The Standard of Foreseeable Relevance in Privacy Enhanced Tax Information Exchange

Case study on FCInet ma³tch technology

Dr. E.A.M. Huiskers-Stoop
T. Hasen Nezhad Nisi
Prof. Dr. I.J. Mosquera Valderrama
Dr. A. Mosna
Prof. Dr. J.W. Ouwerkerk

Leiden University
Institute of Tax Law and Economics
Department of Tax Law
September 2025

Universiteit Leiden
The Netherlands

The Standard of Foreseeable Relevance in Privacy Enhanced Tax Information Exchange

Case study on FCInet ma³tch technology

Dr. E.A.M. Huiskers-Stoop
T. Hasen Nezhad Nisi
Prof. Dr. I.J. Mosquera Valderrama
Dr. A. Mosna
Prof. Dr. J.W. Ouwerkerk

Leiden University
Institute of Tax Law and Economics
Department of Tax Law
September 2025

Universiteit Leiden
The Netherlands

Preface

Since the turn of the century, the exchange of information has become a vital tool in the fight against tax evasion and aggressive tax avoidance. A strong information position of governments worldwide is needed to tackle tax fraud, financial crime, and other crimes that undermine society. At the same time, these governments must uphold and safeguard public values, in particular the protection of taxpayer data and privacy. This creates a challenging dual role for government organisations that collect and use data for the proper execution of their work. The *Forum of Heads of Tax Crime Investigation*, held under the auspices of the OECD, recognised this duality and initiated the FCInet-platform, which houses a built-in privacy enhancing technology named 'ma^{3}tch', to meet this challenge. FCInet is focused on 'getting the right information, at the right time, in the right way, from and to the right place'. Organisations that use this instrument must comply with the legal requirements for international cooperation and information exchange, and the associated data protection and privacy laws.

FCInet can be described as a decentralised government computer system that enables public administrations from different countries to cooperate, while respecting each other's local autonomy. The ma^{3}tch technology generates a filter from local data sources that are autonomously selected by the sending organisation. This filter, created using a sophisticated set of algorithms, is then shared with one or more peer organisations, also selected by the sender. The receiving organisation can anonymously check whether (selected) keys from its own database are present in the filter. The ma^{3}tch technology thus enables competent authorities to comply with their international commitments to share information in support of peer organisations' investigation into criminal offenses and tax fraud. In today's world, technologies like ma^{3}tch, when used under the appropriate legal basis, can conduct such a qualification process in a more efficient and privacy-friendly manner.

A question currently under debate is if all data used for ma^{3}tch needs to have a visible relation to the jurisdiction of the peer organisation *upfront* – so before sharing the filter – or if this is unnecessary, since a hit or commonality regarding an individual under investigation by a peer organisation, based on the data in the filter, is always considered relevant. The present research demonstrates that both aspects of this question must be answered in the negative: (1) the data used for ma^{3}tch does not need to have any visible relationship with the receiving jurisdiction before the filter is shared, except in some cases where certain jurisdictions, for example, require *prior authorisation* by the sending State for the use of the data for *purposes other than taxation* or *transmission to third parties* by the receiving State; (2) a hit or commonality on a person under investigation by a peer organisation cannot be considered 'relevant' for the spontaneous ma^{3}tch exchange, as long as this hit has not also been validated by the sending organisation.

Another question under debate is whether – given the specific characteristics of the technology – the sharing of filters constitutes a form of 'fishing', where one seeks to determine whether certain individuals are active in other jurisdictions. This question must also be answered in the negative. The fact that the persons included in the filter have been subjected to an investigation for a specific fraudulent typology or scheme, is generally a sufficient reason to escape the qualification of fishing expedition: "An ongoing examination or investigation of a person(s) is generally accepted as proof of foreseeable relevance". These and more questions – including how foreseeable relevance should be interpreted for spontaneous exchange of information, such as through FCInet ma^{3}tch, how the standard relates to the right to privacy and data protection, and how the concept of foreseeable relevance relates to the exchange of information in criminal proceedings – are addressed in this report. Chapter 6 brings the findings together and will elaborate on any legal challenges to consider.

This case study is conducted by Leiden University in a collaboration between the departments of Tax Law, represented by Esther Huiskers-Stoop, Tofigh Hasen Nezhad Nisi and Irma Mosquera Valderrama, and Criminal Law, represented by Anna Mosna and Jannemieke Ouwerkerk. The research was completed on July 17, 2025. More recent sources were only selectively taken into account. We thank the Dutch *Ministry of Finance* for the confidence placed in us to conduct this research. More specifically, we would like to thank the board of FCInet and the experts who have patiently given us insight into the innovative ma^{3}tch technology and its operation.

Leiden, September 2025

Executive Summary

Since the early 2000s, the international exchange of information has become an essential tool in the fight against tax fraud, tax evasion, and other financial crimes. Governments face a dual challenge: ensuring that foreseeably relevant data is exchanged swiftly and effectively, while at the same time protecting the privacy and personal data of taxpayers. To address this balance, the *Forum of Heads of Tax Crime Investigation* (held under the auspices of the OECD) launched the FCInet-platform, incorporating the privacy-enhancing ma^{3}tch technology. This study explores how the principle of foreseeable relevance applies within the context of information exchange using FCInet ma^{3}tch.

Article 26 of the OECD Model Tax Convention on Income and Capital provides a legal foundation for the *bilateral* international exchange of tax information. It outlines three methods of exchange: spontaneous, automatic, and upon request. Central to all three, is the principle of foreseeable relevance, which requires that any data exchanged must be potentially useful for the tax enforcement purposes of the receiving State.

FCInet's ma^{3}tch technology operates within this legal framework, by enabling bilateral data comparisons, using filters containing data that is hashed and pseudonymised. This privacy-preserving approach allows authorities to identify potential matches, referred to as 'hits', without disclosing personal data unless further verification confirms the relevance of the information. Only when a hit is validated, personal data protections, under both the sending and receiving States' legal frameworks, come into full effect. Ma^{3}tch does not circumvent or replace existing legal obligations. Instead, it functions as a tool to enhance compliance, by supporting lawful and limited interference with taxpayer privacy.

Building on this legal context, the study presents a comparative analysis of eleven countries, both within and outside the European Union, to assess how the principle of foreseeable relevance is applied in practice. While most jurisdictions adhere to the OECD standard, important national variations influence the operation of information exchange.

Some countries require prior authorisation by the competent authority, or in a rare number of cases advance notification to the taxpayer, before data can be shared. Others permit the use of received information for non-tax purposes, such as for money laundering investigations or oversight activities, subject to specific legal conditions. In certain jurisdictions, the exchange of information is limited strictly to competent tax authorities, whereas others extend this capability to law enforcement agencies, supervisory bodies or even third countries. Countries with well-developed and clear legal frameworks for exchange, such as the United States and France, have demonstrated a higher frequency and broader scope of exchanges.

In all cases, the foreseeable relevance of the data must be established at the moment the filter is shared, or earlier if prior authorisation or prior notification obligations apply. Given the global drive for international exchange of tax information 'to the widest possible extent', these latter cases are rare and will continue to decline in number. Although a validated hit confirms the actual relevance of the data, such confirmation is not required to meet the standard of foreseeable relevance. Robust privacy and data protection laws, such as the EU's GDPR, are critical, particularly when pseudonymised but potentially identifiable data is involved.

Complementing this legal and procedural reality, the ma^{3}tch technology processes compressed, double-hashed data that cannot be directly traced to individuals unless a match is validated. While the data used is pseudonymised, any confirmed match constitutes an interference with the right to privacy, triggering the need to comply with applicable data protection laws. Ma^{3}tch is designed to limit data sharing, as only a verified 'hit' prompts a follow-up information request. This approach aids in preventing so-called fishing expeditions, being random or speculative data requests without a clear investigative link, which are prohibited under Article 26 of the OECD Model Tax Convention.

From these findings it is clear that, in the context of spontaneous information exchange, the principle of foreseeable relevance requires the information 'must at least be capable of being of interest to the receiving State'. This standard is less stringent than that applied to information exchanged upon request, which demands more specific knowledge and justification. The FCInet ma^{3}tch technology supports this framework by limiting data exchange to cases where relevance is likely, thereby enhancing efficiency and privacy. Sharing a filter also does not constitute a fishing expedition, as it targets individuals already under investigation, prevents bulk requests, and limits follow-up to cases where there is a hit and thus relevance. Upon a verified hit, pseudonymised data is subject to applicable privacy regulations, which vary by jurisdiction.

In the context of criminal law, the term foreseeable relevance is not used, but comparable relevance thresholds are applied. The design of ma^{3}tch, which avoids indiscriminate or bulk data exchange, does not seem to be in violation of these standards and does, therefore, not appear to be legally incompatible. However, the study notes that increasing reliance on informal exchanges in criminal matters (nota bene the concept of informality in the field of criminal law refers to modalities that, while still being based on a specific legal framework, impose fewer procedural requirements than what formal exchanges in criminal law would require) in general could undermine the use of formal channels of information exchange and, thus, water down procedural safeguards in criminal proceedings. While the use of ma^{3}tch also enables informal exchange of information in criminal matters, it must be noted that it minimises the interference with the individual rights to privacy and to data protection.

To further enhance the effectiveness and legal consistency of information exchange via FCInet ma^{3}tch, the foreseeable relevance standard should be reassessed in light of emerging digital tools. Domestic privacy laws should be aligned with international standards such as the EU GDPR, to support secure and lawful exchanges. Legal frameworks must clearly define conditions for sharing filters, especially where prior authorisation or taxpayer notification is required. A shared oversight mechanism among participating jurisdictions is recommended to promote consistent application. Anti-discrimination safeguards should be incorporated into the FCInet *User Protocol* to prevent bias in filter design. Additionally, high data precision is essential to reduce false positives and ensure accurate validation. While certain risk factors remain, procedural safeguards and jurisdictional differences in data protection, FCInet facilitates an efficient, lower-risk, and privacy-conscious exchange of tax information. It significantly limits the risk of exchanging irrelevant data or engaging in fishing expeditions, and thus enhances the ability to effectively exchange information.

Table of Contents

Preface **2**

Executive Summary **4**

Tables and Figures **10**

Tables 10

Figures 10

Abbreviations **10**

1. Introduction **13**

1.1 Instruments governing the exchange of tax information 13

1.2 Privacy enhanced FCInet ma³tch technology 18

1.3 The standard of foreseeable relevance in tax information exchange 21

1.4 The concept of relevance in cooperation regarding criminal matters 22

1.5 Main research question 23

1.6 Method and accountability 25

1.7 Scope, aim and relevance 27

1.8 Core concepts 29

2. Reasoning and legal context of the foreseeable relevance standard **35**

2.1 Evolution of Article 26 OECD-MC 35

2.1.1 Changes in 2005 ..... *38*

2.1.2 Changes in 2010 ..... *42*

2.1.3 Changes in 2014 ..... *44*

2.1.4 Changes in 2024 ..... *47*

2.2 Exchange of information on request 49

2.3 Spontaneous exchange of information 52

2.4 Protection of taxpayer information 56

2.5 Preliminary conclusion 58

3. Comparative analyses across jurisdictions: notable trends and practices **63**

3.1 Exchange of information between the EU States 64

3.1.1 Instruments governing the exchange of information *64*

3.1.2 Local differences in the application of instruments *66*

3.1.3 The application of Taxpayer Rights and Secrecy Rules *68*

3.2 Exchange of information by non-EU States 68

3.2.1 Instruments governing the exchange of information *68*

3.2.2 Local differences in the application of instruments *70*

3.2.3 The application of Taxpayer Rights and Secrecy Rules *71*

3.3 Preliminary conclusion 72

4. FCInet ma³tch technology in the light of tax data protection **77**

4.1 FCInet ma³tch technology 77

4.2 Technical phases related to spontaneous exchange of information 78

4.2.1 The start-up phase *78*

4.2.2 The execution phase *81*

4.3 Technical phases related to information exchange on request 83

4.3.1 The verification phase *83*

4.3.2 The completion phase *85*

4.4 Assessment against the universal right to privacy and data protection 85

4.4.1 Is there any processing of personal data? ... *86*
4.4.2 Do the privacy regulations apply? ... *88*
4.4.3 Is the infringement provided by law? ... *90*
4.4.4 Is the infringement necessary? ... *91*
4.4.5 Is the infringement proportionate? ... *92*
4.4.6 Is the infringement subsidiary? ... *92*
4.5 Additional assessment against the EU GDPR ... 93
4.5.1 Is the data processed in a lawful, fair and transparent manner? ... *94*
4.5.2 Have data been collected for specified, explicit and legitimate purposes? ... *95*
4.5.3 Is the right of access to and rectification of the personal data provided? ... *95*
4.6 Preliminary conclusion ... 96
5. Interdisciplinary reflections from a criminal law perspective ... 101
5.1 Examinations and investigations in criminal matters ... 101
5.2 Legal instruments governing the cross-border exchange of information ... 103
5.2.1 Judicial versus police cooperation ... *104*
5.2.2 Formal versus informal exchange ... *105*
5.3 Concepts comparable to the foreseeable relevance standard ... 107
5.3.1 Exchange of information on request ... *107*
5.3.2 Spontaneous exchange of information ... *112*
5.4 Relation between relevance criterion and applicable data protection ... 115
5.5 Preliminary conclusion ... 116
6 Summary and conclusion ... 121
6.1 Reply to the research question ... 123
6.2 Other conclusions ... 130
6.3 Recommendations ... 133
6.4 Final remarks ... 135
Annex 1: Descriptions of States involved in the comparative analyses ... 139
1.1 The EU States ... 139
1.1.1 France ... *139*
1.1.2 Germany ... *142*
1.1.3 Italy ... *144*
1.1.4 Spain ... *146*
1.2 Non-EU States ... 148
1.2.1 Canada ... *148*
1.2.2 Colombia ... *149*
1.2.3 Indonesia ... *150*
1.2.4 Mexico ... *151*
1.2.5 Nigeria ... *152*
1.2.6 South Africa ... *153*
1.2.7 The United States of America ... *154*
Annex 2: Legal instruments governing cooperation in criminal matters ... 159
Applicable legal instruments and respective scope ... 159
Annex 3: Literature and Case Law ... 165
Literature ... 165
Case Law ... 173
Credits ... 174

Tables and Figures

Tables

1. Indicators for the assessment of the foreseeable relevance standard in tax matters (Section 2.5)
2. Questionnaire to identify relevant aspects for the standard of foreseeable relevance (Section 3.3)
3. Technical phases of FCInet ma³tch in the light of personal data protection and the foreseeable relevance standard (Section 4.6)
4. Categorisation of legal instruments generally applicable to the exchange of information in criminal investigation (Section 5.2.2)

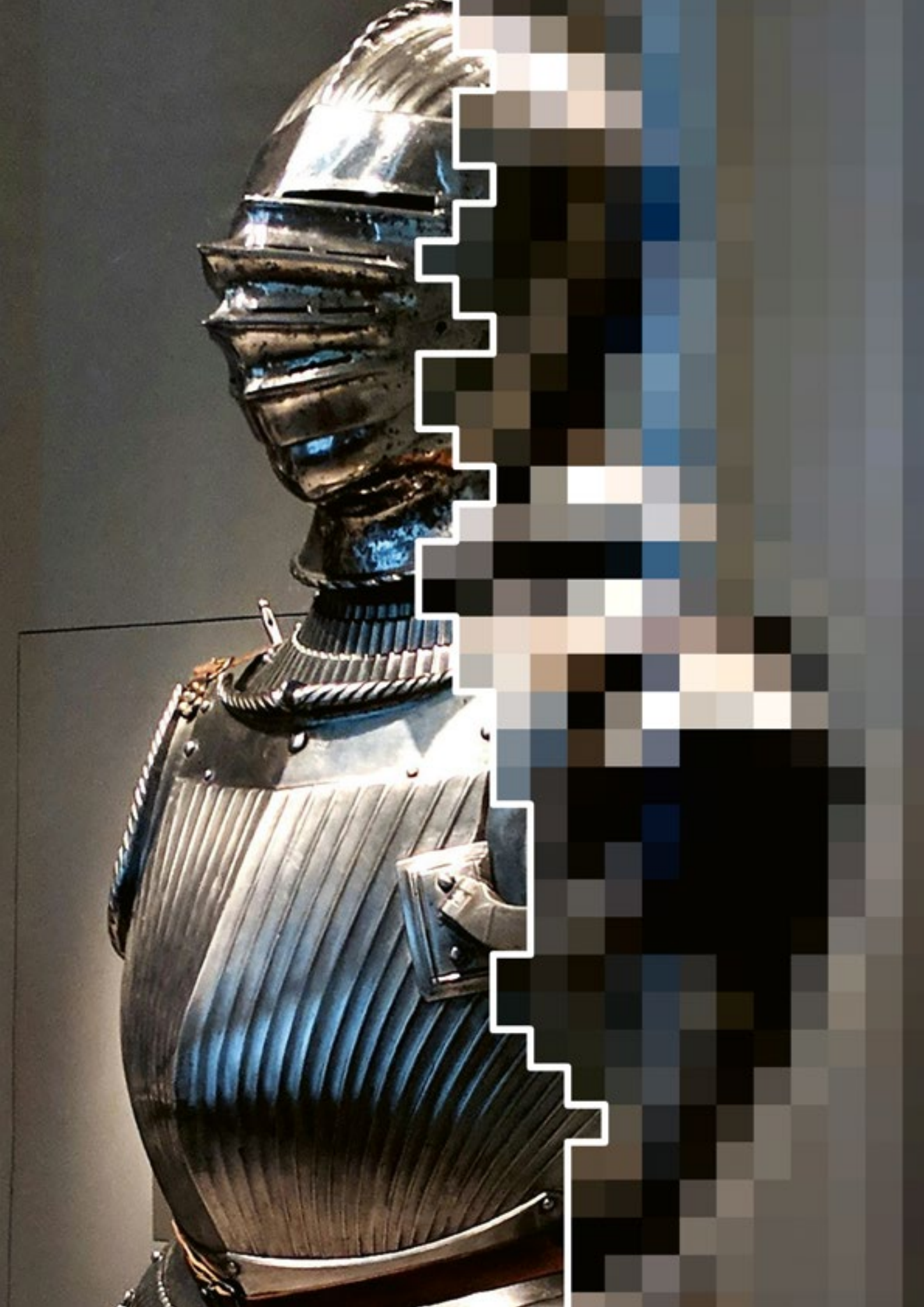
Figures

1. FCInet ma³tch technology and the standard of foreseeable relevance in privacy enhanced tax information exchange (Section 4.1)

Abbreviations

AIA	Access to Information Act
AE	Agenzia delle Entrate
AML	Anti-Money Laundering
ANPR	Automatic Number Plate Recognition
APA	Advance Pricing Agreements
AO	Abgabenordnung
AT	Anagrafe Tributaria
ATR	Advance Tax Rulings
Art.	Article(s)
BDSG	Bundesdatenschutzgesetz
BRIICS	Brasil, Russia, India, Indonesia, China en South Africa
BZSt	Bundeszentralamt für Steuern
CbCR	Country by Country Reporting
CCN	Common Communication Network
CE	(French) Conseil d'État
CE	Constitución Española
Charter	Charter of the fundamental Rights of the European Union
CIAT	Inter-American Center of Tax Administrations
CITA	Companies Income Tax Act
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CRA	Canadian Revenue Agency
CRS	Common Reporting Standard
c.q.	casu quo
DAC	Directive on Administrative Cooperation
DF	Dipartimento delle Finanze
DGFIP	Direction Générale des Finances Publiques
Diss.	Dissertation
DTC	Double Taxation Convention
ECHR	European Convention on Human Rights
ECI	Equipo Central de Información
ECLI	European Case Law Identifier
ECRIS-TCN	European Criminal Records Information System for third-country nationals

EES	Entry/Exit System
e.g.	exempli gratia
EIO	European Investigation Order
EOI	Exchange of information
EOIR	Exchange of information on request
EU	European Union
ETIAS	European Travel Information and Authorisation System
ETS	European Tax Treaties
FCInet	Financial and/or Criminal Investigation network
FIOD	Fiscal Intelligence and Investigation Service
FIRS	Federal Inland Revenue Service
FIU	Financial Intelligence Unit
FTV	Fiscaal Tijdschrift Vermogen
GDF	Guardia di Finanza
GDPR	General Data Protection Regulation
i.a.	inter alia
IBFD	International Bureau of Fiscal Documentation
ICCPR	International Covenant on Civil and Political Rights
i.e.	id est
IRC	Internal Revenue Code
IRM	Internal Revenue Manual
IRS	Internal Revenue Services
ITA	Income Tax Act
LB&I Division	Commissioner of the Large Business and International Division
LEAs	Law Enforcement Authorities
LED	Law Enforcement Directive
LGT	Ley General Tributaria
MAAC	Multilateral Convention on Mutual Administrative Assistance in Tax Matters
MLA	Member of the Legislative Assembly
MLA	Mutual Legal Assistance (in criminal matters)
MNes	Multinationals
NDPR	Nigeria Data Protection Regulation
nr.	number
OECD	Organisation for Economic Co-operation and Development
OECD-MC	OECD Model Tax Convention on Income and Capital
OECD-TIEA	OECD Tax Information Exchange Agreement Model
p.	page
Par.	paragraph
PD 1973	Presidential Decree 1973
PETs	Privacy Enhancing Technologies
PITA	Personal Income Tax Act
Sec.	Section
SteAHG	Steueramtshilfegesetz
TAAA	Tax Administrative Assistance Act
TFEU	Treaty on the Functioning of the European Union
TIEA	Agreement on Exchange of Information on Tax matters
TPB	Tax Procedures Book
UAE	United Arab Emirates
UBO	Ultimate beneficial owner
UN	United Nations
UN Model Tax Convention	UN Model Double Taxation Convention between Developed and Developing Countries
U.S.	United States of America
VAT	Value Added Taxes
VATA	Value Added Tax Act
VIS	Visa Information System
VPN	Virtual Private Network
WWF	World Wide Fund for nature



Chapter 1

Introduction

Since the turn of the century, the exchange of information has become an important tool in the fight against tax evasion and undesirable tax avoidance. A strong information position of governments worldwide is needed to tackle tax fraud, financial crime, and other crimes that undermine society. At the same time, these governments must safeguard and protect public values, particularly the protection of taxpayer information. Hence, there is a challenging dual role for government organisations that collect and use data for the proper execution of their work. The *Forum of Heads of Tax Crime Investigation*, held under the auspices of the *Organisation for Economic Co-operation and Development* (hereinafter: OECD), recognised this duality and initiated the *Financial and/or Criminal Investigation network* (hereinafter: FCInet) with built-in privacy enhancing technology (hereinafter: ma^{3}tch) to meet this challenge, by 'getting the right information, at the right time, in the right way, from and to the right place'.[1] The FCInet ma^{3}tch technology is a form of *Privacy By Design*, and has been developed to increase the efficiency (speed) and effectiveness (targeting) of cross-border information exchange.[2] This technology makes aggregated compressed and non-reversible 'double hashed personal data' available to a partner organisation by sharing filters, without exposing the underlying data. Partners compare the filter with their own data and identify a possible 'hit'. After verification with the sending State, the receiving State may request person-specific tax information. It seems obvious that governments using this instrument must, and aim to, comply with the legal requirements for international cooperation and information exchange, including the associated data protection and privacy laws.

