BZ3640, NJ 2013, 435

Belgium
Court of Cassation 11 March 2011, C.2009.0096.N, 174.