1.1 Instruments governing the exchange of tax information

The international exchange of information in tax matters has a long tradition, based on the understanding that transparency is essential for the effective functioning of a tax system. What started out almost a century ago, has since developed into an extensive network of bi- and multilateral instruments on exchange of information.[3]

1 See for more information on the FCInet initiative: https://www.fcinet.org/. See for a description of the technology: U. Kroon, *Smart Intelligence Beyond Borders: understanding FCInet and ma^{3}th technology, 'a blueprint for privacy by design'*, Thesis Master ICT in Business and the Public Sector, LIACS, Leiden University, 2021, retrieved from: https://theses.liacs.nl/1773 (hereinafter: Kroon 2021).

2 FCInet, *Protocol for Cooperation between FCInet participants*, The Hague (2022), Netherlands, not published (hereinafter: FCInet 2022, *User Protocol*), p. 2. Fundamental elements of Privacy By Design is to guarantee data anonymisation, data minimisation and data security, see for instance P. Balboni and M. Macenaite, 'Privacy by design and anonymisation techniques in action: Case Study of Ma^{3}tch technology', *Computer Law & Security Review* 29 (2013) (hereinafter: Balboni & Macenaite 2013), p. 332.

3 E.A.M. Huiskers-Stoop, A.C. Breuer and M. Nieuweboer, 'Exchange of information, tax confidentiality, privacy and data protection from an EU perspective', *Erasmus Law Review* 2022(2): 86-99 (hereinafter: Huiskers-Stoop, Breuer & Nieuweboer 2022). The roots of the exchange of tax information go back to the League of Nations' 1927 draft for a Bilateral Convention on Administrative Assistance in Matters of Taxation.

These instruments can be divided into three categories: (1) bilateral tax conventions, (2) multilateral tax conventions, and (3) the EU Directive on Mutual Assistance (Directive 2011/16/EU).[4] Below, we examine each of these categories in more detail.

1. Bilateral tax conventions

The first category includes, among other elements, the introduction of Article 26 of the OECD Model Tax Convention on Income and Capital by the OECD (hereinafter: OECD-MC) in 1998, by governing the (i) exchange on request, (ii) automatic exchange in very specific situations and (iii) spontaneous exchange of information.[5] Spontaneous exchange of information differs from the other two forms, in that information is provided without prior request from or agreement with another State.[6] A spontaneous exchange occurs when a State, in the course of the implementation of its own tax legislation, obtains information and considers that it may be of interest to another State and transmits it without the latter State's request.[7] Spontaneous exchange differs from automatic exchange, in that it generally involves the provision of specific information about one or more specific taxpayers, while automatic exchange involves the predetermined provision of information about a specific group of taxpayers.

The OECD-MC is accompanied by an extensive Commentary, which since 2005 also refers to data protection.[8] Article 26 of the OECD-MC provides a framework for the exchange of information by specifying the conditions under which, information relevant to the taxation or enforcement of domestic tax law of the receiving State, may be exchanged. One of the conditions since 2005 is that the information to be provided is 'foreseeably relevant' to the taxation of the receiving State:

> *"The competent authorities of the Contracting States shall exchange such information as is **foreseeably relevant** for carrying out the provisions of this Convention or to the administration or enforcement of the domestic*

4 See in this respect M. Merkx, 'Exchange of Information and Administrative Cooperation between Countries in a Globalised and Digital Economy', *Erasmus Law Review*, 2, (2022): 73-75, retrieved from: https://www.erasmuslawreview.nl/tijdschrift/ELR/2022/2/ELR-D-23-00001.

5 See for instance OECD, *Model Tax Convention on Income and on Capital: condensed Version 2017*, Paris: OECD Publishing (2017), retrieved from: https://www.oecd.org/en/publications/model-tax-convention-on-income-and-on-capital-condensed-version-2017_mtc_cond-2017-en.html#page30, on Article 26: p. 487-507 (hereinafter: OECD Commentary 2017), par. 9.

6 Y. Jeong, 'Spontaneous Exchange of Information', in: O.C. Günther and N. Tüchler (red.), *Exchange of Information for Tax Purposes*, Vienna: Linde Verlag (2013), retrieved from: https://beckassets.blob.core.windows.net/product/toc/13113214/9783707324099_toc_003.pdf (hereinafter: Jeong 2013), p. 447.

7 Inter-American Centre of Tax Administrations (hereinafter: CIAT), *Manual for implementing and carrying out Information exchange for tax purposes. General and legal aspects of information exchange*, CIAT Publishing (2006), retrieved from: https://www.ciat.org/Biblioteca/DocumentosTecnicos/Ingles/2006_CIAT_manual_information_exchange.pdf (hereinafter: CIAT 2006), p. 11.

8 D.M. Ring, 'Article 26: Exchange of information – Global Tax Treaty Commentaries', *Global Tax Treaty Commentaries IBFD* (2016) (hereinafter: Ring 2016), Sec. 1.2. The OECD commentary 2005 refers as an earlier example of a privacy and data protection regulation to the CoE *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, retrieved from: https://www.coe.int/en/web/impact-convention-human-rights/convention-for-the-protection-of-individuals-with-regard-to-automatic-processing-of-personal-data#/.

laws concerning taxes of every kind and description imposed on behalf of the Contracting States, or of their political subdivisions or local authorities, insofar as the taxation thereunder is not contrary to the Convention. The exchange of information is not restricted by Articles 1 and 2."

This foreseeable relevance standard aims to protect taxpayers from unspecified, speculative and irrelevant request and storage of information. However, since its introduction, Article 26 OECD-MC has been amended and expanded many times. The changes aim to improve the conditions for the exchange of information, limit possible rejections of requests and promote data protection.

As a result of the desirability of bilateral tax treaties between developed and developing countries, the United Nations introduced the *Model Double Taxation Convention between Developed and Developing Countries* in 1980 (hereinafter: UN Model Tax Convention).[9] Article 26 of this UN Model Tax Convention embodies rules under which information may be exchanged to 'the widest possible extent', both to facilitate the proper application of the treaty and to assist States in the enforcement of their domestic tax laws.[10] Article 26(1) of the UN Model Tax Convention (version 2021), closely parallels Article 26 of the OECD-MC:

"The competent authorities of the Contracting States shall exchange such information as is ***foreseeably relevant*** *for carrying out the provisions of this Convention or to the administration or enforcement of the domestic laws of the Contracting States concerning taxes of every kind and description imposed on behalf of the Contracting States, or of their political subdivisions or local authorities, insofar as the taxation thereunder is not contrary to the Convention. In particular, information shall be exchanged that would be helpful to a Contracting State in preventing avoidance or evasion of such taxes. The exchange of information is not restricted by Articles 1 and 2".*

In addition to the provision in the OECD-MC, the OECD issued a *Tax Information Exchange Agreement Model* (hereinafter: OECD-TIEA) in 2002, as an important alternative for States wishing to provide for information exchange, despite the absence of a bilateral Double Taxation Convention (hereinafter: DTC).[11] According to Article 5 OECD-MC, TIEAs provide for (bi- and multilateral[12]) information exchange *on request* and do not cover spontaneous or automatic exchange of information, unless "Contracting Parties may wish to consider expanding their co-operation in matters

9 See for the last modified version UN *Model Double Taxation Convention between Developed and Developing Countries*, New York (2021), retrieved from: https://financing.desa.un.org/sites/default/files/2023-05/UN%20Model_2021.pdf (hereinafter: UN Model Tax Convention), Article 26 Exchange of information on p. 41-42 and its Commentary on p. 752-801.

10 See I.J. Mosquera Valderrama, 'EU and OECD Proposals for International Tax Cooperation: A New Road?', *Tax Notes International* (2010), Vol. 59, nr. 8 (hereinafter: Mosquera Valderrama 2010), p. 611.

11 Ring 2016, Sec. 1.2.5.2 and 3.1.1. A DTC can be defined as the basis for classification and sourcing of income and the allocation of taxing rights between source and resident States.

12 See Mosquera Valderrama 2010, p. 611.

of information exchange for tax purposes by covering automatic and spontaneous exchanges and simultaneous tax examinations".[13] OECD-TIEAs can especially help competent authorities of contracting States with bringing traditional 'tax havens' and States – that do not have large bilateral tax treaty networks – into the international system for exchanging tax information. Although the provisions in the OECD-TIEA explicitly focuses on exchange upon request, the wording and meaning of Article 1(1) OECD-TIEA is closely aligned with the provisions of Article 26 of the OECD-MC[14]:

> *"The competent authorities of the Contracting Parties shall provide assistance through exchange of information that is* ***foreseeably relevant*** *to the administration and enforcement of the domestic laws of the Contracting Parties concerning taxes covered by this Agreement. Such information shall include information that is foreseeably relevant to the determination, assessment and collection of such taxes, the recovery and enforcement of tax claims, or the investigation or prosecution of tax matters. Information shall be exchanged in accordance with the provisions of this Agreement and shall be treated as confidential in the manner provided in Article 8. The rights and safeguards secured to persons by the laws or administrative practice of the requested Party remain applicable to the extent that they do not unduly prevent or delay effective exchange of information."*

2. Multilateral tax conventions

In the second category, for example, in 1988 the OECD and the Council of Europe (hereinafter: CoE) jointly developed a *Multilateral Convention on Mutual Administrative Assistance in Tax Matters* (hereinafter: MAAC), which was amended by protocol in 2010.[15] The MAAC is the most comprehensive multilateral instrument available for all forms of administrative cooperation between States in the assessment and collection of taxes, in particular to tackle tax evasion and avoidance. The amended Convention facilitates international cooperation to *all countries*, including developing countries, for a better operation of national tax laws, while respecting the fundamental rights of taxpayers. Article 4(1) of the MAAC (version 2010) contains a general provision for the exchange of information:

13 OECD, *Agreement on Exchange of Information on Tax Matters*, Paris: OECD Publishing (2002), retrieved from: https://www.oecd.org/en/publications.html (hereinafter: OECD Model TIEA 2002), Article 5, par. 1.

14 Article 1 OECD Model TIEA 2002.

15 See OECD and CoE, *The Multilateral Convention on Mutual Administrative Assistance in Tax Matters: Amended by the 2010 Protocol*, Paris: OECD Publishing (2011), retrieved from: https://www.oecd.org/en/publications/the-multilateral-convention-on-mutual-administrative-assistance-in-tax-matters_9789264115606-en.html. See also CoE, *Explanatory Report to the MAAC as amended by the 2010 Protocol*, European Tax Treaties (ETS) No. 127 (2011), retrieved from: https://rm.coe.int/16800cb345. Other examples include among others the *Nordic Assistance Convention* and the *Model Agreement on the Exchange of Tax Information* (Article 4 Spontaneous Information) developed by CIAT.

> *"The Parties shall exchange any information, in particular as provided in this Section, that is **foreseeably relevant** for the administration or enforcement of their domestic laws concerning the taxes covered by this Convention."*

In addition to provisions on the automatic exchange of information (Article 5) and the exchange on request (Article 6), Article 7 of the MAAC contains specific rules on circumstances where information of which a party 'has knowledge', shall be exchanged spontaneously. Although the term 'spontaneous' may carry somewhat non-committal connotations, this form of information exchange generally has a mandatory character. Article 7 can be regarded as the starting point for spontaneous exchange of information between the Member States of the CoE, the Member States of the OECD, and other States which have ratified the MAAC.[16]

3. EU Directive on Mutual Assistance (Directive 2011/16/EU)

At the European level, for example, the Council adopted Directive 77/799/EEC in 1977, concerning mutual assistance between the competent authorities of EU Member States in the field of direct and indirect taxation.[17] The objective of this directive was to strengthen the collaboration between tax administrations of Member States, in order to obtain greater transparency in tax matters. In 2011, the 1977 Directive was replaced by a new *Directive on Administrative Cooperation* in the field of taxation, and established certain procedures for information exchange on request, as well as automatic exchange and spontaneous exchange (Directive 2011/16/EU, hereinafter: DAC).[18] Especially with respect to both the spontaneous exchange of information (Article 9) and the exchange on request (Article 5), Article 1(1) of the DAC requires the information to be 'foreseeably relevant' for the administration and enforcement of the tax laws of the Member States:

> *"This Directive lays down the rules and procedures under which the Member States shall cooperate with each other with a view to exchanging information that is **foreseeably relevant** to the administration and enforcement of the domestic laws of the Member States concerning the taxes referred to in Article 2."*

16 Currently over 140 countries have signed the Convention, including all G20 countries, all BRIICS, almost all OECD countries, major financial centers and a growing number of developing countries. See https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/convention-on-mutual-administrative-assistance-in-tax-matters/status_of_convention.pdf.

17 EC Mutual Assistance Directive, 19 December 1977. This Directive covered direct taxation, excise duties, taxation of insurance premiums and VAT, see Jeong 2013, p. 448.

18 Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, retrieved from: https://eur-lex.europa.eu/eli/dir/2011/16/oj.

Over the years, the DAC has been amended and expanded many times as well, introducing mainly new automatic reporting obligations to taxpayers, tax administrations, financial institutes, tax intermediaries, digital platform operators and crypto-asset service providers.[19]

1.2 Privacy enhanced FCInet ma³tch technology

Although tax authorities have a range of instruments for the exchange of information at their disposal, the OECD-MC, UN Model Tax Convention, OECD-TIEA, the MAAC and the DAC are regarded as the primary instruments for tax purposes.[20] Despite the availability of these instruments, many countries still face legal as well as practical challenges within the realm of information exchange, such as not having the resources to create information management systems which adhere to the law and are feasible to implement and maintain. FCInet ma³tch enables innovation in information exchange systems, thereby helping to ensure that no country is left behind. FCInet, similar to the purpose of Article 26 of the OECD-MC as a general framework, also aims to assist States in achieving proper taxation on a *bilateral basis*, while respecting the *data and privacy rights* of taxpayers. The use of this system carries the potential to minimise bulk requests, and limits further investigations into cases where there is a 'match' between an individual in the database of the sending State and the database of the receiving State, thus achieving a more efficient exchange of information between States.

Since FCInet ma³tch is a *decentralised* system, data is never kept on a centralised server that could be accessed by organisations from partner States. This ensures that the data remains within the power of the sending State, which can decide for itself what data is made available to which partner State and when. While each State can freely decide with which other States it wishes to connect, FCInet emphasises that it is "essential to

19 See the following overview: DAC2 (2014) implements the global Standard for Automatic Exchange of Financial Account Information in Tax Matters (also known as the Common Reporting Standard, (hereinafter: CRS); DAC3 (2015) adds information concerning Advance Tax Rulings (hereinafter: ATR) and Advance Pricing Agreements (hereinafter: APA) to the scope of the mandatory automatic exchange of information; DAC4 (2016) further expands the scope of mandatory automatic exchange of information by including the obligation on multinational enterprises to create Country by Country Reporting (hereinafter: CbCR) and on tax administrations to share the reports with certain other Member States; DAC5 (2016) gives tax authorities of the Member States access to the Anti-Money Laundering (AML) information obtained pursuant to Directive (EU) 2015/849 (the identification of the beneficial owners of intermediary structures); DAC6 (2018) goes further by imposing mandatory disclosure rules for intermediaries engaged in potentially aggressive tax structures and to automatically share this information with all Member States; DAC7 (2021) aims to provide tax administrations with comprehensive information about activities on online platforms; DAC8 (2023) imposes reporting obligations on crypto asset service providers and automatically information exchange with other Member States; DAC9 (2025) aims to help large companies (MNes) with their filing obligations under the Pillar 2 Directive at the central level of an entire group (Directive (EU) 2022/2523).

20 For the sake of completeness, it should be noted that where the European Commission has legislative powers with respect to the DAC, the OECD Model Tax Convention and its Commentary, for instance, are not legally binding, but the result of unilateral acts of an international organisation and the recommendations to its Member States. For a more detailed overview of exchange of information instruments in both tax and criminal matters we refer to the Chapters 5 and 6 of the report on *Enhanced Exchange of Information in Financial Investigations* (University of Groningen, 2021).

establish and maintain strong international cooperation", as no single State can address cross-border issues, such as money laundering, tax fraud, and tax evasion, on its own.[21]

Since academic research by the *University of Groningen* has identified that FCInet can be used under the existing legal frameworks for information exchange, as the ma^{3}tch technology meets the conditions for *spontaneous* exchange of information[22], this study primarily focuses on the spontaneous exchange of information in relation to the concept of foreseeable relevance. It also takes legal challenges into account with respect to privacy and data protection. See below the explanation provided in the report on *Enhanced Exchange of Information in Financial Investigations* (University of Groningen 2021):

> *"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 standardizing 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 standardizing 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 (standardizing) personal data. As a consequence, data protection rules apply."*

A closer look at the report reveals that Chapter 2 explains how, in practical terms, the provision of information is carried out in the following steps: 1) selecting data, 2) standardising data, 3) processing data, 4) creating a filter, 5) sharing the filter and 6) using the filter in order to file a request for information about the suspect via the formal channels of mutual legal assistance. Another report, titled *The use of ma^{3}tch technology by JenV to carry out access and deletion requests* (Pels Rijcken and VKA 2023), describes four phases: the start-up, execution, verification and completion

21 FCInet 2022, *User Protocol*.

22 W. Geelhoed & R.A. Hoving, *Enhanced Exchange of Information in Financial Investigations*, Groningen: University of Groningen (2021), retrieved from: https://pure.rug.nl/ws/portalfiles/portal/193148668/Enhanced_Exchange_of_Information_in_Financial_Investigations.pdf (hereinafter: Geelhoed & Hoving 2021).

phase.[23] However, the start-up phase consists of selecting, standardising and processing the data, as well as creating the filter (refer to step 1 to 4 of the University of Groningen 2021 report), and the execution phase corresponds to sharing the filter (step 5). Finally, the verification and completion phase consist of the use of the filter, the validation of a hit and the submission of a request for information (step 6). Although formatted differently, both reports describe the same procedure. Depending on the level of detail in the description of the phases, several steps can be distinguished. In this study, we align with the four phases, as distinguished by *Pels Rijcken and VKA* in 2023, because the transition from the *execution* to the *verification phase* reflects the transition from spontaneous exchange, in which FCInet ma^{3}tch technology plays a role, to the regular exchange on request in an accessible manner.

Given the bilateral exchange of information under FCInet ma^{3}tch, the use of a multilateral assessment framework for the interpretation of the foreseeable relevance principle is not obvious. For example, there is a considerable difference in the way information is exchanged for the DAC and the way FCInet operates. The DAC mainly provides a mandatory *automatic exchange* of information between Member States. In some cases, the information needs to be exchanged with *all* Member States including those who are not involved in a particular activity, for example on the basis of DAC3 (exchange of *tax rulings: Advanced Pricing or Transfer Pricing agreements*), DAC6 (*Mandatory Disclosure* of potential aggressive tax planning structures) and DAC8 (reporting obligations on *crypto exchange*). With regard to information exchanged with all Member States, the European Commission developed and operates a *central database* in which the information collected and shared is recorded.[24] This exchange is carried out by electronic means through a secure platform based on the *Common Communication Network* (hereinafter: CCN).[25] This network has been developed for all electronic transmissions between the competent EU authorities in the field of taxation. The competent authorities of all Member States have access to the information in this database, based on a multilateral competent authority agreement. The information collected based on DAC2 (*Common Reporting Standard*), DAC4 (*Country by Country Reporting*), DAC5 (*Ultimate Beneficial Owner*), DAC7 (*Platform Sellers*) and DAC9 (reporting obligations *Pillar Two*) is not automatically shared with all Member States, but only with Member States concerned. In the latter cases, the information is exchanged *bilaterally*. Because the DAC is predominantly multilateral in nature, like the MAAC, while the application of the ma^{3}tch technology involves bilateral exchange, in this study we primarily focus on the application of *Article 26 OESO-MC for bilateral exchanges*. This does not alter the fact that experiences with other exchange instruments can also provide valuable insights for the interpretation of the foreseeable relevance standard.

23 Pels Rijcken and Verdonck Klooster & Associates (2023), *De inzet van Ma^{3}tch-technologie door JenV ter uitvoering van inzage- en verwijderingsverzoeken* (*authors' translation: The use of Ma^{3}tch technology by JenV to carry out access and deletion requests)*, retrieved from: https://realisatieibds.nl/file/download/fc3e7035-29e5-46df-b541-c8e78de65eef/20231003_rapport-ma3tch-use-case-def.pdf (hereinafter: Pels Rijcken & VKA Report 2023), Sec. 6.4.

24 Article 21 DAC.

25 Article 3(13) DAC. The CCN has been operational since 1999 and interfaces between IT systems of and between EU and European Economic Area-Member States. The CCN is developed and operated under the responsibility of the Commission, whereas the interfaces with the domestic tax systems are the responsibility of the Member States.

1.3 The standard of foreseeable relevance in tax information exchange

Article 26 OECD-MC provides guidance on relevant aspects of the exchange of information, including the duty to exchange, the mechanism by which information shall be exchanged and since 2005 the duty to protect information.[26] Article 26(1) of the OECD-MC sets out the basic obligation to exchange information as 'is foreseeably relevant' to the implementation of a tax treaty, the administration or enforcement of a State's domestic tax law or political subdivisions or local authorities (i.e. taxation). For bilateral tax treaties, the relevant actors in each State are the competent authorities. They are responsible for handling the exchange of information, which may also involve other actors, such as those involved in the investigation that give rise to the request, usually being someone in the tax administration. Since Article 26(2) of the OECD-MC allows a State to use information for *other than taxpayer-specific purposes* – if the information may generally be used for such purposes under the national laws of both States and the sending State authorises such use – the receiving State may share this information with other law enforcement authorities (hereinafter: LEAs), for example, in the area of money laundering and (tax) fraud. Article 26(3) of the OECD-MC contains some specific grounds for rejecting an information request, for example if granting a request would conflict with – the requested or requesting State's – domestic laws or can, for instance, be classified as a 'fishing expedition' (see Section 2.1.1).

An essential condition for the exchange of information is therefore that the information to be exchanged is foreseeably relevant. The *foreseeable relevance standard* should deter tax administrations from making unspecified bulk requests to other States and requesting information which is not relevant to the investigation in question. Since the historical evolution of Article 26 of the OECD-MC provides insight into the reasoning and legal context of the foreseeable relevance standard, we will discuss this in more detail in Chapter 2. Due to the lack of an unambiguous definition of foreseeable relevance in Article 26 itself, or the Commentary thereon, the interpretation of the concept by States involved in the exchange of information may differ, which could jeopardise the effective functioning of the tax information exchange system. We will see such differences between countries in Chapter 3. Furthermore, this study also discusses specific questions regarding the technical operation of FCInet ma^{3}tch for spontaneous information exchange (Chapter 4), such as: whether a distinction in interpretation should be made between foreseeable relevance in *spontaneous exchange* and the *exchange on request*, whether the ma^{3}tch filter represents *bulk data*, whether sharing the filter is considered a *fishing expedition*, whether the foreseeable relevance standard must be met at the time of the *spontaneous provision* of the filter or earlier, whether each *individual* in the filter must be mentioned by name, whether the fact that individuals in a filter are under *investigation* or *examination* constitutes relevance, whether the sharing of the filter can be considered as *foreseeable in itself*, and whether the presence of a 'hit' after checking the filter by the receiving State implies relevance. These and other questions regarding the application of FCInet ma^{3}tch, in the light of

26 Ring 2016, Sec. 1.1.1.

the foreseeable relevance concept and in relation to applicable data protection rules, are answered in the course of this research and summarised in Chapter 6.

Key takeaway:

Governments face a dual obligation in the exchange of tax information: to combat tax evasion effectively and to protect taxpayer privacy and data rights. This calls for a balanced approach. That is why FCInet and its ma³tch technology were introduced. The OECD and EU, among others, have created international standards to support global cooperation through information exchange, however this exchange needs to be privacy-conscious and can exclusively take place if the foreseeable relevance threshold is met.

1.4 The concept of relevance in cooperation regarding criminal matters

The exchange of tax information is not only important for administrative proceedings, but also for criminal proceedings, where the different procedures have their own rules.[27] An important difference, for instance, is that administrative sanctions are imposed by the tax authorities, while criminal sanctions are imposed by a judge, at the request of the public prosecutor. As the divide between administrative proceedings, such as tax investigations, and criminal proceedings increasingly fades – due to the possibility of evidence gathered in administrative proceedings to be admitted in criminal trials as well, and due to the oftentimes punitive nature of sanctions imposed in administrative proceedings – the way in which information and evidence are gathered in tax proceedings could have repercussions in matters of criminal law. To assess such repercussions, this study includes an interdisciplinary section consisting of an analysis of requirements applicable to the exchange of information in criminal proceedings, and in a comparison of those requirements with the foreseeable relevance standard established for the exchange of information in tax matters.

Unlike legal instruments in tax law, many instruments for cooperation in criminal matters exist (see Annex 2 for an overview). These may have different sources, e.g. UN, CoE, EU, or bilateral conventions as opposed to the multilateral treaties. While there are no multilateral treaties dealing specifically with the countering of tax fraud, cooperation in criminal matters to investigate tax fraud is based on generally applicable cooperation instruments. The criminal law analysis discusses these generally applicable cooperation instruments, in the context of cross-border tax fraud investigations, which often encompass provisions regulating the exchange of information with and without prior request. These instruments include the 1959 CoE MLA Convention[28]

27 F. Cannes, 'Tax Cooperation and Exchange of Information: The Issue of 'Circulation of Evidences', *Erasmus Law Review*, 2, 2022:125-135, retrieved from: https://www.boomportaal.nl/tijdschrift/ELR/ELR-D-22-00022 (hereinafter: Cannes 2022).

28 European Convention on Mutual Assistance in Criminal Matters (adopted 20/04/1959, entered into force 12/06/1962) 30 ETS 1 (hereinafter: 1959 MLA Convention).

and its Second additional protocol adopted in 2001[29], the 2000 EU MLA Convention[30], Directive 2014/41/EU on the European Investigation Order (hereinafter: EIO Directive)[31], Directive (EU) 2023/977 on the exchange of information between the LEAs of Member States (repealing Council Framework Decision 2006/960/JHA)[32], and the Europol Regulation (EU) 2016/794.[33] These legal instruments will be examined in Chapter 5. At this introductory stage it is important to note that these instruments do *not* use the *concept of foreseeable relevance*. However, they do include *other requirements* that can be compared to the principle of foreseeable relevance. This will be the point of reference for the assessment of the implications from a criminal law perspective of using the FCInet ma^{3}tch technology for the exchange of information.

1.5 Main research question

Article 26 of the OECD-MC provides a general framework for the bilateral international exchange of information, and does not impose any restrictions on the forms or ways in which such exchange takes place, for example by using *Privacy Enhancing Technologies* (hereinafter: PETs) like FCInet ma^{3}tch (see Section 1.8 for a definition). In view of the OECD Commentary on Article 26, there is no regulation restricting the methods of exchange of information[34]:

> *"These three forms of exchange (on request, automatic and spontaneous) may also be combined. It should also be stressed that the Article does not restrict the possibilities of exchanging information to these methods and that the Contracting State may use* ***other techniques*** *to obtain information which may be relevant to both Contracting States such as simultaneous examinations, tax examinations abroad and industry-wide exchange information (…)."*

Article 26 OECD-MC allows for the extension of the three most well-known methods of information exchange, i.e. spontaneous, automatic and upon request. The possibilities for exchanging information to achieve a proper taxation should be understood broadly.

29 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (adopted 08/11/2001, entered into force 01/02/2004) 182 ETS 1 (hereinafter: Second Additional Protocol to the 1959 MLA Convention).

30 Council Act establishing in accordance with Article 34 of the Treaty on EU, the Convention on Mutual Assistance in Criminal Matters between the Member States of the EU (29 May 2000) OJ C197/1.

31 Directive (EU) 2014/41 of the European Parliament and of the Council regarding the European Investigation Order in criminal matters (3 April 2014) OJ L130/1.

32 Directive (EU) 2023/977 of the European Parliament and of the Council on the exchange of information between the LEAs of Member States and repealing Council Framework Decision 2006/960/JHA (10 May 2023) OJ L134/1.

33 Regulation (EU) 2016/794 on the EU Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JH (11 May 2016) OJ L 135/53 as amended by Regulation (EU) 2021/1133 and by Regulation (EU) 2022/991.

34 See for instance OECD Commentary 2017, par. 9.1, p. 494.

The FCInet ma³tch technology enables competent authorities to comply with their international information exchange obligations to *assist peer organisations* in their investigation of criminal offences or tax fraud. It should be noted that the foreseeable relevance principle was already included in tax treaties when PETs didn't exist. Prior to the introduction of PETs, the only means an organisation had to qualify information as relevant for another jurisdiction, was a *clear and visible relation* to that specific jurisdiction in its own data. In today's world, technologies like FCInet ma³tch, when used under the appropriate legal basis, can conduct an information exchange process in a more efficient and privacy-friendly manner. However, since the publication of the report titled *Enhanced Exchange of Information in Financial Investigations* in 2021, some ambiguity has arisen regarding the interpretation of the principle of foreseeable relevance. Since this debate specifically affects the use of FCInet ma³tch, the FCInet Board decided that an independent study, into the foreseeable relevance principle in international exchange of information in relation to ma³tch, is necessary to gain insight. The research question to be answered in this study is:

> *"How should the principle of foreseeable relevance be interpreted in relation to the spontaneous exchange of information via FCInet ma³tch from a tax law perspective, what criteria do the competent authorities in jurisdictions (involved in the underlying study) distinguish to assess whether the principle has been met, how is this principle related to the right to privacy and the protection of taxpayers' personal data, and how does the concept of foreseeable relevance compare to requirements for information exchange in criminal proceedings?"*

This main question can be answered based on the following sub-questions: What is the reasoning and legal context behind the principle of foreseeable relevance from a tax law perspective, and how is this related to the right to privacy and the protection of personal tax data (Chapter 2, Legal interpretation)? What criteria do jurisdictions (involved in the study) apply to assess whether the principle of foreseeable relevance has been met in the case of bilateral exchange of information (Chapter 3, Comparative analyses)? Does the way in which FCInet ma³tch is applied, more specifically in the light of the right to privacy and data protection, have an impact on the assessment of whether the requirement of foreseeable relevance is met (Chapter 4, Technical assessment)? Considering that the principle of foreseeable relevance is not used in criminal matters, how does foreseeable relevance compare to information exchanges in criminal proceedings and what issues may this create from a criminal law perspective, given that information gathered by tax authorities often is admitted as evidence in criminal proceedings (Chapter 5, Criminal law perspective)? Chapter 6 brings the findings together and will elaborate on any legal challenges to consider (Summary and conclusion).

1.6 Method and accountability

This research concerns a *case study* on FCInet ma³tch technology, more specifically on its functioning within the legal context of the bilateral international exchange of tax information. It maps out the meaning of the requirement of foreseeable relevance in relation to the application of the technology, identifies differences in interpretation between countries involved in the research, and highlights some challenges in the protection of personal data. To address the main research question, desk research based on a literature review is carried out, including the examination of eleven countries' available information on foreseeable relevance, found in government documents, peer review documents, domestic legislation and scholarly literature.[35] The research methods used for the comparative country analyses (Chapter 3) and the technical assessment of the FCInet ma³tch technology in the light of data protection (Chapter 4) require further explanation.

Comparative country analyses

Comparative analyses in the context of this research consist of describing and explaining similarities and differences in the interpretation, and handling, of the foreseeable relevance standard in the context of international information exchange in tax matters. To assess the application of the foreseeable relevance principle across various jurisdictions, a comparative analysis of eleven countries is undertaken. The methodology encompassed three primary approaches. Initially, a comprehensive review of OECD peer review reports pertaining to spontaneous information exchange and exchange on request in each country is conducted. This review has focused on the evolution of the foreseeable relevance standard, particularly in the context of DTCs, where the principle is applied. In the country research the following components are examined: instruments governing the exchange of information, local differences in the application of instruments and the application of taxpayer rights and secrecy rules, like data protection rules. Taxpayer rights and secrecy refers to provisions of national law that ensure that information relating to a taxpayer remains confidential and is protected from unauthorised disclosure.[36] Following this examination, the findings are analysed and cross-country comparisons are conducted. Through this process, we gain insight into both the divergence and convergence between jurisdictions, thereby moving closer to a deeper understanding of the foreseeable relevance standard.

Technical assessment of the FCInet ma³tch technology in the light of data protection

For a reconstruction of the technical operation of FCInet ma³tch, we use the description in the previous reports: *Enhanced Exchange of Information in Financial Investigations* (University of Groningen 2021) and *The use of ma³tch technology by JenV to carry out access and deletion requests* (Pels Rijcken and VKA 2023).[37] In addition, we rely on the experiences we have gained during an introductory explanation of the technology

35 Among others with the help of the extensive country documentation of the *International Bureau of Fiscal Documentation* (hereinafter: IBFD) in Amsterdam, see https://www.ibfd.org/.

36 CIAT 2006, p. 20.

37 See Geelhoed & Hoving 2021 and Pels Rijcken & VKA Report 2023.

and a specific training organised by FCInet. During the introductory explanation we worked with the operation of FCInet ma³tch in a particular situation (technical training). During the more advanced training, we gained insight into the operation of the *FCInet network*. Although the operation of mat³ch is principally divided into three phases – autonomous, anonymous, analysis[38] – this study adopts a four-phase model for greater clarity in assessing the right to data protection, and identifying and addressing potential breaches: the *start-up*, *execution*, *verification* and *completion* phase.

The technical operation of FCInet ma³tch is subsequently assessed against the conditions for privacy and data protection as set out in the more universally applicable Article 17 of the *International Covenant on Civil and Political Rights* (hereinafter: ICCPR)[39], Article 8 of the *European Convention on Human Rights* (hereinafter: ECHR)[40] and the Articles 7 and 8 of the *Charter of the Fundamental Rights of the European Union* (hereinafter: Charter)[41], as a general framework (*technical assessment*). This framework has been chosen because international (model) agreements on the exchange of tax information do not always contain their own provision on the protection of personal data. Although tax treaties based on the OECD-MC do contain rules on the secrecy of tax information, the elaboration of these rules is often left to the national laws of the States themselves.

Article 8 of the Charter on data protection has been further elaborated in the *EU General Data Protection Regulation* (hereinafter: EU GDPR).[42] However, the EU GDPR does not apply if personal data is *anonymised*, as anonymous data does not qualify as personal data. In general, data can be considered anonymous when they cannot be

38 Autonomy is guaranteed because each information owner controls what data is included in the filter, how long the filter is valid, what the precision of the filter is, with which parties the filter is shared and - after a hit - whether, when and what personal data is exchanged. To ensure anonymity within ma³tch, individual dimensions and records are minimised and aggregated in such way that it seems impossible to trace or establish a link to individual personal records. Through analysis, received filters are integrated with local information. See U. Kroon, 'Ma³tch: Privacy AND Knowledge: "Dynamic Networked Collective Intelligence"', *IEEE International Conference on Big Data* (2013): 23-31 (hereinafter: Kroon 2013), p. 26.

39 Article 17 ICCPR (1967): "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks".

40 Article 8 ECHR (1970): "1. Everyone has the right to respect for his private and family life, his home and his correspondence, 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

41 Charter (2009): "Article 7 - Respect for private and family life: Everyone has the right to respect for his or her private and family life, home and communications; Article 8 - Protection of personal data: 1. Everyone has the right to the protection of personal data concerning him or her, 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified, 3. Compliance with these rules shall be subject to control by an independent authority".

42 For a complete overview see: https://gdpr.eu/article-1-subject-matter-and-objectives-overview/.

reversed to the original identifying data.[43] However, if the data – with the help of other input – can be traced back to the person in question, i.e. is re-*identifiable*, then it is not anonymous, but *pseudonymised* data. The EU GDPR does apply to pseudonymised data, because it qualifies as personal data.[44] Although ma³tch contains an aggregation of compressed non-reversible 'double hashed personal data' and this data cannot be traced back to the data in the local filter of the sending State directly (see Section 4.4.1), the receiving State is able to determine whether there is a 'hit' between the data in the shared filter and its own database, which can be validated by the sending State as belonging to a specific person upon request. Even though the FCInet ma³tch filter consists of hashed and irreversible data, if the person behind the data can be traced after validation of a hit (and is therefore identifiable), this data should be considered pseudonymised data in retrospect. The terms 'anonymised' and 'pseudonymised' are legal concepts, so it's important to keep in mind that their interpretation may vary from country to country. It is therefore also important to assume that personal data is provided when using the FCInet ma³tch technology (see section 4.4).[45]

1.7 Scope, aim and relevance

This study mainly focuses on the interpretation of the foreseeable relevance standard in relation to the use of FCInet ma³tch for bilateral exchange of tax relevant information between States. More specifically, the research focuses on the interpretation of the foreseeable relevance threshold during spontaneous exchange (by sharing the ma³tch filter in the execution phase), and as a possible consequence thereof the subsequent exchange on request (in the verification and completion phase). Administrative assistance for the purposes of *tax collection* falls outside the scope of this study, since this is dealt with in Article 27 of the OECD-MC as from the revision of Article 26 OECD-MC in 2005.

Although the foreseeable relevance standard may be applicable to the automatic exchange of information under circumstances, this form of exchange of information falls outside the scope of this study.[46] Automatic exchange of information can be defined as the mandatory exchange between contracting States of *predetermined tax*

43 Balboni & Macenaite 2013, p. 336-337 with reference to Recital 23 of the Draft EU GDPR (COM (2012) 0011-C7-0025/2012-2012/0011(COD)): "[t]his Regulation should not apply to anonymous data, meaning any data that cannot be related, directly or indirectly, alone or in combination with associated data, to a natural person or where establishing such a relation would require a disproportionate amount of time, expense, and effort, taking into account the state-of-the-art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed".

44 Article 4(5) EU GDPR defines pseudonymisation 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".

45 In this connection, see also the report of Geelhoed & Hoving 2021, University of Groningen.

46 See Huiskers-Stoop, Breuer & Nieuweboer 2022, p. 94, where the authors argue that the foreseeable relevance principle should also be considered applicable to the automatic exchange of information under certain circumstances.

information at *predetermined intervals*. Automatic exchanges are – due to the nature of the data to be exchanged (e.g. bank balances, tax rulings, tax avoidance structures) and the agreements made in advance by contracting States – not suitable for ongoing tax fraud investigations concerning a specific taxpayer or a specific group of taxpayers. It should therefore be noted that regular updating of the filter cannot be regarded as an automatic exchange of tax information. Making the filter available to a contracting State to check whether there is a 'hit' with a person in one's own database does not imply making tax information available. So automatic exchange of tax information is not yet an issue. Tax information is provided only after a request has been made by the receiving State to the sending State in the completion phase (see Section 4.3.2).

While multilateral instruments for the exchange of information are in principle not taken into account, developments in the interpretation of the concept of foreseeable relevance for DAC purposes (most recently in DAC7, see Section 2.2), and MAAC purposes (for instance Article 22(4) on the use for non-tax purposes, see Section 2.1), will be considered where this is of added value. These developments in interpretation may be relevant for the (further) bilateral provision of information on the basis of Article 26 OECD-MC. In addition, the *Court of Justice of the European Union* (hereinafter: CJEU) confirmed in the *Berlioz case* that the principle of foreseeable relevance under the DAC aligns with the concept used in Article 26 of the OECD-MC (a concept that is almost identical to the meaning of Article 4 MAAC and also Article 1 OECD-TIEA) by providing the following interpretation: "there must be a *reasonable possibility* that the requested information *will be relevant*".[47]

The comparative analyses in this study are restricted to the following eleven States, which may potentially participate in the FCInet ma^{3}tch network: *France, Germany, Italy, Spain, Canada, Colombia, Indonesia, Mexico, Nigeria, South Africa* and *The United States of America* (hereinafter: U.S.). For the selection of countries, primary consideration is given to the distinction between the EU and non-EU States. Within this distinction, both developed (such as Canada, France, Germany) and developing countries (such as Colombia, Mexico) are included. Additionally, to the extent possible, we considered characteristics such as a more progressive or conservative approach to adopting modern exchange methods. Although all selected countries are considered progressive in the sense that they show willingness to exchange information, there is a difference in the capacity to actually do so: for example, the U.S. has more resources available than Nigeria. The selection method is intended to ensure a comprehensive

47 Case 682/15, *Berlioz*, 16 May 2017, ECLI:EU:C:2017:373, at 67: "As a number of governments and the Commission argued, this concept of foreseeable relevance reflects that used in Article 26 of the OECD Model Tax Convention, both because of the similarity between the concepts used and given the reference to OECD conventions in the explanatory memorandum to the proposal for a Council Directive COM(2009) 29 final of 2 February 2009 on administrative cooperation in the field of taxation, which led to the adoption of Directive 2011/16. According to the Commentary on that article adopted by the OECD Council on 17 July 2012, Contracting States are not at liberty 'to engage in fishing expeditions', nor to request information that is unlikely to be relevant to the tax affairs of a given taxpayer. On the contrary, there must be a reasonable possibility that the requested information will be relevant". Article 5a DAC largely codifies this decision, including the decision in the joined cases 245/19 and 246/19, *État luxembourgeois v. B and Others*, 6 October 2020, ECLI:EU:C:2020:795, at 106-118.

representation of potentially participating organisations in the context of FCInet ma³tch.

For the assessment of whether the technical operation of FCInet ma³tch complies with the right to privacy and data protection, the study is limited to the safeguards provided by the provision of Article 17 ICCPR (from 1967), the general European provision of Article 8 ECHR (from 1970), Articles 7 and 8 of the Charter (from 2009) when specific Union law applies, and the further elaboration on the latter Article in the EU GDPR since its introduction in 2018. Several FCInet participants are EU Member States and as a result, EU law applies to them. Others are based outside the EU, so other data protection rules may apply. Given the cross-border scope of EU legislation with non-EU States and its interpretation in case law – whereby six (ECHR, Charter) or nine (EU GDPR) questions need to be answered, in order to assess whether there has been a breach of the right to privacy and data protection (see Section 4.4) and if so, whether there is a justification for this – this framework can be seen as a standard framework for assessing privacy and data protection rights.[48] Although the rights to respect for privacy and the protection of personal data are intended for *natural persons*, they can also be invoked by *legal entities* under certain circumstances.[49] However, for the purposes of this study, we assume that these rights only apply to natural persons.

The aim of the case study is to provide new insights into the functioning of FCInet's ma³tch in light of the applicable data protection rules and to contribute to the (academic) discussion on the interpretation of the principle of foreseeable relevance in (spontaneous) international information exchange in general and in the use of PETs, such as FCInet ma³tch, in particular. The functioning of such technologies is important for the effective international exchange of information, which in turn is essential to combat tax fraud, financial crime or other crimes that undermine societal stability.

1.8 Core concepts

The following concepts are central to this research:

PETs for the exchange of tax information

PETs can be considered as technologies that embody fundamental data protection principles, maximise data security, and simultaneously minimise unnecessary personal data collection and processing. These technologies include encrypted analytics, de-identification techniques, and secure multi-party computation. PETs can be divided into *hard and soft privacy* technologies. Soft technologies are used where it can be assumed that a third-party can be *trusted* for the processing of data. For example, an organisation that collects and stores data in the cloud. A soft privacy technology model is based on compliance, control and auditing. With hard technologies the assumption is that third parties cannot be trusted; the model is designated in such a way that the privacy cannot be violated. For example, by the use of a *Virtual Private*

48 Geelhoed & Hoving 2021, p. 25.

49 See Huiskers-Stoop, Breuer & Nieuweboer 2022, p. 97-98.

Network (hereinafter: VPN) for democratic elections. On the one hand, the FCInet ma³tch instrument can be considered a hard privacy technology, because there is essentially no direct third-party access to the data, nor direct third-country exchanges of tax information (only possible follow-up exchanges by the receiving State), and the filter does not contain any source data; it only allows another State to check via a secure peer-to-peer VPN network[50], whether a taxpayer is present in the filter. On the other hand, FCInet ma³tch also has characteristics of a soft privacy technology, since its design allows for human intervention during each step of the process, for example, the constructing and sharing of the filter. Since the personal data in the filter is aggregated compressed non-reversible and double hashed, a breach of the protection of personal data by this human intervention does not seem to be an issue, so that the characteristics of a hard privacy technology predominate.

The FCInet ma³tch technology

The FCInet decentralised network was initially designed by the *Ministry of Justice and Security* in the Netherlands for the use by the *Financial Intelligence Units* (hereinafter: FIUs) in the EU to create an information exchange network regarding financial investigations. It started with six countries working together to handle cases. There was no central 'supranational' party involved, such as an FIU or an EU agency, as this might discourage countries from joining for fear of losing their autonomy. Therefore, a decentralised approach where all countries remain in complete control of their data was chosen. The technology for privacy friendly matching and analysing is called ma³tch. This technology was also developed by the *Ministry of Justice and Security*. In 2016 the technology was further developed by the Dutch *Ministry of Finance*. FCInet and ma³tch are deeply intertwined, with the integration of the ma³tch technology facilitating the analysis function of the FCInet system. The ma³tch technology uses a sophisticated set of algorithms to generate a filter from local data sources, (autonomously) selected by the sending organisation. The filter is shared with one or more peer organisations, as (autonomously) selected by the sending organisation. The receiving organisation can check (anonymously) whether (selected) keys from its own database are present in the filter. With this technology it is possible to identify whether any information in the receiving participant's database, is most probably present in the sender's database as well, a so-called 'hit'.[51] After verification and validation (analysis) of the hit, a request for tax information can be made by (human intervention by) the receiving organisation. For the technical operation of FCInet ma³tch in the four phases of information exchange, we refer to Chapter 4.

50 Kroon 2021, p. 27-29 and 72.

51 Geelhoed & Hoving 2021, p. 10.

The interpretation of the foreseeable relevance standard

The interpretation of the standard of foreseeable relevance allows for a degree of discretion in its assessment. Within the context of this study, we will start from a working definition according to paragraph 5 of the OECD-MC Commentary on Article 26: "in order to comply with the principle of foreseeable relevance, there should be a reasonable possibility that information will prove to be relevant". It is expected that there will be a slight difference in interpretation of the principle between spontaneous exchange (by sharing the filter) and the exchange on request, after a hit, in the follow-up verification and validation phase. For a detailed discussion of the foreseeable relevance principle, we refer to Chapter 2.

Domestic rules on prior authorisation and/or prior notification

Under a few tax treaties – and also the MAAC and DAC (within EU exchanges) – States are permitted to use information for *purposes beyond taxation*, provided such use is allowed by the laws of both States and *authorised* by the competent authority of the sending State. If a receiving State is required to have *prior authorisation* of the source State for the use of information for purposes *other than taxation* or to transmit it *to third parties*, the condition of foreseeable relevance must be met at the time of obtaining this authorisation, which is earlier than the moment of the spontaneous exchange itself. Although the cases where this occurs are rare, it is nevertheless important to consider. For example, if the receiving State does not have separate tax and criminal domains, and exchanged information could (unintentionally) have a cross-domain effect. In addition, in a rare number of cases States are required by their national laws to inform its taxpayers before sending relevant (tax) information to a contracting State (i.e. *prior notification*). For the purposes of FCInet ma^{3}tch, the prior authorisation or prior notification obligation means that data used for ma^{3}tch must have a visible relationship with the jurisdiction of the receiving organisation prior to sharing the filter. See Chapters 2 and 3.

A framework for privacy and data protection

International (model) agreements on the exchange of tax information do not always contain a general provision on the protection of personal data. However, tax treaties based on the OECD-MC do contain rules on the secrecy of tax information, but the details regarding their interpretation are often left to the national policies of the States themselves. In the context of this study, the right to privacy and personal data protection is understood to mean the protection provided by Article 17 ICCPR, Article 8 ECHR and Articles 7 and 8 Charter. According to Article 17 ICCPR no one shall be subjected to 'arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation' and everyone has the 'right to the protection of the law against such interference or attacks'. In the light of Article 8 ECHR everyone has the right of 'respect for his private and family life'. Under Articles 7 and 8 of the Charter everyone has the right to respect for 'his

private and family life, home and communications and to protection of personal data'.[52] Article 7 of the Charter is the equivalent of Article 8 of the ECHR.[53] Article 8 of the Charter has no separate equivalent in the ECHR.[54] See Chapter 4 for an assessment of the FCInet ma^{3}tch technology in the light of data protection rules.

52 See Case 131/12, *Google Spain*, 13 May 2014, ECLI:EU:C:2014:317, at 69: "Article 7 of the Charter guarantees the right to respect for private life, whilst Article 8 of the Charter expressly proclaims the right to the protection of personal data. Article 8(2) and (3) specify that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, that everyone has the right of access to data which have been collected concerning him or her and the right to have the data rectified, and that compliance with these rules is to be subject to control by an independent authority. Those requirements are implemented inter alia by Articles 6, 7, 12, 14 and 28 of Directive 95/46".

53 Article 7(3) Charter and Article 52(3) Charter.

54 Article 8 Charter is based on Article 286 of the Treaty establishing the European Community and on Directive 95/46/EC of the European Parliament and of the Council of 25 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, EC Treaty (OJ L 281, 23 November 1995, p. 31) as well as on Article 8 ECHR and the Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* of 28 January 1981, ratified by all Member States and more like Armenia, Azerbaijan, Georgia, Iceland, Russian Federation and Ukraine. See Huiskers-Stoop, Breuer & Nieuweboer 2022, p. 91 and Commentaries on Article 8 Charter, OjEU, 14 December 2007, C 303/17.

Chapter 2

Reasoning and legal context of the foreseeable relevance standard

Spontaneous exchange of tax information can help to proactively enable States to detect and address potential tax evasion instead of having to launch a tax fraud investigation after criminal offences have been committed. However, in international exchange of information, the foreseeable relevance standard must be met in order to protect, among other elements, personal taxpayer data. This Chapter addresses the following question: *What is the reasoning and legal context behind the principle of foreseeable relevance from a tax law perspective and how is this principle related to the protection of personal data?*

The reasoning and legal context will be mapped based on indicators for the interpretation of the foreseeable relevance standard in the light of its historical context. Relevant questions are how the term 'foreseeably relevant' should be interpreted in the meaning of Article 26 OECD-MC, and when the foreseeable relevance threshold should be met when it comes to the spontaneous provision of the ma^{3}tch filter. Although the wording of Article 26 OECD-MC does not distinguish between spontaneous exchange of information and exchange on request, the relevance requirements imposed on spontaneous exchanges appear to be *less stringent* than on exchanges upon request. After a historical consideration of the principle of foreseeable relevance (Section 2.1), the interpretation of relevance for both exchanges on request (Section 2.2) and spontaneously is examined (Section 2.3). Subsequently, the relationship between the foreseeable relevance principle and the protection of personal data will be examined (Section 2.4).

2.1 Evolution of Article 26 OECD-MC

Although there is no clear definition, the original standard of foreseeable relevance is addressed in Article 26(1) of the OECD-MC. The interpretation has, however, changed over the years. Some guidance can be found in the Commentaries, the scope of taxes covered by the Convention and (domestic) application of secrecy rules and purposes of use of received information. Based on important amendments to Article 26 OECD-MC and/or the Commentaries thereon in 2005, 2010, 2014 and 2024, we will discuss the evolution of the concept below.

On 29 April 1998, the *OECD Council of Ministers* published the report *Harmful Tax Competition: An Emerging Global Issue*.[55] In this report the lack of an effective exchange of information is mentioned as one of the characteristics of harmful preferential tax regimes. As a result, the OECD insists on the need for an effective exchange of information between tax authorities. When, as a follow-up, the exchange provision of

55 OECD, *Harmful Tax Competition: An Emerging Global Issue*, Paris: OECD Publishing (1998), retrieved from: https://www.oecd.org/en/publications/harmful-tax-competition_9789264162945-en.html.

Article 26 of the OECD-MC was introduced in 1998, it consisted of two paragraphs:

1. *The competent authorities of the Contracting States shall exchange such information as **is necessary** for carrying out the provisions of this Convention or of the domestic laws of the Contracting States **concerning taxes covered by the Convention** insofar as the taxation thereunder is not contrary to the Convention. The exchange of information is **not restricted by Article 1**. Any information received by a Contracting State shall be treated as **secret** in the same manner as information obtained under the domestic laws of that State and shall be disclosed only to persons or authorities (including courts and administrative bodies) concerned with the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, **the taxes** covered by the Convention. Such persons or authorities shall use the information **only for such purposes**. They may disclose the information in **public court proceedings** or in **judicial decisions**.*
2. *In **no case** shall the provisions of paragraph 1 be construed so as to impose on a Contracting State the obligation:*
   a) *to carry out administrative measures **at variance** with the laws and administrative practice of that or of the other Contracting State;*
   b) *to supply information which is **not obtainable** under the laws or in the normal course of the administration of that or of the other Contracting State;*
   c) *to supply information which would disclose any trade, business, industrial, commercial or professional **secret or trade process**, or information, the disclosure of which would be contrary to public policy (ordre public).*

Article 26 OECD-MC embodies the rules under which information may be exchanged to the 'widest possible extent'.[56] Article 26(1) allows information to be exchanged spontaneously, on request and automatically.[57] The text makes it clear that the exchange of information is not restricted by Article 1 OECD-MC (Persons Covered), so that the information may include particulars about non-residents.

Scope of taxes

The taxes covered by the Convention are laid down in Article 2 and regard all taxes on income and capital, i.e. "All taxes imposed on total income, on total capital, or on elements of income or of capital, including taxes on gains from the alienation of movable or immovable property, taxes on the total of wages or salaries paid by enterprises, as well as taxes on capital appreciation". Information should be given

56 See OECD, *Model Tax Convention on Income and on Capital: Condensed Version 1998*, Paris: OECD Publishing (1998), retrieved from: https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-1998_mtc_cond-1998-en#page264, on Article 26: p. 260-266 (hereinafter: OECD Commentary 1998), Preliminary remarks.

57 OECD Commentary 1998, par. 9.

insofar as the national tax in question is covered by the Convention and the taxation under the domestic legislation concerned is not contrary to the Convention.[58]

Secrecy rules

Although reciprocal assistance between administrations is feasible only if each administration is assured that the other administration will treat with proper confidence the information which it will receive in the course of their cooperation, maintenance of such secrecy in the receiving State is a matter of domestic laws.[59] In general, secrecy – or the duty of confidentiality – can be understood to mean that information exchanged may only be used and disclosed in accordance with the legal basis on which the information was exchanged. Therefore, the exchange of information requires *confidence* between the States exchanging information.[60] Competent authorities also need the confidence of their citizens. Competent authorities can find themselves in a difficult situation if they have to balance the interests of other competent authorities to provide information and those of their citizens. For this reason, there are confidentiality requirements: the authorities may exchange information if that information is treated confidentially by the receiving authority. Tax secrecy, or the lack thereof, is therefore liable to limit the exchange of information. A State from which the information is requested can suspend assistance under Article 26 OECD-MC, if the receiving State does not comply with the confidentiality requirements.

Use for other than tax purposes

If information received appears to be of value to the receiving State for other than tax purposes covered by the Convention, the State may not use the information for such purposes, but must resort to means specially designed for those purpose (e.g. in case of a non-tax crime, to a treaty concerning judicial assistance).[61] Therefore, under Article 26 OECD-MC, information *may not be disclosed* to authorities not involved specifically in tax matters.[62] However, States may *agree to provide for disclosure* to supervisory bodies in their bilateral negotiations. Once information is used in *public court proceedings* or in *court decisions* and is therefore public, this information from the court decisions can be cited for other purposes, even as possible evidence.[63]

Limitations

Article 26(2) contains limitations to the main rule in favour of a requested State: (1) a contracting State is not bound to go beyond its own internal laws and administrative practice in putting information at the disposal of the other contracting State; (2) the contracting State does not need to go so far as to carry out administrative measures that are not permitted under the laws or practice of the requesting State or to supply information that is not obtainable under the laws or in the normal course of

58 OECD Commentary 1998, par. 5.

59 OECD Commentary 1998, par. 11.

60 Huiskers-Stoop, Breuer & Nieuweboer 2022, p. 65.

61 OECD Commentary 1998, par. 12.

62 OECD Commentary 1998, par. 12.1.

63 OECD Commentary 1998, par. 13.

administration of the requesting State (*principle of reciprocity*); and (3) the contracting State has a certain *discretion* to refuse requested information on the items listed in sub-paragraph c in order to protect the interests of its taxpayers.[64] In these cases a State may refuse to provide information.

2.1.1 Changes in 2005

Until 2005, it followed from Article 26 OECD-MC that information had to be exchanged if it was 'necessary' for the implementation of the Convention or domestic laws. However, since 2005, the term has been replaced by 'is foreseeably relevant'.[65] The aim of the revision is to ensure that Article 26 OECD-MC (re)aligns with international information exchange practices, including improved access to so-called banking information.[66] In addition, the application of the term 'necessary' could lead to discussion. The term foreseeably relevant would better reflect the intention of the principle, namely that information to be exchanged is foreseeably relevant *to the receiving State*.[67] The standard is intended to provide for exchange of information in tax matters to the *widest extent possible* and, at the same time, to clarify that contracting States are not at liberty to engage so-called 'fishing expeditions' or to request information that is unlikely to be relevant to the tax affairs of a given taxpayer.[68] A *fishing expedition* can be defined as a random or speculative request for especially incriminating information that has *no* apparent *nexus* to an examination or investigation.[69] Fishing expeditions refer, for example, to information requests that do *not identify* a specific taxpayer, but instead have a broader scope to find information about taxpayers who may be non-compliant with applicable tax laws or that do concern a specific taxpayer, but are addressed at a *very large number of countries*.

The revision of Article 26 in 2005 extended the Article to five paragraphs:

1. *The competent authorities of the Contracting States shall exchange such information as **is foreseeably relevant** for carrying out the provisions of this Convention or **to the administration or enforcement** of the domestic laws concerning **taxes of every kind** and description imposed on behalf of the Contracting States, or of their political subdivisions or local authorities, insofar as the taxation thereunder is not contrary to the Convention. The exchange of information is not restricted by Articles 1 **and 2**.*

64 OECD Commentary 1998, par. 14-19.

65 Some countries had already replaced the term 'necessary' with 'relevant' in their bilateral conventions, as this would better express the meaning of the provision, see OECD Commentary 1998, par. 5.

66 See Jeong 2013, p. 449.

67 See OECD, *Model Tax Convention on Income and on Capital: Condensed Version 2005*, Paris: OECD Publishing (2005), retrieved from: https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2005_mtc_cond-2005-en#page1, on Article 26: p. 313-327 (hereinafter: OECD Commentary 2005), par. 5.

68 Contracting States may agree to an alternative formulation of this standard that is consistent with the scope of the Article, e.g. by replacing 'necessary' or 'relevant' with 'foreseeably relevant', see OECD Commentary 2005, par. 5.

69 OECD Commentary 2005, par. 5.

2. *Any information received under paragraph 1 by a Contracting State shall be treated as secret in the same manner as information obtained under the domestic laws of that State and shall be disclosed only to persons or authorities (including courts and administrative bodies) concerned with the assessment or collection of, the enforcement or prosecution in respect of, the determination of appeals in relation to the taxes referred to in paragraph 1,* ***or the oversight of the above****. Such persons or authorities shall use the information only for such purposes. They may disclose the information in public court proceedings or in judicial decisions.*
3. *In no case shall the provisions of paragraphs 1 and 2 be construed so as to impose on a Contracting State the obligation:*
   a) *to carry out administrative measures at variance with the laws and administrative practice of that or of the other Contracting State;*
   b) *to supply information which is not obtainable under the laws or in the normal course of the administration of that or of the other Contracting State;*
   c) *to supply information which would disclose any trade, business, industrial, commercial or professional secret or trade process, or information the disclosure of which would be* ***contrary to public policy*** *(ordre public).*
4. *If information is requested by a Contracting State in accordance with this Article, the other Contracting State shall use its information gathering measures to obtain the requested information, even though that other State* ***may not need such information for its own tax purposes****. The obligation contained in the preceding sentence is subject to the limitations of paragraph 3 but in no case shall such limitations be construed to permit a Contracting State to decline to supply information solely because it has no domestic interest in such information.*
5. *In no case shall the provisions of paragraph 3 be construed to permit a Contracting State to decline to supply information solely because the information is held by a* ***bank****, other financial institution, nominee or person acting in an agency or a fiduciary capacity or because it relates to ownership interests in a person.*

Scope of taxes

In 2005, the scope of the taxes covered by the Convention was extended to 'taxes of every kind'. Thus, there is no longer any limitation of taxes covered by Article 2 of the Convention.[70] Despite this extension, *custom duties* are not covered by the Article, as their exchange has a legal basis in other international instruments.[71] Neither *Value Added Taxes* (hereinafter: VAT) or *inheritance tax* fall within the scope of the Convention. As a result, information collected in a custom duty investigation, a VAT

70 Since some Contracting States may not be in a position to exchange information, or use the information obtained from a treaty partner, in relation to taxes that are not covered by the Convention under the general rule of Article 2, such States are according to the Commentary free to restrict the scope to taxes covered by the Convention. See OECD Commentary 2005, par. 10.1.

71 OECD Commentary 2005, par. 5.2.

carrousel investigation or an inheritance investigation cannot be exchanged under a bilateral tax treaty based on Article 26 OECD-MC.

Secrecy rules

In addition, the Commentary makes it clear that the information to be exchanged, is not limited to taxpayer-specific information; the competent authorities may also exchange other *sensitive information* related to taxation and compliance improvement, for example risk analysis techniques or tax avoidance or evasion schemes.[72] Information provided shall be treated as secret in the receiving State in the same manner as information obtained under the domestic laws of that State.[73] Information received may 'not be disclosed to a third party', unless there is an express provision in the bilateral treaty allowing such disclosure.[74] However, contracting States that may wish to allow the sharing of tax information by tax authorities with other *LEAs* and *judicial authorities* on certain high priority matters, e.g. to combat money laundering, corruption, terrorism financing, may add the following *optional* text[75]:

> *"Notwithstanding the foregoing, information received by a Contracting State may be used* ***for other purposes*** *when such information may be used for such other purposes under the laws of both States and the competent authority of the Supplying State* ***authorizes*** *such use."*

At the national level, States may provide for *exceptions* to the tax secrecy. These exceptions can be made based on *national legislation*, making it possible to send information to non-tax authorities, such as other supervisory bodies. Since 2005, information may be disclosed also to 'oversight bodies', like authorities that *supervise* tax administration and enforcement authorities as part of the general administration of the government of the contracting State.[76] Thus, the data collected by the tax authorities and exchanged with other (European) tax authorities should, in principle, only be used for the administration and enforcement of the tax law, but some of the international agreements on the exchange of information (including MAAC and DAC) allow the information exchanged to be used for *non-tax purposes* or to be disclosed *to third parties*.[77] For example, sending States may stipulate that information must not be disclosed to authorities outside the scope of tax matters, whereas receiving States may allow for transmission to other authorities through provisions in their *bilateral treaties*. However, taxpayers whose tax information is exchanged should be able to rely on the fact that non-tax use, or transmission to other States, has a *legal basis* and that a *balance of interests* has taken place, showing that a further dissemination is significant enough to justify an *exception to the main secrecy rule* of no further disclosure than is

72 OECD Commentary 2005, par. 5.1.

73 OECD Commentary 2005, par. 11.

74 OECD Commentary 2005, par. 12.2.

75 OECD Commentary 2005, par. 12.3. When Article 26 was amended in 2010, this optional provision was included in OECD-MC itself.

76 OECD Commentary 2005, par. 12.1.

77 Huiskers-Stoop, Breuer & Nieuweboer 2022, p. 87 and Article 16(2) and (3) DAC.

necessary for the enforcement of taxation.[78] It is the receiving State, which becomes a sending State, that bears the responsibility for this.

Exchange techniques and timelines

Furthermore, since the way the exchange of information will be affected can be decided upon the competent authorities, contracting States may wish to use appropriate security systems, like PETs, to improve the timelines and quality of exchanges of information. Contracting States which are required to observe data protection laws, may according to the Commentary wish to include provisions in their bilateral conventions concerning the *protection of personal data* exchanged.[79]

Limitations

Although a State may refuse to provide information where the requesting State would be precluded by law from obtaining or providing the information or where the requesting State's administrative practices result in a lack of reciprocity, it is recognised that too rigorous an application of the *principle of reciprocity* could frustrate effective exchange of information and that reciprocity should be interpreted in a broad, pragmatic manner.[80] In addition, States must use their domestic information gathering measures, like laws and administrative or judicial procedures, even though *invoked solely* to provide information to the other State; a State cannot argue that under its domestic laws or practices it only supplies information in which it has an interest for its *own tax purpose*.[81] In most cases of information exchange, no issue of trade, business or other secret will arise.[82] Issues of public policy – a limitation with regard to information which concerns the vital interest of the State itself[83] – rarely arise in the context of information exchange between treaty partners.[84] Finally, Article 26(5) stipulates that a contracting State shall not refuse to supply information to a treaty partner solely because the information is held, inter alia, by a *bank* or other *financial institution*.[85]

Concluding statement

So between 1998 and 2005 the nature of the concept developed from 'necessary' to 'foreseeably relevant' to align with relevant developments in international exchange of information, which include, among others, the introduction of the ideal standard

78 Huiskers-Stoop, Breuer & Nieuweboer 2022, p. 87.

79 OECD Commentary 2005, par. 10: "Data protection concerns the rights and fundamental freedoms of an individual, and in particular, the right to privacy, with regard to *automatic* processing of personal data".

80 OECD Commentary 2005, par. 15.

81 OECD Commentary 2005, par. 19.6-19.9: some "countries may wish to clarify expressly in the convention that Contracting States must ensure that their competent authorities have the necessary powers to do so".

82 OECD Commentary 2005, par. 19.2: "A trade or business secret is generally understood to mean facts and circumstances that are of considerable economic importance and that can be exploited practically and the unauthorized use of which may lead to serious damage (e.g. may lead to severe financial hardship)".

83 CIAT 2006, p. 21.

84 OECD Commentary 2005, par. 19.5.

85 OECD Commentary 2005, par. 19.11.

of access to information mentioned in the *Improving Access to Bank Information for Tax Purposes* in 2000 and the OECD-TIEA (bilateral and multilateral version) in 2002.[86] The 2000 standard was drawn up by the *Committee on Fiscal Affairs* and aims to examine how international cooperation for tax purposes can be improved with regard to the exchange of information held by banks and other financial institutions. The 2002 agreement consists of two models of bilateral agreements, drawn up in the light of agreements between the OECD and relevant jurisdictions, which mark the first results of international cooperation to improve transparency and effective exchange of information in tax matters. The insertion of the words 'to the administration or enforcement' was made to achieve consistency with this agreement and was not intended to alter the effect of the provision.[87] Most OECD countries have followed the change in terminology, but some have taken a different approach (see Chapter 3).[88] Despite the intention of the OECD to provide clarity, the term foreseeable relevance still leaves room for interpretation. The key is the interpretation of the term *foreseeable*.

2.1.2 Changes in 2010

Article 26(2) OECD-MC was amended in 2010 to allow the competent authorities to use information received for *other than tax purposes*, provided such use is allowed under the laws of both States and the competent authority of the sending State authorises such use[89]:

1. *Any information received under paragraph 1 by a Contracting State shall be treated as secret in the same manner as information obtained under the domestic laws of that State and shall be disclosed only to persons or authorities (including courts and administrative bodies) concerned with the assessment or collection of, the enforcement or prosecution in respect of, the determination of appeals in relation to the taxes referred to in paragraph 1, or the oversight of the above. Such persons or authorities shall use the*

86 The report on *Improving Access to Bank Information for Tax Purposes* (2000) was prepared to consider ways to improve international cooperation with respect to the exchange of information in the possession of banks and other financial institutions for tax purposes, see https://www.oecd.org/en/publications/improving-access-to-bank-information-for-tax-purposes_9789264181267-en.html. See also E. Fort and A, Rust, *Exchange of Information and Bank Secrecy*, Alphen aan den Rijn: Kluwer Law International (2012) (hereinafter: Fort & Rust 2012).

87 See OECD Commentary 2005, par. 4.1.

88 See OECD, *Model Tax Convention on Income and on Capital: Condensed Version 2014*, Paris: OECD Publishing (2014), retrieved from: https://www.oecd.org/en/publications/model-tax-convention-on-income-and-on-capital-condensed-version-2014_mtc_cond-2014-en.html, on Article 26: p. 414-433 (hereinafter: OECD Commentary 2014), par. 5.3: "Contracting States may agree to an alternative formulation of the standard of foreseeable relevance that is consistent with the scope of the Article and is therefore understood to require an effective exchange of information (e.g. by replacing, 'is foreseeably relevant' with 'is necessary', 'is relevant' or 'may be relevant')".

89 See OECD, *Model Tax Convention on Income and on Capital: Condensed Version 2010*, Paris: OECD Publishing (2010), retrieved from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2010/08/model-tax-convention-on-income-and-on-capital-condensed-version-2010_g1g10b68/mtc_cond-2010-en.pdf, on Article 26: p. 397-410 (hereinafter: OECD Commentary 2010). In the OECD Commentary 2005, this provision was optional, par. 12.3.

information only for such purposes. They may disclose the information in public court proceedings or in judicial decisions. ***Notwithstanding the foregoing, information received by a Contracting State may be used for other purposes when such information may be used for other purposes under the laws of both States and the competent authority of the supplying State authorises such use.***

Use for other than tax purposes

Information provided to a competent authority should in principle only be used for tax purposes in the receiving State and not for other purposes. The receiving competent authority is generally bound by secrecy, however, the domestic (legal) interpretation of the secrecy requirement is often left to the receiving State, meaning that the interpretation may vary locally. Therefore, under circumstances, information received may be used also for *non-tax purposes*. The use for non-tax purposes may include, but is not limited to, sharing of tax information by tax authorities with other LEAs and judicial authorities on *certain high priority matters*, such as a suspicion of tax fraud related to money laundering, corruption or terrorism financing.[90] For example, in Italy the *Guardia di Finanza* acts as both a tax authority and a criminal investigative body (see Section 3.1.2 and Annex 1.1.3). This means that tax information received may immediately be used for criminal purposes, such as in cases involving money laundering or corruption. In such systems, the line between tax and non-tax use is less clear.

Similar development in the MAAC (2010)

Article 22 of the MAAC gives substance to the principle of secrecy. In principle, all information obtained by a receiving State shall be treated as secret. However, paragraph 4 of this Article does allow the information to be used for other purposes or transmission to third parties:

> *"Notwithstanding the provisions of paragraphs 1, 2 and 3, information received by a Party may be used* ***for other purposes*** *when such information may be used for such other purposes under the laws of the supplying Party and the competent authority of that Party* ***authorises*** *such use. Information provided by a Party to another Party may be transmitted by the latter* ***to a third Party,*** *subject to* ***prior authorisation*** *by the competent authority of the first-mentioned Party."*

According to the Explanatory Report to the MAAC as amended by the 2010 Protocol (ETS No. 127), there may be situations in which two States agree that the principle of confidentiality undesirably limits the scope of mutual legal assistance. Paragraph 4 therefore makes it possible for the information received by a State to be used for other purposes when such information may be used (1) for such purposes under de laws of

90 See OECD Commentary 2010, par. 12.3. See for a broad scope for exchange of information CIAT (2006), *Manual for implementing and carrying out Information exchange for tax purposes. General and legal aspects of information exchange*, retrieved from: https://www.ciat.org/Biblioteca/DocumentosTecnicos/Ingles/2006_CIAT_manual_information_exchange.pdf, p. 29.

the sending State and (2) the competent authority of that State authorises such use. In this context, the Explanatory Report explicitly cites the *1959 European Convention on Mutual Assistance in Criminal Matters*, ETS No. 30 (i.e. the 1959 CoE MLA Convention, see Section 1.4 and Chapter 5) as an example of an instrument specifically designed for such other purposes. The explanation also refers to situations where information obtained from one State may be of interest to a third State. To prevent the third State from obtaining information which it could not have obtained directly, paragraph 4 provides that the transmission of information from the second to the third State is subject to *prior authorisation* of the State which originally supplied the information.

2.1.3 Changes in 2014

Although the wording of Article 26 was not changed in 2014, the Commentary provided further clarification about the concept of foreseeable relevance. In the context of information exchange *upon request*, the standard requires that at the time a request is made there is a 'reasonable possibility' that the requested information *will be relevant*; whether the information, once provided, actually *proves to be relevant* is immaterial.[91] A request may therefore not be refused in cases where the assessment of the relevance of the information to an ongoing investigation can only be made after receipt of the information. The competent authorities should consult in situations in which the content of the request, the circumstances that led to the request, or the foreseeable relevance of requested information are not clear to the requested State. However, once the requesting State has provided an explanation as to the foreseeable relevance of the requested information, the requested State may not decline a request or withhold requested information because it believes that the information lacks relevance to the underlying investigation or examination. Where the requested State becomes aware of facts that call into question whether part of the information requested is foreseeably relevant, the competent authorities should consult, and the requested State may ask the requesting State to clarify foreseeable relevance in the light of those facts.

Identifiable taxpayers

A request for information does not constitute a fishing expedition solely because it does *not* provide the *name or address* (or both) of the taxpayer under examination or investigation.[92] The same holds true where names are spelt differently or information on names and addresses is presented using a different format. However, in cases in which the requesting State does not provide the name or address (or both) of the taxpayer under examination or investigation, the requesting State must include other information sufficient to identify the taxpayer.

Group of taxpayers

Having regard the OECD Commentary 2014 the interpretation of the concept was broadened in the sense that the standard of foreseeable relevance can be met both in cases involving a 'single taxpayer' (named or unnamed) or 'several taxpayers' (whether

91 See OECD Commentary 2014, par. 5.

92 OECD Commentary 2014, par. 5.1.

or not named or unnamed).[93] Where a contracting State undertakes an investigation into a particular group of taxpayers in accordance with its laws, any request related to the investigation will typically serve 'the administration or enforcement of its domestic tax laws' and thus comply with the requirements of paragraph 1, provided it meets the standard of foreseeable relevance. However, where the request relates to a group of taxpayers *not individually identified*, it will often be more difficult to establish that the request is not a fishing expedition, as the requesting State cannot point to an ongoing *investigation into the affairs of a particular taxpayer*, which in most cases would by itself dispel the notion of the request being random or speculative. In such cases it is therefore necessary that the requesting State provides a *description of the group* and the *specific facts and circumstances* that have led to the request, an explanation of the applicable law and why there is reason to believe that the taxpayers in the group for whom information is requested, have been non-compliant with that law supported by a clear factual basis. This change to a *group* of persons has made the foreseeable relevance requirement a little more flexible.

When applying FCInet ma^{3}tch, the hashed data of a group of taxpayers is made available by means of the filter. In the case of a spontaneous exchange involving a group of taxpayers, a *minimum link* for foreseeable relevance must be met for each taxpayer in relation to a particular receiving State. A specific investigation or examination of a person generally assumes a *minimum of relevance*, as it implies a reasonable suspicion of non-compliance with a specific legal obligation in the source State, which may be indicative of any relevance for taxation in the receiving State.[94] In the application of FCInet ma^{3}tch, it is up to the State that spontaneously makes the filter available to assess whether the data in the filter – relating to persons in a particular investigation – may have any relevance for taxation in the receiving country. It is not necessary that the name of each person in question is shared, which allows the use of *hashed names* to protect personal data. To meet the link, the persons in the filter must, however, be 'identifiable'. This means that the information provided is sufficient to identify a person. With FCInet ma^{3}tch, hashed data is made available in the filter, but after a *validated hit*, that data must be classified as *pseudonymised*, and therefore as personal data, because the person behind has become identified (see Section 4.4.1). After a validated hit, the receiving State can make an additional request for information for a single taxpayer and not for the group as a whole. In the exceptional case that information is requested about all taxpayers in the filter, the foreseeable relevance requirement must be met with regard to each taxpayer. For the purposes of this study, we will consider the spontaneous exchange of information about groups, since the data in a filter is always based on a group of taxpayers (or a certain theme). We do not include group requests in the follow-up information exchange on request (from the verification phase onwards), as this exchange is in principle outside the scope of the FCInet ma^{3}tch technology, and we limit ourselves to verification requests about *specific taxpayers* after a hit.

93 OECD Commentary 2014, par. 5.2.

94 See OECD Commentary 2014, par. 5.2 and Case 437/19, *État du Grand-Duché de Luxembourg*, 25 November 2021, ECLI:EU:C:2021:953, at 72 for the mirror-image situation when providing information on request. Although the forms of exchange are not the same, the Commentary and the court judgement provide clues that an ongoing investigation is generally accepted as a minimal link for relevance.

Use for other than tax purposes

When a receiving State desires to use the information for an additional purpose (i.e. non-tax purpose), according to the OECD Commentary 2014 the receiving State should specify to the sending State the other purpose for which it wishes to use the information and 'confirm' that the receiving State can use the information for such other purpose under its laws.[95] Where the sending State is in a position to do so, having regard to, among others, international agreements or other arrangements between the contracting States relating to mutual assistance between other LEAs and judicial authorities, the competent authority of the sending State would generally be expected to 'authorise such use for other purposes' if the information can be used for similar purposes in the sending State. As from 2014 contracting States may replace the last sentence of paragraph 2 with the following *optional* text[96]:

> *"The competent authority of the Contracting State that receives information under the provisions of this Article may, with the **written consent** of the Contracting State that provided the information, also make available that information to be used **for other purposes** allowed under the provisions of a mutual legal assistance treaty in force between the Contracting States that allows for the exchange of tax information."*

Exchange techniques and timelines

The Commentary further provides for an optional default standard of time limits within which the information is required unless a different agreement has been made by the competent authorities.[97] Contracting States that deem it desirable to ensure the speed and timelines of the exchange of information may either include optional paragraph 6 to Article 26, which sets out default standard time limits, or come to different agreements (on a *case-by-case basis*).

Key takeaway:

For the purposes of FCInet ma³tch a specific investigation or examination of a person generally assumes a minimum of relevance, as it implies a reasonable suspicion of non-compliance with a specific legal obligation in the source State, which may be indicative of any relevance for taxation in the receiving State.

---

95 OECD Commentary 2014, par. 12.3.

96 OECD Commentary 2014, par. 12.4.

97 OECD Commentary 2014, par. 10.4: "The default standard time limits are two months from the receipt of the information request if the requested information is already in the possession of the tax authorities of the requested Contracting State and six months in all other cases".

2.1.4 Changes in 2024

An update of the Commentary on Article 26 of the OECD-MC was published in 2024, in particular with respect to 'confidentiality rules' and the 'disclosure of obtained information to the taxpayer'.[98] Confidentiality rules also apply to "reflective non-taxpayer specific information, i.e. information about or generated on the basis of the information that was received by a contracting State through the exchange of information such as, statistical data, as well as non-taxpayer specific notes, summaries, and memoranda incorporating exchanged information".[99]

Notwithstanding the confidentiality rules, the update to the Commentary states that "non-taxpayer specific information may be disclosed to third parties if the information does not, directly or indirectly, reveal the identity of one or more taxpayers and the sending and the receiving States have consulted with each other and it is concluded that the disclosure and use of such information would not impair tax administration in either the sending or the receiving State".[100] According to paragraph 11 of this Commentary update, the requirement that the receiving State obtains authorisation from the sending State for the disclosure of non-taxpayer specific information to third parties has been reduced to a *consultation* between these States, with the intention being to draw up a written record of this consultation and its outcome.

In addition, the update leaves the requirement of secrecy in the receiving State to the domestic laws of such State, and only in cases where, for example, a requested State determines that the receiving State does not comply with its duties regarding confidentiality, the requested State may suspend assistance under this Article. However, this assessment by the requested State will be made *a posteriori*, after the information may have been exchanged and used by the receiving State.

Furthermore, the information obtained may be communicated to a taxpayer to the extent that such information "has a bearing on the outcome of a tax matter concerning that particular taxpayer" (i.e. person concerned). Moreover, the update states that "such use is not limited to the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to the taxes referred to in paragraph 1 in respect of the person or persons for which the information was received, but also includes the use for such [read: tax] purposes in respect of any other person. The receiving Contracting State is not required to inform or to request authorisation from the sending Contracting State regarding such use".[101] Therefore, this update will make the exchange of information more efficient, as the sending State

98 See OECD (2024), *Update on the commentary on Article 26 of the OECD Model Tax Convention*, Paris: OECD Publishing, retrieved from: https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-transparency-and-international-co-operation/update-commentary-article-26-oecd-model-tax-convention.pdf, p. 1-3 (hereinafter: OECD Commentary 2024).

99 OECD Commentary 2024, par. 11.

100 OECD Commentary 2024, par. 11.

101 OECD Commentary 2024, par. 12.

does no longer have to inform the taxpayer prior to the exchange of information and the receiving State does not need to obtain prior authorisation for the use of the information for *taxpayer(s) other than those for whom the information was received* (except for information covered by paragraph 1 which may not be disclosed to persons or authorities not mentioned in paragraph 2).

The above-mentioned update makes the exchange of information more swift and efficient, as it not only extends to *non-taxpayer information* and the use of information *for other taxpayers*, but also provides for *consultation among tax authorities*, thereby reducing the requirement for prior authorisation by the sending State regarding the use of exchanged information. In practice, a reduction will be particularly noticeable in cases where the sending State issues a so-called 'whitelist' of cases in which prior authorisation for the use of exchanged data no longer needs to be obtained, for example in high-priority cases. The implementation of DAC7 in 2021 (*Platform Sellers*) provides starting points for the use of such a list. DAC7 has made it possible for EU Member States to publish a whitelist of 'other purposes' for which, in accordance with their national law, information and documents may be used without prior authorisation. The last two sentences of paragraph 2 of Article 16 DAC were amended:

> "*The competent authority of each Member State may communicate to the competent authorities of all other Member States a* ***list of purposes*** *for which, in accordance with its national law, information and documents may be used, other than those referred to in paragraph 1. The competent authority that receives information and documents may use the received information and documents* ***without the permission*** *referred to in the first subparagraph of this paragraph for any of the purposes listed by the communicating Member State*".

In our view, these changes to the Commentary on Article 26 OECD-MC enhance the use of exchange of information (taxpayer and non-taxpayer information) among tax authorities and the disclosure to third parties, by taking away, in certain cases, some requirements for States involved, such as *prior authorisation* regarding the use of information or *prior notification* of the taxpayer. The possibility to have consultations among both States as well as leaving the tax secrecy to the domestic rules of the receiving State, shows that the OECD also wants to enhance tax cooperation and exchange of information based on mutual trust among contracting States. Using a whitelist may contribute to this.

Concluding statement

Despite an increase in the number of information exchanges, in the amount of information to be exchanged and in the use of data exchanged for non-tax purposes, since 2010 only the Commentary on Article 26 OECD-MC has been changed, not the wording itself. However, the 2024 update to the Commentary also shows that the OECD aims to have a more swift and efficient exchange of information among States, as well as to facilitate the use of the information exchanged by competent authorities and by third parties, without the requirement of prior authorisation from or notification by the sending State, by using for instance a so-called whitelist.

Key takeaway:

The foreseeable relevance standard is a flexible legal standard requiring that information must be potentially useful to the receiving State's tax enforcement. Its wording has changed over time, but its interpretation has remained constant over time. The ma³tch filter must meet this standard at the point of sharing, or earlier if for instance prior authorisation is legally required. The use of a whitelist by the sending State could give substance to the latter.

2.2 Exchange of information on request

We take a closer look at the role of the foreseeable relevance standard in the exchange of information on request. In case of information exchange on request, the competent authority of the requesting State makes a request to the competent authority of the requested State, who will then work through its internal procedures to confirm the information request to be appropriate under the treaty, secure the requested information and transmit it to the competent authority of the requesting State.[102] Although the intention of Article 26 OECD-MC is to exchange information to the *widest extent possible*, it follows from paragraph 5 of the OECD Commentary that States are not at liberty to carry out fishing expeditions, nor to request information that is unlikely to be relevant to the tax affairs of a given taxpayer[103]:

> *"In the context of information exchange upon request, the standard requires that **at the time a request** is made there is a **reasonable possibility** that the requested information **will be relevant**; whether the information, once provided, actually proves to be relevant is immaterial."*

The requirement of foreseeable relevance of requested information is a *prerequisite* for the lawfulness of the information to be provided by the requested State and for the use of that information by the requesting State.[104] To protect the taxpayer's personal data, fishing expeditions must be prevented.

102 For a distinction between three phases of information exchange on request, see W. Boei and J. van Dam, 'Legal Protection in the Context of International Exchange of Information upon Request between Tax Authorities', *Erasmus Law Review,* 2, 2022:76-85, retrieved from: https://www.erasmuslawreview.nl/tijdschrift/ELR/2022/2/ELR-D-22-00033 (hereinafter: Boei & Van Dam 2022).

103 OECD Commentary 2017, par. 5.

104 Case 682/15, *Berlioz*, 16 May 2017, ECLI:EU:C:2017:373, at 74: "that Article 1(1) and Article 5 of Directive 2011/16 must be interpreted as meaning that the 'foreseeable relevance' of the information requested by one Member State from another Member State is a condition which the request for information must satisfy in order for the requested Member State to be required to comply with that request, and thus a condition of the legality of the information order addressed by that Member State to a relevant person and of the penalty imposed on that person for failure to comply with that information order".

Foreseeable relevance in tax information exchange on request

Although the term foreseeable relevance must be interpreted broadly, this does not mean that information can be requested without *nexus*. Thus, the requesting State cannot ask for 'anything and everything', there should be *some degree of knowledge* about taxpayers, persons or activities.[105] According to the OECD, the requesting State must provide sufficient information to *identify* the relevant taxpayer(s).[106] This restriction does not mean that a request must immediately identify a specific taxpayer, therefore, it is not necessary that the taxpayer is always referred to by name.[107] The request must be *individualisable* and *sufficiently specific*. A *specific examination or investigation* is generally accepted as proof that a request is neither random nor speculative.[108] It is sufficient for the requesting State to *substantiate* clearly and sufficiently that it is conducting an examination or investigation into a person (or a limited group of persons) on the basis of *well-founded suspicions*.[109] In the absence of a *link* between the information requested on a person and an examination or investigation in the requesting State, the foreseeable relevance standard is not met. In principle, it is the requesting State that oversees the examination or investigation giving rise to the request, in order to assess the foreseeable relevance.

In the application of FCInet ma^{3}tch, the presence of a hit is sufficient for the receiving State to meet the foreseeable relevance requirement for the validation request (see verification phase, Section 4.3.1). The subsequent validation of the hit by the sending State confirms the *actual* link, but that is not a requirement for the application of the foreseeable relevance principle. In this respect, the requesting State has some *discretion*, assuming that there is at least a nexus with the examination or investigation. However, it is for the requested State to verify that the information requested is of some foreseeable relevance to the investigation carried out.[110] In addition, the foreseeable relevance standard must be met at the time the *request for validation* is made. As

105 Ring 2016, Sec. 2.1.3.

106 OECD Commentary 2017, par. 5.1 and 5.2.

107 Case 437/19, *État du Grand-Duché de Luxembourg*, 25 November 2021, ECLI:EU:C:2021:953, at 51: "(…) it should be noted that the term 'identity' designates, in accordance with its everyday meaning, all the characteristics enabling a person to be individually distinguished, without being limited to identifying that person individually by his or her name (…)".

108 Ring 2016, Sec. 2.1.4.

109 Case 437/19, *État du Grand-Duché de Luxembourg*, 25 November 2021, ECLI:EU:C:2021:953, at 72: "(…) that a request for information must be regarded as relating to information which does not appear to be manifestly devoid of any foreseeable relevance, where the persons under examination or investigation within the meaning of that latter provision are not identified individually and by name by that request but the requesting authority provides a clear and sufficient explanation that it is conducting a targeted investigation into a limited group of persons, justified by reasonable suspicions of non-compliance with a specific legal obligation".

110 Case 682/15, *Berlioz*, 16 May 2017, ECLI:EU:C:2017:373, at 82: "The review to be carried out by the requested authority is not limited, therefore, to a brief and formal verification of the regularity of the request for information in the light of those matters, but must also enable that authority to satisfy itself that the information sought is not devoid of any foreseeable relevance having regard to the identity of the taxpayer concerned and that of any third party asked to provide the information, and to the requirements of the tax investigation concerned."

mentioned, in a rare number of States the competent authorities, based on national laws, are required to *inform their residents* of an imminent request for information exchange (*prior notification*).[111] In those cases, the competent authorities will have to demonstrate *at the time of informing* that the foreseeable relevance standard has been met, which is earlier than the moment of the request itself.

Furthermore, States involved in the exchange of information may be subject to *additional restrictions* based on domestic legislation. For example, information does not have to be provided if, it would put *public order* or other essential interests under pressure, or the information could *not be obtained* based on the national laws of the requesting State, or *national possibilities* to obtain the requested information have not been (fully) exhausted, et cetera.

More precise definition in DAC7

The implementation of DAC7 in 2021 provides further insights for the interpretation of the foreseeable relevance principle. It is important to note that the design of the EU DAC is based on Article 26 of the OECD-MC.[112] Article 1(1) DAC describes that Member States shall cooperate with each other with a view to exchanging information that is foreseeably relevant to the administration and enforcement of the domestic laws of the Member States. The exchange of information on request is provided for in Article 5 DAC, which specifically refers to Article 1(1) DAC (subject matter), so that the standard for foreseeable relevance also applies here:

> *"This Directive lays down the rules and procedures under which the Member States shall cooperate with each other with a view to exchanging information that is **foreseeably relevant** to the administration and enforcement of the domestic laws of the Member States concerning the taxes referred to in Article 2."*

To ensure the effectiveness of the exchanges of information and to prevent unjustified refusals of requests, as well as to provide legal certainty for both tax administrations and taxpayers, the internationally agreed standard of foreseeable relevance should, according to recital 3 of DAC7, be clearly *delineated* and *codified*.[113] In DAC7 a new Article 5a was introduced (effective as from 2023 onwards), which includes a more precise definition of foreseeably relevant information requests:

111 However, in view of Case 276/12, *Sabou*, 22 October 2013, ECLI:EU:C:2013:678, such a prior notification is not mandatory.

112 For an analysis of the development of the foreseeable relevance principle in EU law, see S.M. González, 'Transparency and foreseeable relevance in exchange of information procedures', in: M. Serrat Romaní, J. Korving & M. Eliantonio (red.), *Exchange of Information in the EU*, Cheltenham: Edward Elgar Publishing (2024): 8-35, retrieved from: https://www.elgaronline.com/edcollchap/book/9781035314560/book-part-9781035314560-9.xml#:~:text=The%20purpose%20of%20this%20chapter%20is%20to%20analyse%20the%20evolution.

113 Council Directive (EU) 2021/514 of 22 March 2021 amending Directive 2011/16/EU on cooperation in the field of taxation, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021L0514 (hereinafter: DAC7), recital 3.

> *"For the purposes of a request referred to in Article 5, the requested information is foreseeably relevant where, at the time the request is made, the requesting authority considers that, in accordance with its national law, there is a* ***reasonable possibility*** *that the requested information* ***will be relevant*** *to the tax affairs of one or several taxpayers, whether identified* ***by name or otherwise****, and be* ***justified for the purposes of the investigation****".*

With the aim to demonstrate the foreseeable relevance of the requested information, the requesting authority shall provide at least (a) the *tax purpose* for which the information is sought and (b) a *specification* of the information required for the administration or enforcement of its national law.[114] According to the CJEU "the identity of the taxpayer under investigation" is, in principle, a necessary element of the request for information, in order to substantiate the expected interest and to oblige the requested State to comply with the request.[115] However, according to the CJEU, the identity of a taxpayer can also be interpreted on the basis of "data that make it possible to recognize a person as a person", and these are not limited to the identification of a person by their name.[116] According to the OECD Commentary, it is not necessary to provide *names and addresses* of the taxpayers concerned, but *contextual information* to identify the taxpayer is sufficient.[117] So both the OECD Commentary and the CJEU decision make it clear that it is sufficient that taxpayers are *identifiable*.

Concluding statement

Under Article 26 OECD-MC States are required to exchange information upon request, but there is no obligation to cooperate in fishing expeditions or requests that are unlikely to contribute to taxation.[118] It can be stated that although the principle of foreseeable relevance has a broad interpretation, information requests should not be made (1) without reason (*nexus*), and the request must be (2) *individualisable* and *sufficiently concrete* in order to meet the standard (3) *at the time the request is made*. In the application of FCInet ma^{3}tch the presence of a hit, prior to its validation, implies sufficient nexus for the receiving State to meet the foreseeable relevance threshold for the follow-up verification request (Section 4.3.1). See Section 2.3 below for the point at which the foreseeable relevance requirement must be met in the context of spontaneous exchange through the use of FCInet ma^{3}tch.

2.3 Spontaneous exchange of information

The Commentary on Article 26 OECD-MC also provides some guidance on the interpretation of the standard of foreseeable relevance for the spontaneous exchange of information. Spontaneous exchanges usually begin when a tax authority or investigative

114 Article 5b(2) DAC7.

115 Case 437/19, *État du Grand-Duché de Luxembourg*, 25 November 2021, ECLI:EU:C:2021:953, at 72.

116 Case 437/19, *État du Grand-Duché de Luxembourg*, 25 November 2021, ECLI:EU:C:2021:953, at 51.

117 OECD Commentary 2017, par. 5.2.

118 See also Article 5/5a DAC, and Articles 26 OECD Model TIEA 2002 and 6 MAAC.

agency collects information about a taxpayer from another State during their own tax investigation or in the course of an audit.[119] Spontaneous exchange of information is "usually effective, since it concerns particular things detected and selected by tax officials of the State providing information during an audit or investigation".[120] However, even in the case of a spontaneous exchange, the foreseeable relevance principle must be complied with. The question is how minimal the information on a person for the taxation by the receiving State must be to meet the foreseeable relevance standard.

Foreseeable relevance in spontaneous tax information exchange

In view of the Commentary on Article 26 OECD-MC, a competent authority may provide information to another State spontaneously if "it supposes to be of interest to the other State".[121] The relevant indicator here is that the information *is supposed to be relevant* to the taxation in that other State. This terminology implies – like the information exchange on request – that it is *not* necessary that the information to be exchanged *must* ultimately *be relevant*. The terminology 'supposes to be of interest' does seem to indicate that a *minimal link* (minimal nexus) between the information and the State to which spontaneous exchange takes place is needed and is also sufficient. To meet the standard of foreseeable relevance regarding spontaneous exchange of information, we can conclude that the (personal) data shared must *at least be able to be of interest* for the taxation in the receiving State. In the case of spontaneous exchange about a group of taxpayers, this minimum link must be met for *each taxpayer* at the time of the spontaneous exchange. In the application of FCInet ma^{3}tch this means at least the moment of making the filter available. A specific investigation or examination of a person will usually involve a minimum level of relevance, as it raises reasonable suspicion of non-compliance with a specific legal obligation in the source State, which may indicate relevance for tax purposes in the receiving State. When using ma^{3}tch, in principle all persons whose hashed data is included in the filter are involved in an investigation, so that a minimum link with the receiving State will be assumed to be present quite easily.

In this regard, too, it should be noted that as from the changes to the OECD-MC in 2005 (see Sections 2.1.1 and 2.1.2) in some States the competent authorities are obliged, based for instance on an international agreement on the exchange of information (including DAC and MAAC), to require prior authorisation from the source State for the use of exchanged information for *non-tax purposes* or to be *disclosed to third parties*. In those cases, the foreseeable relevance standard will have to be met *at the time of obtaining authorisation*. We will illustrate this with a few examples from the country analysis (see Chapter 3 and Annex 1). An example can be found in the DTC between the Netherlands and Germany. Article 27(2) provides that exchanged information may be used for other purposes if it may be used for such purposes under

119 Jeong 2013, p. 459.

120 Jeong 2013, p. 447 with reference to OECD (2006), 'Module 2 on Spontaneous Exchange of Information', in: *Manual on the Implementation of Exchange of Information Provisions for Tax Purposes*, p. 3.

121 OECD Commentary 2017, par. 9-c, p. 494.

the laws of both States and the competent authority of the sending State *consents* to such use. Another example can be found in the DTC between Canada and Germany; under Article 26(1) exchanged information may only be disclosed in public court proceedings or in judicial decisions if the competent authority of the sending State *raises no objection*, which contains an element of prior authorisation. This is different, for example, in the DTC between Canada and the Netherlands, where based on Article 26 exchanged information may be disclosed in public court proceedings or in judicial decisions without such consent. The wording of the exchange article in tax treaties may contain nuances on the point of authorisation by the sending State. The same regards for a rare number of States in which the competent authorities are obliged, based on national legislation, to inform their residents of a spontaneous exchange of information.[122] In such cases, the competent authorities will have to demonstrate *at the time of notification* that the standard for foreseeable relevance has been met. Examples of States where this applies are Italy (see Annex 1.1.3), Liechtenstein (pursuant to Article 28a *Steueramtshilfegesetz*, hereinafter: SteAHG) and Switzerland (see Article 22b Tax Administrative Assistance Act, hereinafter: TAAA). For the purposes of FCInet ma^{3}tch, the prior authorisation or prior notification obligation means that the data used for ma^{3}tch must have a minimum link with the jurisdiction of the receiving State *prior to sharing the filter*.

By its very nature, spontaneous exchange of information depends on the "active participation and cooperation of local tax officials (e.g. tax auditors, etc.)".[123] However, spontaneous exchange of information can also be challenging, because it may give the impression that the sending State does not protect personal information of their citizens.[124] The protection of personal data is important in any case if personal data is processed automatically. However, even in the case of spontaneous exchange of information, there may be a breach of the privacy of a taxpayer and more specifically of the protection of personal data (see Section 2.4). It should be noted, however, that spontaneous exchange of information also does *not* require sharing the *name of the person* in question, allowing, for example, hashed names to be provided to protect personal data, as FCInet ma^{3}tch does.[125] The condition that must be met in this regard is that the information provided is *sufficient to identify* a person (identifiable).

Furthermore, the effective functioning of spontaneous exchange of information depends on the willingness and ability of the States involved to provide information on their own initiative. A State does not receive any *financial compensation* for the spontaneous exchange of information to receiving States, so there is no direct incentive

122 Generally, tax authorities are not obliged to notify taxpayers about their intention to either request or send information to another state; states are at liberty to implement such notification procedure. See Boei & Van Dam 2022, p. 81-82 with reference to CJEU 22 October 2013, nr. C-276/12, ECLI:EU:C:2013:678 (*Sabou*).

123 Jeong 2013, p. 447.

124 Jeong 2013, p. 459.

125 OECD Commentary 2017, par. 5.2, p. 489: "The standard of 'foreseeable relevance' can be met both in cases dealing with one taxpayer (*whether identified by name or otherwise*) or several taxpayers (*whether identified by name or otherwise*)".

to provide the information from a financial point of view.[126] However, the OECD provides a number of example cases where spontaneous exchange of information should be considered[127]:

- "Where one Contracting State finds *grounds for suspecting* that there may be *a significant loss of tax in another country*;
- Where one Contracting State finds payments made to residents of another country where there is *suspicion* that they have *not been reported*;
- Where a person liable to tax obtains a reduction in or an exemption from tax in one country which *could give rise* to an *increase in liability* to tax in another country;
- Where business dealings are conducted through one or more countries in such a way that a *saving in tax* (i.e. tax avoidance or tax evasion) *may result* in one of the other countries or in both;
- Where a country has *grounds for suspecting* that a *saving of tax* may result from artificial transfers of profits within groups of enterprises;
- Where there is a *likelihood* of a particular *tax avoidance* or *evasion* scheme being used by other taxpayers."

These cases have in common that they result in a reduction of tax liability in another State, while it would have been particularly difficult for the other State to become aware of these cases without the spontaneous exchange of information.

Concluding statement

In the light of societal developments to facilitate the exchange of information in the fight against tax avoidance and tax evasion, it can be stated that – in order for the foreseeable relevance principle to apply in spontaneous exchange of information – there must be a *minimum link* (minimum nexus) between the information to be provided about a taxpayer and its relevance for taxation in the other State. Where this link is absent, the requirement of foreseeable relevance is not fulfilled. The link must at least be there when the information is provided spontaneously, i.e. for the application of FCInet ma^{3}tch when sharing the filter. In principle, all persons whose hashed data is included in the ma^{3}tch filter are involved in an investigation, which may facilitate the assumption of a minimal link with the receiving State.

Key takeaway:

To meet the principle of foreseeable relevance under Article 26 OECD-MC, information must be individualised, concrete, and linked to taxation in the receiving State. In the context of FCInet, a detected hit provides sufficient nexus for follow-up, though the minimum link must already exist at the moment of sharing the filter. This standard also applies earlier in cases where for instance prior authorisation is legally required. Without such a link, the requirement of foreseeable relevance is not fulfilled.

126 Jeong 2013, p. 458.

127 Jeong 2013, p. 460 with reference to OECD (2006), p. 3 and Urtz, *EC Tax Review* (1996), p. 172-173.

2.4 Protection of taxpayer information

Collecting, combining and analysing information offers benefits, but it can also easily infringe on the privacy of citizens when it comes to personal data.[128] Benefits include increasing knowledge and identifying certain trends and threats. The right to privacy and data protection imposes limits on the purposes for which provided data can be used. It is therefore important for governments to know what they can and cannot do with the personal data collected. Data protection concerns the rights and fundamental freedoms of an individual, and in particular the right to privacy, in relation to the *processing of personal data*. Such processing may be defined as *any automated operation on personal data*. It includes, among others, the collection, consultation, use, transmission and exchange of personal data.[129]

The OECD Commentary 2005 explicitly addresses the importance of the protection of personal data in the exchange of information under Article 26 OECD-MC.[130] As discussed in Chapter 1, for universal purposes these taxpayer rights are laid down in Article 17 ICCPR and for EU purposes in Articles 8 EHRM and 7 and 8 of the Charter. To protect taxpayers' information, it is important that States – that provide taxpayer data to another State – can ensure that the information is used appropriately. States are therefore in a delicate situation; on the one hand forced to carefully consider the data protection needs of taxpayers and, on the other hand, the need to exchange information to combat tax fraud, financial crime or other crimes that undermine society.

Although international (model) agreements on the exchange of tax information do not always contain a general provision on the protection of personal data, they do contain rules on the confidentiality of tax information (*tax secrecy*). Under Article 26(2) of the OECD-MC, requesting States are required to treat all information received as secret under the domestic law of that State. Thus, once information has been exchanged, the requesting State must follow *its own laws* regarding the protection of taxpayers' data. The exchange of tax information therefore requires confidence between the competent authorities exchanging information. This applies not only to the data exchanged itself, but also to the information provided in the request for information. After all, this information can also constitute a breach of the privacy of individuals. In addition, it is important for taxpayers to be able to control the information they have provided to national tax authorities. This control may be jeopardised if the information exchanged is used for non-tax purposes or, for example, is forwarded to other States.[131]

Data protection in exchange of tax information

Paragraph 10 of the 2005 OECD Commentary on Article 26 recognises that States may "wish to include provisions in their bilateral conventions concerning the protection of personal data exchanged". The Commentary provides rules to protect the right to privacy and personal data and recommends that States include provisions

128 Kroon 2013, p. 23.

129 Huiskers-Stoop, Breuer & Nieuweboer 2022, p. 91 with reference to Article 4(2) EU GDPR.

130 OECD Commentary 2005, par. 10.

131 Huiskers-Stoop, Breuer & Nieuweboer 2022, p. 88.

that safeguard those rights, since the OECD-MC as such does not provide for this. This raises the question of how States should deal with the exchange of information, if they have not included a data protection and privacy protection provision in the bilateral tax treaty. The provision is not a prohibition because it is not worded as 'may not' but can be *applied voluntarily* because it is worded as 'may refrain from'.[132] Thus, States have a choice to exchange information that is covered by a privacy rule; i.e. it is not prohibited. It is therefore important that States *adopt national legislation* that safeguards data protection rights.

Once the competent authority has received information, it is responsible for processing it appropriately. It is also the responsibility of the tax administration to ensure that the exchange of information provides sufficient safeguards to protect the confidentiality and privacy of the information exchanged.[133] The tax administration, for instance, must implement appropriate technical measures to ensure the security of personal data.

The main rule is that personal data may only be collected and processed in a proper and careful manner in accordance with the law.[134] Other conditions are that data should only be processed to the extent that they are *adequate*, *relevant* and *not excessive*.[135] According to the EU GDPR the processing must also be *lawful*, *fair* and *transparent* and for the purpose for which it was collected.[136] Furthermore, the data may *not* be kept *longer than is necessary* for the purposes for which they are processed (storage limitation).[137] Moreover, individuals have the right to *transparency* about what happens to their personal data and the *protection* thereof (integrity and confidentiality must be guaranteed).

132 Huiskers-Stoop, Breuer & Nieuweboer 2022, p. 92.

133 I. Mosquera Valderrama & F. Debelva, 'Privacy and Confidentiality in Exchange of Information: Some Uncertainties, Many Issues, but Few Solutions', *Intertax*, (2017) 45(5):362-381.

134 Huiskers-Stoop & Nieuweboer 2018, p. 11.

135 Case 131/12, *Google Spain*, 13 May 2014, ECLI:EU:C:2014:317, at 72: "Under Article 6 of Directive 95/46 and without prejudice to specific provisions that the Member States may lay down in respect of processing for historical, statistical or scientific purposes, the controller has the task of ensuring that personal data are processed 'fairly and lawfully', that they are 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes', that they are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed', that they are 'accurate and, where necessary, kept up to date' and, finally, that they are 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed'. In this context, the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified".

136 Article 6 EU GDPR.

137 Article 5(1)(e) EU GDPR.

If there is a legal breach of the right to privacy and the protection of personal data, that infringement must be *justified* and also *understandable* for the taxpayer.[138] In addition, an infringement is only permitted if it is in the interest of the "national security, public safety or economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".[139] In order to assess whether an infringement is *necessary*, it is also important to determine whether it is *proportionate* and whether the data can also be obtained in another, l*ess burdensome* way (subsidiary). According to the CJEU, a request for the exchange of information seeking to engage in a fishing expedition qualifies as an arbitrary or disproportionate intervention by the public authorities and is impermissible.[140] Therefore, it can be argued that *only* the exchange of information that is *foreseeably relevant* can be considered to have a *legal provision* (i.e. is lawful) and may be exchanged under (European) data protection rules as.[141] Thus, compliance with the foreseeable relevance principle precedes the protection of personal data, in other words foreseeable relevance of the information to be exchanged is in our view a *prerequisite* for complying with data protection rules for tax purposes. However, the fulfilment of the foreseeable relevance standard (no bulk data exchange, no fishing expeditions) referred to in Article 26 of the OECD-MC is not in itself sufficient to justify an interference with the right to privacy and data protection. To justify an infringement, more requirements must be met. See Section 4.4.

2.5 Preliminary conclusion

In order to answer the sub-question regarding *the reasoning and legal context behind the principle of foreseeable relevance in relation to the exchange of tax information*, it is important from a historical perspective to note that between 1998 and 2005, the nature of the concept evolved from 'necessary' to 'foreseeably relevant', to align with developments in the international exchange of information. It is also important to note that in 2005 the scope of the taxes covered by the Convention was extended from taxes imposed on 'income and capital' to taxes of *every kind*. In addition, it is important that the information to be exchanged is *not limited to taxpayer-specific data*. Competent authorities may also exchange other *sensitive information*, for example, with a view to improving tax compliance. Furthermore, the information provided must be treated as *secret* in the receiving State, in the same manner as information obtained locally, under the domestic law of that State. The maintenance of secrecy in the receiving State is governed by domestic law, and at the national level, States may provide for exceptions to tax secrecy.

138 Huiskers-Stoop, Breuer & Nieuweboer 2022, p. 91.

139 Article 8(2) ECHR.

140 Case 245/19, *État luxembourgeois v. B and Others*, 6 October 2020, ECLI:EU:C:2020:795, at 113: "a decision ordering that information be provided, by which the requested authority followed up on a request for exchange of information from the requesting authority seeking to engage in a 'fishing expedition' as referred to in recital 9 of Directive 2011/16 would be tantamount to an arbitrary or disproportionate intervention by the public authorities".

141 Huiskers-Stoop, Breuer & Nieuweboer 2022, p. 93.

Since 2005, information may also be disclosed to 'oversight bodies', including authorities responsible for supervising tax administrations and enforcement agencies that operate within the general administrative framework of the contracting State. Thus, data collected by tax authorities and exchanged with other tax authorities should, in principle, be used solely for the administration and enforcement of tax law. However, some tax treaties and other international agreements on the exchange of information, such as the MAAC and the DAC, permit the use of exchanged information for *non-tax purposes* or its *disclosure to third parties*. Article 26(3) OECD-MC contains limitations which dictate a State's ability to refuse to provide information.

In order to comply with the principle of foreseeable relevance in the exchange of information *on request*, Article 26 OECD-MC obliges States in principle to cooperate with such a request, but there is no obligation to cooperate in *fishing expeditions* or requests which are *unlikely to contribute to taxation in the other State*.[142] Although the principle of foreseeable relevance has a broad interpretation, information requests should not be made without reason, there should at least be *some degree of knowledge* of an examination or investigation (nexus), the request must allow the *identification of a specific individual* and be *sufficiently concrete*, and the standard must at least be met *at the time the request is made*. In the application of FCInet ma^{3}tch, the presence of a 'hit' after checking the filter is sufficient for the receiving State to meet the requirement of foreseeable relevance for the follow-up verification request (Section 4.3.1). The subsequent validation of the hit by the sending State confirms the actual link, but that is not a requirement for the application of the foreseeable relevance principle.

To comply with the principle of foreseeable relevance in *spontaneous* exchange of information, there must be a *minimum link* (minimum nexus) between the information to be provided about a taxpayer and its relevance for the taxation in the other State. This means that the information *must be able to be of interest*. In the case of spontaneous exchange about a group of taxpayers, this minimum link must be met regarding each taxpayer in relation to a particular receiving State. The link must be there at least *at the time of spontaneous provision* of the information. In the application of FCInet ma^{3}tch this means the moment of making the filter available and in a few cases earlier if *prior authorisation* from the sending State (or in rare cases *prior notification* to the taxpayer) is required. In principle, all persons whose hashed data is included in the ma^{3}tch filter are involved in an investigation, which may facilitate the assumption of a minimal link with the receiving State. If this minimal link is missing, the foreseeable relevance principle is not met.

The examination of Article 26 OECD-MC shows that despite an increase in the number of information exchanges, in the amount of information to be exchanged and in the use of data exchanged for non-tax purposes, since 2010 only the Commentary on Article 26 OECD-MC has been changed, *not the wording itself*. However, the 2024 update to the Commentary also shows that the OECD aims to have a *more swift and*

142 See a similar interpretation regarding the Articles 26 UN Model Tax Convention, 26 OECD Model TIEA 2002, 6 MAAC and 5/5a DAC.

efficient exchange of information among States, as well as to facilitate the use of the information exchanged by competent authorities and by third parties, without the requirement of prior authorisation (or notification) from the sending State. The use of a so-called whitelist of cases in which prior authorisation for the use of exchanged data no longer needs to be obtained, for example in high-priority cases, can contribute to this.

Furthermore, following the analysis of the protection of taxpayer information, it is important to keep in mind that the standard of foreseeable relevance must be interpreted "in the light of the general principle that taxpayers must be protected against arbitrary or disproportionate interference by public authorities in the course of their private activities".[143] In any case, the principle of foreseeable relevance must comply with the right to privacy and protection of personal data, because the absence of this detracts from the lawfulness of the exchange. Important aspects of the protection of personal data are the *lawfulness* of and *transparency* in the collection and processing of the information, the specification of the *purpose* for which the data is collected, the *accuracy* and *control* of the quality of the data, as well as the *security* and *prevention* of the data. The indicators to comply with the foreseeable relevance in general, in the exchange of information on request and spontaneously are summarised in Table 1 (p. 61).

The table shows that the spontaneous exchange of information requires that the foreseeable relevance standard is at least be complied with at the time of spontaneous exchange. In the application of FCInet ma^{3}tch this means at least the *moment of sharing the filter*. In the few cases where a State is required to obtain prior authorisation from the source State for the use of information for non-tax purposes or for its disclosure to third parties – or in the rare cases where a State is required under its national law to inform taxpayers of the exchange before the information is provided to a receiving State – the tax authorities must be able to demonstrate that the condition of foreseeable relevance is met at the time of obtaining prior authorisation or informing the taxpayer. For the purposes of FCInet ma^{3}tch, this prior authorisation or prior notification obligation means that the data used for ma^{3}tch must have a minimum link with the receiving State prior to sharing the filter. A specific investigation or examination of a person generally assumes a minimum of relevance, as it implies a reasonable suspicion of non-compliance with a specific legal obligation in the source State, which may be indicative of any relevance for taxation in the receiving State. The threshold of foreseeable relevance in the case of spontaneous exchange of information must be interpreted as meaning that the information to be provided is supposed to be of interest to the receiving State, in the sense that the information must *at least be able to be of interest*, which may be qualified as a *less onerous requirement* than the requirement of some degree of knowledge of an examination or investigation in the case of an exchange of information on request.

143 Case 245/19, *État luxembourgeois v. B and Others*, 6 October 2020, ECLI:EU:C:2020:795, at 111: "that expression must be interpreted in the light of the general principle of EU law consisting in the protection of natural or legal persons against arbitrary or disproportionate intervention by the public authorities in the sphere of their private activities".

Table 1: Indicators for the assessment of the foreseeable relevance standard.

Indicators to comply with the foreseeable relevance standard	Conditions resulting from Article 26 OECD-MC	Other relevant remarks (resulting from e.g. OECD-TIEA, UN Model Tax Convention, MAAC, DAC)
General	No *fishing expeditions* are allowed	
	No exchange of information that is unlikely to be relevant (*no bulk information*)	
	Relevance must be based on well-founded suspicions (*nexus*)	
	An ongoing examination or investigation to a person(s) is generally accepted as a proof of relevance (*minimum link*)	
On request	At least nexus to an examination or investigation is required (*some degree of knowledge*)	
	It is to the requesting State to *assess* the standard of foreseeable relevance	
	Local usual sources of the requesting State should be *exhausted* first	
	The request must contain sufficient information to identify the relevant taxpayer(s) (*individualisable*)	
	The request must be sufficiently *specific*	
	Domestic restrictions to provide the requested information may apply to the requested State	
	The foreseeable relevance standard must be complied with at least *at the time the request* is made	• In the few cases that a receiving State requires *prior authorisation* from the source State to use tax information for purposes *other than taxation* or to disclose the information to *third parties*, the foreseeable relevance standard must be complied with at the time of obtaining authorisation • In the rare cases that a State is required to inform its residents before providing the requested information (*prior notification*), the foreseeable relevance standard must be complied with *at the time of informing* their residents
Spontaneously	The sending State must *assess* the standard of foreseeable relevance	
	It must be information that is 'supposed to be relevant' to the determination of the tax liability in the receiving State	
	The information must at least *be able to be of interest*	
	There must be a *minimal link* (minimal nexus) for each taxpayer in relation to a particular receiving State	
	The foreseeable relevance standard must at least be met at the time *the information is shared*	• In the few cases that a receiving State requires *prior authorisation* from the source State to use tax information for *purposes other than taxation* or to disclose the information to *third parties*, the foreseeable relevance standard must be complied with at the time of obtaining authorisation • In the rare cases that a State is required to inform its residents before providing the information spontaneously (*prior notification*), the foreseeable relevance standard must be complied with *at the time of informing* their residents

Chapter 3

Comparative analyses across jurisdictions: notable trends and practices

To assess the application of the foreseeable relevance standard across various jurisdictions, a comparative analysis of eleven States is undertaken, among others, to discover whether there are local differences in the way in which the standard is applied. This Chapter offers a general perspective on how States interpret the foreseeable relevance standard and highlights the key differences among them. Although we have used Article 26 of the OECD-MC as a general framework in Chapter 2, we also consider other exchange instruments in this comparison between States. The eleven jurisdictions involved regard EU States, i.e. France, Germany, Italy and Spain (Section 3.1) and non-EU States, i.e. Canada, Colombia, Indonesia, Mexico, Nigeria, South Africa and the United States (Section 3.2). For more detailed descriptions of the States involved in this research, we refer to Annex 1. This Chapter addresses the following question: *What criteria do jurisdictions (involved in the study) distinguish to assess whether the principle of foreseeable relevance has been met in the case of bilateral exchange of information?*

The comparison of the States will highlight differences in the application of the foreseeable relevance standard in the context of exchange of information. Sub-questions in this context are: Who is the competent authority concerned with the levying of taxes? What kind of taxes may this competent authority levy? Are there bi- and/or multilateral instruments to exchange information? Is spontaneous exchange in particular facilitated under domestic law and/or international treaties? How are secrecy rules defined in domestic law? Attention is also paid to the role of tax officials as gatekeepers who manage the flow of information, both internationally and within domestic boundaries among associated public administrative bodies, under established legal frameworks. This gatekeeper role is crucial, as officials must ensure that data sharing adheres to legal requirements. Systems such as FCInet could be well suited to support this role, by enhancing privacy and implementing controls that align with national and international regulations regarding the safeguarding of taxpayer rights and efficient exchange of information. The analysis will identify challenges to effective exchange of information, including issues related to privacy, secrecy, and the variation in domestic rules that govern information sharing. It will also explore the nuances associated with spontaneous information exchanges, where differing national standards may impact the assessment of the foreseeable relevance principle. Although the comparison provides valuable insights, for a deeper understanding of each State's national legal framework, additional research may be required.

3.1 Exchange of information between the EU States

This Chapter starts with an examination of the exchange of information framework within the EU, focusing on the regulations and practices that govern the application of the foreseeable relevance standard. The EU States in the study concern: France, Germany, Italy and Spain. Within the EU, the foreseeable relevance principle is shaped by a unified regulatory framework that aims to standardise data sharing practices among Member States. In this Section, we discuss the instruments governing the exchange of information, local differences in the application of instruments, and the application of taxpayer rights and secrecy rules.

3.1.1 Instruments governing the exchange of information

The instruments mainly used by the EU States to facilitate an effective exchange of information is the OECD-MC, the OECD-TIEA, and the DAC. Foreseeable relevance in the OECD-MC and the TIEAs is fairly similar, as both aim at the exchange of information, and both mention the standard of foreseeable relevance in the OECD-MC in Article 26 and the TIEA model in Article 5. However, a significant difference is that the OECD-MC *includes the spontaneous exchange of information* within Article 26 itself, applying the same threshold of foreseeable relevance to both requested and spontaneous exchanges. On the other hand, Article 5 of the OECD-TIEA model does not mention spontaneous exchange of information. The Commentaries explicitly state that Article 5 of the OECD-TIEA model *does not include spontaneous exchange*, and countries wishing to engage in spontaneous exchanges should include it separately. This is for instance evident in the OECD-TIEA between Spain and Aruba, where both States have included spontaneous exchange of information within Article 6 (see Annex 1.1.4 for Spain). Notably, this Article mentions that information for which the sending State "has grounds for supposing that there may be a loss of tax in the other Party" may be exchanged. The phrase "supposing that there may be" suggests a lower threshold for spontaneous exchanging information – compared to "foreseeably relevant" in exchanging information on request – indicating that a minimal link is sufficient in this case between Spain and Aruba (see also Section 2.3).

Although the DAC is a multilateral tax exchange instrument – and therefore not directly applicable to the bilateral exchange using FCInet ma^{3}tch – the evolution of the foreseeable relevance standard is also important for the bilateral exchange of information, based on for instance the OECD-MC. Within the EU context there is a more *detailed explanation* of the foreseeable relevance standard for the exchange of information on *request* in DAC7 (see also Section 2.2). Article 5a of DAC7 defines foreseeable relevance in the context of information exchange between EU Member States and requires that the requesting State demonstrates that, based on its national law, there is a *reasonable possibility* that the requested information will be pertinent to the tax affairs and necessary for the investigation or enforcement of tax laws. The requesting State must specify the tax purpose and detail the information required, ensuring that the request is well-founded and directly related to the tax matter at hand.

Following this, Article 9 of the DAC covers *spontaneous* exchanges of information. This provision allows for the exchange of information without a formal request when certain conditions are met. Such as when there is a suspicion of potential tax loss in another Member State, or when information might prevent or address tax savings from artificial transactions or business dealings across borders. The threshold for spontaneous exchanges is intentionally *lower* than for requests, acknowledging that immediate sharing of relevant information can be important for an effective tax administration.

Germany serves as a practical example of the domestic implementation of spontaneous exchange based on the DAC (see Annex 1.1.2 for Germany). German national legislation permits tax officials to engage in unilateral spontaneous exchanges of information, as outlined in Section 117(3) of the Fiscal Code (*Abgabenordnung*, hereinafter: AO). This provision allows the German tax authority to disclose information independently, provided certain conditions, such as reciprocity with the foreign recipient country, are met. It is important here to mention that the *Bundeszentralamt für Steuern* (hereinafter: BZSt) or German Federal Central Tax Office, distinguishes between automatic and non-automatic exchanges of information. According to the BZSt, non-automatic exchanges include both spontaneous exchanges and information exchanges on request. The BZSt appears to apply the standard of foreseeable relevance *equally* to both spontaneous exchange of information and the exchange of information on request, suggesting that the threshold for spontaneous information exchange in Germany might be higher compared to the DAC and Article 26 OECD-MC. Different thresholds for spontaneous information exchange used by the EU States may hinder a harmonised interpretation of foreseeable relevance.

Furthermore, Article 10 of the DAC stipulates that once information is communicated under Article 9 DAC, the receiving State must acknowledge receipt as promptly as possible, and at the latest within seven working days of receipt. This requirement ensures that the information exchange process is transparent and that the sending State is informed of the receipt aligning well with the system used by FCInet ma^{3}tch, where, in case of a hit, information is validated after the filter has been shared.

In addition, the concept of foreseeable relevance has been further refined by EU case law, shaping how it is interpreted across the Union. In Case C-682/15, *Berlioz*, resulting from a referral by the Luxembourg administrative court, the CJEU initially clarified the concept, sticking closely to the DAC definitions and outlining broad principles for tax authorities to follow (see also Section 1.7). While this provided a degree of flexibility in requesting information, it emphasised that such requests must remain relevant to the investigation. Building on this, the cases *État luxembourgeois v B* (C-245/19) and *État luxembourgeois v C* (C-246/19) introduced more detailed guidelines. The CJEU determined that information from third parties must be directly related to the taxpayer and the specific focus of the investigation. This means that third parties must have relevant documents, such as contracts or invoices, rather than being randomly chosen. These case judgments seem to aim at ensuring that information exchanges are tightly aligned with the investigation's goals, with a focus on the avoidance of the transfer of irrelevant data.

3.1.2 Local differences in the application of instruments

Laws governing the processing and exchange of information can vary significantly between States, reflecting differences in legal frameworks and institutional structures. These variations may result in different levels of government – such as a *tax law* or *criminal law domain* or even disparate bodies within the same domain – being assigned the authority to handle and share information. One can interpret this as two or more government branches, which are assigned similar tasks. For instance, Italy has three functioning tax agencies (see Annex 1.1.3). It is also noteworthy that some countries designate specific agencies or departments for tax administration, while others involve broader governmental bodies or specialised units. For example, in the U.S., although that is outside the EU, the *Federal Bureau of Investigation* may be involved in an investigation by the *Internal Revenue Services* (hereinafter: IRS). This fragmentation can lead to inconsistencies in how information is managed and exchanged, which is important for systems like FCInet ma^{3}tch, since the competent authority for exchanging information and its use might differ per State.

States have diverse approaches to managing the flow of information between different levels of government. For example, limitations on information exchange between administrative and criminal police departments can be more stringent in some jurisdictions. France, for instance, allows the exchange of tax information with its criminal police but limits the exchange with its administrative police branch (see Annex 1.1.1 for France). These limitations are often aimed at safeguarding privacy and ensuring that information is not misused. However, the *lack of clear and consistent guidelines* can pose challenges, particularly when utilising technologies such as FCInet ma^{3}tch, for which the scope of the local authority and the use of information exchanged can be important for a proper functioning of the technique.

Although criminal law exchange of information instruments may contain requirements compared to the principle of foreseeable relevance, the lack of a standardised concept may complicate the exchange and use of information across different jurisdictions and administrations (see Section 5.3.2). Although the tax and criminal domains are separated within FCInet ma^{3}tch[144], it may be that certain States would like to participate in the network where this is not the case. For such States it is important to gain insight into the *legal and institutional framework* and into possible different levels of competent authorities and in particular whether such levels also extend to the criminal domain. This is particularly important because in certain countries data exchanged for tax purposes, may be used in the criminal domain of the recipient country *upon authorisation of the source State* (see also Chapter 2). If such authorisation is required, it is necessary for the application of FCInet ma^{3}tch for the receiving State to obtain the authorisation before sharing the filter. To gain the necessary insight into possible competency levels and the use of exchanged information in the criminal law domain

144 FCInet 2022, *User Protocol*, p. 7: "Some jurisdictions may have an existing legal framework for exchanging information under both the TAX and LEA domains, while other jurisdictions only have the framework to administer one of the domains. As stated before, FCInet treats the two domains as distinct, and if an agency can exchange under both domains, it will have two distinct FCInet nodes".

or for other purposes, we have developed a *questionnaire* that can be used as a tool to collect the relevant information, and included this in Section 3.3.

The advantage of technologies like FCInet ma^{3}tch is that they offer the capability to implement and enforce specific limitations within both international and domestic systems of information exchange. This built-in flexibility allows for the establishment of tailored controls that respect each State's legal boundaries and institutional practices, rather than relying solely on manual legal application for each spontaneous information exchange. By incorporating these controls, FCInet ma^{3}tch could enhance the proper separation of information flows among different administrative branches and simultaneously improve compliance with domestic regulations, thereby maintaining the integrity of the data exchange process.

Having an exchange process in place – along with its regular or at least reciprocal use – is an important aspect of effective information exchange. A *lack of reciprocity* is one of the reasons a State may reject a request for information exchange, as outlined in paragraphs 15 and 15.1 of the Commentaries on Article 26 OECD-MC (see Section 2.1.1). However, these Commentaries also stress that the standard should be interpreted *broadly and pragmatically* to avoid hindering the exchange of information. For instance, France can exchange information with other EU Member States without a specific exchange of information treaty, provided that the exchange is reciprocal.[145] Italy for instance also reserves the right to withhold information from States that do not meet a certain level of reciprocity in exchange of information.

In the light of reciprocity, in Germany for example, the BZSt distinguishes between spontaneous exchange of information with EU and non-EU members. For EU members, it generally permits the transmission *of almost any information* that can aid in the accurate taxation of a taxpayer in the other EU State, which seems to offer more flexibility than the foreseeable relevance threshold typically allows. Conversely, for non-EU members with which Germany has a DTC, the emphasis is on the presence of *a specific information clause* and *reciprocal arrangements* to determine whether spontaneous exchange of information should be pursued.

According to domestic laws and international information exchange treaties, reciprocity is a significant consideration for the exchange of tax information. As for instance, the DTC between Belgium and France maintains unconditional reciprocity, while agreements between Germany and Finland include exceptions that allow refusal if reciprocity threatens state sovereignty, public security, or the public interest. Such exceptions can impede the efficiency of spontaneous exchanges.

145 As specified in Articles L.114A, R114A-3, and R*114A-4 of the French *Book of Tax Procedures*, retrieved from: https://www.wipo.int/wipolex/en/legislation/details/6038.

3.1.3 The application of Taxpayer Rights and Secrecy Rules

The primary concern in international information exchange is that States are reluctant to share information with jurisdictions that do not maintain *comparable standards of privacy and secrecy*. Within the EU this issue is largely mitigated, as the EU GDPR establishes stringent privacy and data protection standards that ensure a high level of confidentiality (see Section 4.5). This regulatory framework fosters an environment where privacy is rigorously protected, which facilitates more efficient information exchanges among EU Member States.

However, when it comes to information exchange between the EU and non-EU States, these privacy and secrecy standards become more prominent. Non-EU States may not always align with the same levels of privacy protection as those mandated by EU regulations. This discrepancy can create challenges, as States with stringent privacy laws, may be hesitant to exchange information with jurisdictions that do not meet their privacy and secrecy requirements. For example, French domestic law explicitly permits the tax administration to share data with other States that have entered into an exchange of information agreement with France.[146] However, it can only occur if the other State has comparable secrecy rules or agrees to comply with French secrecy standards concerning the exchanged information.[147] As a result, the exchange of information across international borders can be significantly impacted by the varying privacy standards and regulatory frameworks of the States involved.

3.2 Exchange of information by non-EU States

The examination will now shift to the non-EU landscape, presenting insights from comparative analyses on how these countries approach the exchange of information and the foreseeable relevance principle. The States in this Section concern: Canada, Colombia, Indonesia, Mexico, Nigeria, South Africa and the U.S.. In non-EU States, the approach varies more significantly, often aligning with OECD standards, but with some differences in its practical execution. Also, for the non-EU States we discuss the instruments governing the exchange of information, local differences in the application of instruments, and the application of taxpayer rights and secrecy rules.

3.2.1 Instruments governing the exchange of information

The main instruments governing information exchange and tax treaty obligations are largely shaped by the OECD guidelines and the OECD-TIEAs. Across the States involved in this study, there is a strong alignment with the OECD's standard of foreseeable relevance as included in Article 26 OECD-MC. Most countries have incorporated this standard into their bilateral tax treaties and information exchange agreements, ensuring a consistent approach.

146 This authorisation is grounded in Article L. 114 of the French *Book of Tax Procedures*.

147 As specified in Article R*114A-1 of the French *Book of Tax Procedures*.

While there are some minor differences in terminology – such as the use of terms like 'necessary' (used by the OECD until 2005) instead of 'foreseeably relevant' (as from 2005) – these differences do not significantly impact the overall interpretation. Contracting States interpret terms as 'necessary' or 'may be relevant' in line with the concept of foreseeable relevance. For example, the 2016 peer review assessment indicated that most of Nigeria's DTCs use the term 'necessary' (see Annex 1.2.5 for Nigeria). This terminology is consistent with the guidance provided in the 1998 Commentary on Article 26(1) of the OECD-MC, which allows for flexibility in adopting alternative formulations of the 'is necessary' standard. Since 2005, the term 'is necessary' or 'is relevant' should have been replaced by 'foreseeably relevant' to fit with the Article's scope. This trend is reflected in two DTCs, which utilise the term 'foreseeably relevant'. The authorities in Nigeria have also clarified that, when terms like 'is necessary' or 'may be relevant' are employed, they interpret them to imply foreseeably relevant information exchange. While this is a straightforward example, we observed a range of similar terminological variations across tax treaties, especially in older agreements.

An example of the language specifically used for spontaneous exchange in OECD-TIEAs, as illustrated with the case of Spain and Aruba (Section 3.1.1), is also evident in the OECD-TIEA between the U.S. and Uruguay concluded in 2023. In Article 7 of this agreement, it is stipulated that information should be exchanged if the tax authority 'supposes it to be foreseeably relevant'. This wording indicates a lower threshold for information exchange compared to the standard of foreseeable relevance in the exchange of information on request, again suggesting that *a minimal assumption of relevance* is sufficient for the spontaneous exchange to take place. However, it is interesting to see that this language also differs from the one used in the OECD-TIEA between Spain and Aruba. These differences are further illustrated in the country comparison descriptions in Annex 1, which shows that, despite minor linguistic variations, the core principle of foreseeable relevance is consistently applied in practice.

However, the tax authorities' competence to use the information received can vary significantly depending on the treaty's provisions. For instance, the DTC between Italy and Mexico restricts the use of information to *tax purposes only*, as specified in Article 25(1) (see Annex 1.2.4 for Mexico). In contrast, other treaties (and also the MAAC and the DAC in EU exchanges) may permit the use of information for *purposes beyond taxation*, provided such use is *permitted by the laws* of both States and *authorised* by the competent authority of the sending State (see Chapter 2). For example, Article 29(2) of the DTC between Germany and Sweden allows for information to be used for other purposes, if permitted under the laws of both States and authorised by the competent authority of the sending State. Similarly, Article 30(1) of the DTC between the U.S. and the Netherlands extends the use of information to criminal proceedings, but only if prior authorisation has been granted by the competent authority that supplied the information (see Section 2.1.2 and Annex 1.2.7 for the U.S.).

A third possibility is that countries *agree* to use exchanged information for purposes beyond taxation without needing to notify the other party. An example of this is the DTC between South Africa and India, where Article 25(2) states that, notwithstanding

the preceding provisions, information received by a contracting State may be used for other purposes, if such use is permitted under the laws of both States and authorised by the competent authority of the sending State (see Annex 1.2.6 for South Africa). These three approaches show the varying degrees of flexibility in tax information exchange treaties, which influence the usefulness of information when exchanged with partner countries.

Lastly, an interesting feature in some tax treaties is the requirement to exchange information even if it is *not relevant to the domestic tax interests* of the requested State (see Section 2.1.1). For example, Article 25(4) of the DTC between Colombia and Canada stipulates that a partner must provide information even if it does not pertain to the requested State's own tax purposes. This provision illustrates a broader approach to information exchange, emphasising that data sharing must take place regardless of immediate domestic (tax) relevance (see Annex 1.2.1 for Canada and 1.2.2 for Colombia).

3.2.2 Local differences in the application of instruments

Domestic regulations on information exchange reveal significant variations between States. In certain States, such as Indonesia and Nigeria, access to information about the exchange process is often limited (see Annex 1.2.3 for Indonesia). In contrast to States such as the U.S. and Canada, which have established sophisticated systems for handling information exchanges.

The U.S. serves as an exemplary model for best practices in the exchange of tax information due to its well-structured domestic laws and procedures. Under Article 26 U.S.C. § 6103(k)(4), U.S. law explicitly permits the exchange of tax information with foreign governments based on tax treaties or other agreements. This legal framework ensures that information sharing occurs in strict alignment with the conditions specified in each treaty or agreement. This codification in U.S. law provides a clear and consistent approach to information exchange.

For spontaneous exchanges, the IRS has detailed guidelines in the U.S. set forth in Section 4.60.1.3.1 of the *Internal Revenue Manual* (hereinafter: IRM). The IRM establishes a systematic approach where IRS personnel, under the oversight of the U.S. competent authority, the *Commissioner of the Large Business and International Division* (hereinafter: LB&I Division), can send spontaneous information to foreign counterparts. This procedure is notably precise compared to practices in other States, ensuring transparency and adherence to established protocols.

While the threshold of foreseeable relevance is explicitly required for information exchange upon request, the U.S. does not apply this standard with the same specificity for spontaneous exchanges.[148] Instead, Section 4.60.1.3.1 focuses on the potential usefulness of information to the foreign tax administration, rather than a strict

148 As detailed in Sec. 4.60.1.2.1 (4)(J) of the IRM, retrieved from: https://www.irs.gov/irm.

demonstration of foreseeable relevance. This approach allows the IRS to determine the relevance of information based on its potential utility, rather than requiring a specific forecast of its relevance. The U.S. model could therefore serve as a benchmark for best practices in information exchange, showcasing an effective system for integrating structured legal frameworks with practical information-sharing procedures.

It is also worth noting that many of the best practices observed outside the EU are U.S. standards. Additionally, the States in this study did not present any other notable best practices regarding exchange of information beyond those examples discussed in the country comparison.

3.2.3 The application of Taxpayer Rights and Secrecy Rules

There is a significant difference in taxpayer rights and secrecy rules between *developed and developing countries*, which can affect the effectiveness of international information exchange. Developed countries generally have *well-established frameworks* that balance taxpayer privacy with the need for transparency and information sharing. These States typically adhere to international standards, such as those set by the OECD or the EU, and have defined procedures for exchanging information that ensure strong privacy protections.

In contrast, developing countries may encounter more challenges in aligning with these standards due to variations in legal infrastructure, legal resources, and legal frameworks. These States might implement more restrictive secrecy rules and have less comprehensive taxpayer rights protections, which can impede an effective information exchange. For example, stringent confidentiality requirements in some developing countries can limit their ability to share information or adopt international best practices.

Nonetheless, there is a trend toward improvement as developing countries begin to adopt regulations that *align with global standards*, such as the EU GDPR. A pertinent example is Nigeria, which has introduced the *Nigeria Data Protection Regulation* (hereinafter: NDPR). The NDPR incorporates many principles from the EU GDPR. Similarly, Mexico recognises privacy as a human right in its Constitution under Article 16 and specifies in Article 6 that private information is protected and must be distinguished from public information (see Annex 1.2.4 for Mexico). In Colombia, the general principle of privacy rights is also evident, as enshrined in Article 15 of the 1991 Constitution. This article establishes the legal framework for transparency in tax information and tax secrecy in Colombia. We also notice that, according to a study conducted by *Greenleaf* in 2017, Indonesia has recently also satisfied international criteria for having a data privacy law. From these examples, we notice a growing commitment to enhance data protection and privacy standards.

However, when it comes to the design of privacy safeguards in non-EU States, there are not only differences between developing countries, but there are also notable differences between developed countries, such as Canada and the U.S.. This is particularly

significant given Canada's comprehensive privacy protections under the *Constitution Act*, the *Income Tax Act*, the *Privacy Act*[149], and the *Access to Information Act*, among others. Canada adheres to a *principle of proportionality* in its data collection and makes a strict *distinction* between *civil* and *criminal tax matters*, with the latter subject to stricter search and seizure protections, resulting in a more restrained approach to data gathering. In contrast, the U.S. does *not have* a comparable *proportionality principle* in its data collection practices and has *wider access* to a taxpayer's personal data. These differences can be challenging for the operation of techniques such as FCInet ma^{3}tch, as compliance with the foreseeable relevance standard sometimes requires taking into account domestic rules in the sending or receiving State on, for example, *prior authorisation* (or in rare cases *prior notification*).

Key takeaway:

While most States adhere to the OECD standard of foreseeable relevance, national differences exist in how the standard is applied, particularly regarding spontaneous exchange, the competent authorities, and the use of information for non-tax purposes. Domestic laws and treaty provisions often impose varying requirements, such as prior authorisation or taxpayer notification, which affect the timing and legality of data exchange. These differences can create challenges for the use of FCInet. However, FCInet also seems to play a significant role in facilitating the secure exchange of information between nations and ensuring a minimum standard of privacy for all parties involved.

3.3 Preliminary conclusion

While the previous Chapter was mainly about the reasoning and legal context of the foreseeable relevance principle, the country comparison in this Chapter takes a more practical approach. In order to answer the sub-question *how the different jurisdictions (involved in the study) comply with the principle of foreseeable relevance in the case of bilateral exchange of information*, we have assessed the application of the principle across various jurisdictions by comparative analyses of eleven countries inside and outside the EU.

The research shows that legislation generally places more emphasis on information exchanges upon request than on spontaneous exchanges. This has to do with the fact that a requesting State is usually better able to articulate the relevance of requested information than a spontaneously sending State can when assessing its relevance within the tax system of the receiving State. As a result, the threshold for what qualifies as relevant in spontaneous exchanges *tends to be lower* than in requested exchanges.

149 Privacy Act (Revised Statutes of Canada 1985, c. P-21), retrieved from: https://laws-lois.justice.gc.ca/eng/acts/p-21/FullText.html.

Globally, most States adopt the OECD standard for the principle of foreseeable relevance, resulting in a generally consistent application across various jurisdictions. The standardisation provided by the OECD facilitates a uniform approach to information exchange, thereby minimising potential barriers to the integration of advanced privacy enhancing technologies. However, we have also observed significant variations in how the use of exchanged information for purposes beyond taxation is addressed in different DTCs, which could present challenges regarding the competence of tax authorities. States generally adopt one of the three following approaches: restricting the use of received information solely to tax matters; allowing its use for additional purposes, subject to authorisation by the competent authority of the sending State; or permitting its use for non-tax purposes without requiring prior notification to the partner State (by using for instance a so called 'whitelist'), provided it complies with the laws of both States.

An interesting finding is that Article 26(4) of the OECD-MC, as reflected in the DTC between Colombia and Canada, requires the exchange of information even if it is not relevant to the domestic tax interests of the requested State. This raises an important question regarding spontaneous information exchange: does such a provision require States to spontaneously share information, even when it is not directly related to their own tax assessments? Since the amendment of Article 26 of the OECD-MC in 2005, this question must be answered in the affirmative for the exchange of information on request. In our view, this question does not play a role in the case of spontaneous exchange of information, since the relevant information has already been obtained in the course of the tax authority's own investigation. Information already obtained should be exchanged with other States spontaneously if an exchange instrument requires so.

Privacy and secrecy regulations may pose challenges in relation to information sharing. Some States are reluctant to share information with jurisdictions that do not adhere to *equivalent standards of privacy and secrecy*. This caution reflects a priority for protecting sensitive data and ensuring that international partners uphold comparable confidentiality levels. Such concerns highlight the importance of maintaining privacy and secrecy, by for example applying the EU GDPR standards to enable effective international collaboration. The need for similar privacy and secrecy standards can be viewed as an aspect of reciprocity as well, which has proven to be a significant consideration for States when exchanging information.

Additionally, laws governing the exchange of information between *different levels of government* can create barriers. In certain jurisdictions, prior authorisation is required before information can be used for *purposes beyond tax administration* and/or submission to *third countries*. While some DTCs, such as Article 30(1) of the DTC between the U.S. and the Netherlands, extend the use of information to criminal proceedings without prior authorisation, others may not. If States with such requirements want to use FCInet ma^{3}tch, it is important to be aware of these requirements, because in those cases the foreseeable relevance standard may need to be met *before* sharing the filter.

The questionnaire in Table 2 (p. 75) can be used to gather information on a number of specific issues relating to the interpretation of the principle of foreseeable relevance in practice. The questions relate to the domestic legal procedure for the competent authority regarding spontaneous exchange of information following from Article 26 OECD-MC, the assessment criteria to safeguard the foreseeable relevance standard, the minimum link required between the information to be provided and the relevance for taxation in the receiving State, additional requirements with regard to the exchange of information on request, the applicability of data protection rules, the use of information received for other purposes than taxation, the submission to third countries or to non-tax administrative bodies and whether special rules for prior authorisation or prior notification apply.[150] Although the questionnaire has a wide application it does not aim for completeness because States may have different rules locally.

Key takeaway:

For the application of FCInet ma³tch it is important to know whether certain provisions apply to the participating countries in the network. Therefore, creating an oversight of such requirements with respect to the organisations participating in the FCInet ma³tch network is recommended. The questionnaire to identify relevant aspects for the standard of foreseeable relevance below, can be used for this purpose.

150 This questionnaire is intended for tax professionals who *regularly engage with exchange of information in their administrative practice*. Ideal respondents include tax inspectors with practical knowledge and experience in spontaneous exchange of information and the exchange of information on request. It is also possible to answer the questions based on experiences with another international information exchange instrument, such as the MAAC or others.

Table 2: Questionnaire to identify relevant aspects for the standard of foreseeable relevance

Questionnaire to identify relevant aspects for the standard of foreseeable relevance in Exchange of Information (EOI)	
Questions	**Answers**
I. Could you briefly describe who the **competent authority** is in your country for EOI following from Article 26 OECD-MC (i.e one or more levels of government, only tax domain or also criminal domain, other supervisory bodies, et cetera)?	
II. Could you briefly describe the **domestic legal procedure** in your country for the competent authority regarding **spontaneous** EOI following from Article 26 OECD-MC (i.e. is this procedure based on the law and/or further elaborated in policy et cetera)?	
III. Regarding **spontaneous** EOI following from Article 26 OECD-MC, could you briefly describe which **indicator(s)** (i.e. assessment criteria, steppingstones et cetera) should be assessed in your country to safeguard the foreseeable relevance (FR) standard?	
IV. Is the FR standard interpreted consistently between EOI **upon request** and **spontaneous** EOI? If not, what accounts for the difference(s)?	
V. Could you briefly describe the **minimum link** required in your country – between the information to be provided and the relevance for taxation in the other State – to meet the FR standard for **spontaneous** EOI following from Article 26 OECD-MC?	
VI. Are there **any additional requirements** in your country with regard to EOI **upon request** following from Article 26 OECD-MC to meet the FR standard (e.g. is a minimum link between the information to be provided and taxation in the other State sufficient or are more stringent requirements applicable, such as a 'reasonable possibility' that the information will be relevant)?	
VII. Are there any **privacy or data protection regulations** in your country (e.g. domestic rules or Article 8 EHRM, Articles 7 and 8 Charter, Article 17 ICCPR) or in the applicable EOI instrument? How are the terms 'anonymised' and 'pseudonymised' interpreted in your country in light of the application of data protection rules?	
VIII. Does the international instrument permit the use of information received for **purposes other than taxation**, and if so, under what conditions (e.g. in all cases, specific cases, or with **prior authorisation** of the source State) and for what purposes (e.g. for criminal investigations, anti-money laundering or otherwise)?	
IX. Does the international instrument permit the use of information received for **submission to third countries**, and if so, under what conditions (e.g. in all cases, specific cases, or with **prior authorisation** of the source State) and for what purposes (e.g. for criminal investigations, anti-money laundering or otherwise)?	
X. Does the international instrument permit the use of information received for **submission to non-tax administrative bodies**, and if so, under what conditions (e.g. in all cases, specific cases, or with **prior authorisation** of the source State) and for what purposes (e.g. for criminal investigations, anti-money laundering or otherwise)?	
XI. Does the taxpayer based on domestic regulations have the **right to be notified** by the tax authority before the EOI relating to them with another State (prior notification)? Does it make a difference whether there is **spontaneous** EOI or EOI **upon request**?	
XII. Finally, have you identified any legal or interpretative gaps in the application of the FR standard in **spontaneous** EOI or EOI **upon request**?	


ZNC492Q
9015
R48 R50
C34
R64
R68
R69
RAL24F0
C40
SP
C/D
E1
R71 C45 R73 DSP SP C48
R74 R72
R90 SP
R79
LS01
XJM016
611100-003
JAPAN

Chapter 4

FCInet ma³tch technology in the light of tax data protection

The FCInet ma³tch technology runs within a fully digital infrastructure of connected computers, a so-called *peer-to-peer network*. The source data remain locally under the control of the data owner. With the ma³tch filter, a unique code consisting of a series of numbers is generated based on personal data in the database of the source owner. This filter aggregates and 'hashes' data of any size and combines it into a *fixed-size output*.[151] If there is a hit between personal data in the database of the receiving State and the data used for creating the filter, the receiving State can – after verification and validation of the hit – create a regular request for tax information within the existing legal framework. This Chapter addresses the following question: *Does the way in which FCInet ma³tch is applied, more specifically in the light of the right to privacy and data protection, have an impact on the assessment of whether the requirement of foreseeable relevance is met?*

To answer this question, we distinguish between spontaneous exchange of information and exchange on request, because sharing the filter qualifies as spontaneous exchange, while exchanges on request comes into play when the receiving State detects a hit. After description of the operation of FCInet ma³tch in Section 4.1, we will discuss the technical phases related to spontaneous exchange of information in Section 4.2 and those related to information exchange on request in Section 4.3. Relevant sub-questions for FCInet are whether the sharing of the filter can be considered foreseeable relevant itself and whether detection of a hit automatically implies relevance (see the questions raised in Section 1.3). In addition, the technical process of creating, sharing and checking the filter will be tested against the requirements for privacy and data protection (Sections 4.4 and 4.5).

4.1 FCInet ma³tch technology

For a good understanding of the technical operation of FCInet ma³tch, we refer to the previously discussed reports on *Enhanced Exchange of Information in Financial Investigations* (University of Groningen 2021) and *The use of ma³tch technology by JenV to carry out access and deletion requests* (Pels Rijcken and VKA 2023).[152] On the basis of these reports, supplemented with the guidance and training we received from FCInet, the technical operation of ma³tch can be described by the following four phases[153]:

151 A hash can be described as a 'message digest, fingerprint or compression function', which is the result of a mathematical function that 'takes any size input string' and convert it into a fixed-size binary sequence. See Kroon 2021, p. 51.

152 See the glossary in Pels Rijcken & VKA Report 2023.

153 Pels Rijcken & VKA Report 2023, Sec. 6.2.

1. the start-up phase (i.e. creating the filter);
2. the execution phase (i.e. sharing the filter);
3. the verification phase (i.e. verifying and validating a hit), and
4. the completion phase (i.e. requesting and providing tax information).

Below we will discuss these phases in more detail, related to the phase of spontaneous exchanging the FCInet ma³tch filter and subsequent information exchange requests by the States concerned. In this analysis we will also consider the role played by the foreseeable relevance principle in the application of the technique and discuss at what point attention should be paid to the few cases in which the receiving State is subject to the requirement of prior authorisation and, in rare cases, the sending State to the requirement of prior notification.

4.2 Technical phases related to spontaneous exchange of information

To use ma³tch in the FCInet peer-to-peer network, the competent authorities in the participating States generate their own *local filter*.[154] Next to that, each State creates its own *filter to share*. Multiple filters can be created based on the same source database. The source data is kept with the local State, and only selected data is included in the filter when creating one. The filter is not shared with the partner State until done manually by the source State, ensuring there is always human oversight. Each new filter overwrites an old one, ensuring that data never resides longer than needed. Creating and sharing a filter, followed by a verification and/or tax information request, is explained in more detail below. Figure 1 (p. 79) visualises a simplified representation of this.

4.2.1 The start-up phase

The selection of data to create the local filter

Each competent authority, usually the tax administration, selects the persons whose data will be converted to the filter. This assumes that the sending State only uses information in accordance with its domestic laws and ensures that sharing the filter to another participating State is governed by the provisions of the applicable international legal framework and domestic law regarding the exchange of information.[155] For example, filters can be created based on information from ongoing tax audits, intelligence, investigations, i.e. information that *may be able to be relevant* to a receiving State.

The selection of data to create a shareable filter

It is the sending State who must decide which data from the local filter will be processed into the shareable filter. For instance, personal data like names, dates and places of birth, addresses, bank accounts, tax number et cetera.[156] This data can relate to all

154 FCInet 2022, *User Protocol*, p. 5.

155 See FCInet 2022, *User Protocol*, p. 7 and Kroon 2021, p. 67.

156 See Geelhoed & Hoving 2021, p. 18.

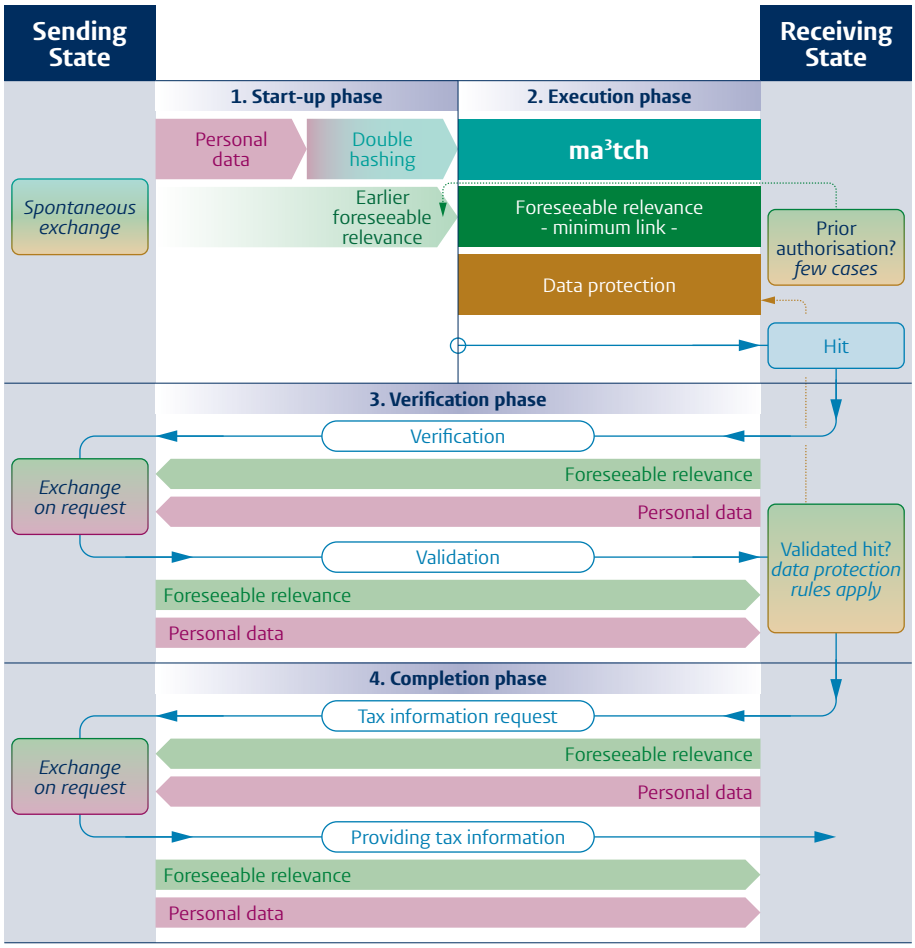


Figure 1: FCInet ma³tch technology and the standard of foreseeable relevance in privacy enhanced tax information exchange.

individuals in the local database or a selection. It is also possible to select on a specific type of crime, such as money laundering, fraud or corruption. Or by 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". Even on "non-personal data or personal data of individuals who are not (yet) regarded as suspects". Although the *User Protocol* of the FCInet ma³tch technology does not allow the creation of filters based on values of skin colour, religion, et cetera, the (unconscious) use of potentially discriminatory characteristics cannot be completely ruled out either, as the competent authority that creates the filter determines which values are used (see also Section 5.5).[157] For the time being, the ma³tch technology can only be used with structured data, e.g. personal data that is stored in a structured manner in a database.[158] Unstructured data, including personal data in documents, such as e-mails and WhatsApp files, cannot be used, however, this may be possible in the future.

157 FCInet 2022, *User Protocol*, p. 6: "On the domestic side, each participant is to decide based on its own legal framework which information is used to build a filter (as a local filter or a shareable filter), which filter is shared with which participant, which filter is updated or withdrawn, how to responded to a hit or whether and how further collaboration occurs after a hit" and p. 7: "Shareable filters are to be based on information from intelligence, signals, (preliminary) investigations or audits, etc. and all other information that is related to the participant's mission".

158 Pels Rijcken & VKA Report 2023, Sec. 6.5.

Standardisation and optimalisation of personal data

The data of a selected person will be standardised and optimised. This means, for example, putting names in the same order, formatting dates, and removing special characters. In the usual case the name in combination with the date of birth is selected. *Algorithms* are used to further standardise the data.[159] The amount and type of algorithms used is important for the degree of accuracy (see below). The standardised data is converted to (hashed) keys, aggregated and re-hashed to create the so-called ma³tch filter. The ma³tch filter itself does not reveal any sensitive information because the filter does not contain such information as a result of the hashing.[160]

Creating the ma³tch filter

A ma³tch filter contains the aggregated *characteristics of the personal data* of the selected individuals, for example, suspects of a particular crime.[161] To ensure that the data in the ma³tch filter itself cannot be reversed back to the original content of the local filter, the data is hashed twice.[162] The first time when the personal data is converted into characteristics, and a second time when the aggregated characteristics are converted into the ma³tch filter. Data that is hashed twice is considered to be *irreversible* to the individuals behind.[163] This can be detailed as follows.

Hashing uses algorithms to isolate certain characteristics, which means that personal data of an arbitrary size is converted into a series of a fixed size using a hash function.[164] A 'dynamic salt' is used to prevent unauthorised use and to make ma³tch filters domain specific (e.g. to *Civil Tax Agencies* or *LEAs*). Subsequently, a smaller hash is made from the salted hash, a so-called 'stripped hash'.[165] This stripped hash is re-hashed into a multiple 'generated numeric hashes' (i.e. *iterative hashing*). How the *numeric hashes* are generated depends largely on the precision of the matching process. For example, a filter with 3 records and an accuracy of 99% requires a hash generated from the numbers 1-29. These hashes form 'bit positions' (a series of numbers consisting of 0 and 1).

After this aggregation, it is no longer possible to determine which individual 'bit hash' belongs to which person. The filter has no link back to the original data in the local source data base. When creating the ma³tch filter, the *margin of error* is also taken into account.[166] The algorithms of the ma³tch software ensure that there is a *standard chance* of a random *false positive* hit when checking the filter. This chance has to do with the precision of the ma³tch filter. This precision can be set *high*, which means that

159 Geelhoed & Hoving 2021, p. 18.

160 FCInet 2022, *User Protocol*, p. 5.

161 Geelhoed & Hoving 2021, p. 20.

162 Geelhoed & Hoving 2021, p. 21. Balboni & Macenaite 2013, p. 333, talk about: "'hashing' the hash".

163 Geelhoed & Hoving 2021, p. 21 with reference to Balboni & Macenaite 2013, p. 337. See also Kroon 2021, p. 53-54.

164 Pels Rijcken & VKA Report 2023, Sec. 6.4.

165 Pels Rijcken & VKA Report 2023, Sec. 6.4.

166 Geelhoed & Hoving 2021, p. 21.

the chance of a random false positive hit is very low, say 1 in 10,000 (which represents a precision of 99.99%). For example, if checking 10,000 records with 99.99% accuracy yields 20 hits, statistically 1 of these hits is a false positive (5%).[167] Conversely, this also means that 95% of the hits is also a *match* after validation, and therefore the chance of a false positive is relatively small.

4.2.2 The execution phase

Sharing the filter

Via the FCInet ma³tch infrastructure a State can make its filter available to another State.[168] The State that creates the filter decides autonomously whether to share the filter or not. Important to note is that *all* connections between the States in the network are on a *bilateral* information exchange basis.[169] Within the FCInet ma³tch network, it is the sending State that always retains control over its filter, as only the sending State can *remove or update* the ma³tch filter and determine how often it is renewed.[170] The receiving State can *check* the shared filter, but never outside the context of the FCInet network. Assuming that a spontaneous provision of the ma³tch filter with data resulting from ongoing tax audits, intelligence or investigations may be *able to be of interest* for the taxation in the receiving State, the foreseeable relevance standard following from Article 26 OECD-MC is met (see also Section 2.3).

Checking the filter

After the ma³tch filter has been shared with the receiving State, it is checked with the recipient's own local dataset. Although the receiving State is bound by the selection made by the sending State, the receiving State is *not obliged to test against the same criteria*. For example, the sending State can base a filter on money laundering suspects, while the receiving State tests on, for example, suspects of fraud or corruption. In this context, it is important to note that the sharing of the ma³tch filter takes place within the tax domain and is not intended to work across-domains. Going back to the example of Italy, where the *Guardia di Finanza* acts as both a tax authority and a criminal investigative body (Section 2.1.2). This means that tax information received may immediately be used for criminal purposes, making the boundary between tax and non-tax use less distinct.

The receiving State can use the filter to check whether a person or suspect in its own database can also be found in the database of the sending State, by testing the information from its own database against the shared filter and drawing conclusions whether there is a hit or a no-hit (see below).[171] The *same algorithms* as those used by the sending State are used to transform the personal data.[172] If the sending and receiving

167 Kroon 2021, p. 51.

168 Pels Rijcken & VKA Report 2023, Sec. 6.4.

169 FCInet 2022, *User Protocol*, p. 2.

170 FCInet 2022, *User Protocol*, p. 8-9.

171 Geelhoed & Hoving 2021, p. 21.

172 Geelhoed & Hoving 2021, p. 21.

States have the same person in their database, they will have the same *characteristics*. It is important to note that the receiving State *never sees the original data* with which the ma³tch filter was created; they can only see which *readable data in their own local filter* result in a hit with the shared filter.[173]

The sending State knows that the receiving State can check the filter but does not know whether the check produces hits.[174] Checking the filter concerns a one-sided (unilateral) 'matching process', which is carried out by the receiving State. This checking can lead to two outcomes[175]:

- a *hit*, i.e. a potential match between a name of a person in the database of the receiving State and the filter made available, or
- a *no-hit*, which means that there is no common characteristics with the dataset on which the shared filter is built, at least not under the name under which the receiving State knows the person or suspect.

The meaning of a hit is no more than that it provides an *indication* to the receiving State that the sending State probably used the same personal information to build the filter as that which the receiving State has included in its local database.[176] A hit means that the data in the recipient's database is most likely also present in the database of the sending State, though there is a *chance of a false positive*, where the receiving State detects a hit, but the hit does *not concern the same individual* as included in the sending State's database, and can therefore not be validated by the sending State.

Optimising the accuracy and precision of the ma³tch filter

The chance that a hit will be a false positive decreases as the accuracy and precision of the ma³tch filter increases. The challenge for the FCInet ma³tch technology will be to optimise the algorithms so that the accuracy and precision is as high as possible. Although the chance for a random false positive can be configured, it is never zero. Therefore, the receiving State must always go back to the sending State to *verify the hit* and have it *validated*. Once validated, a relevant request for the underlying tax information can be made by the receiving State.

Special requirements in the application of the foreseeable relevance standard

The spontaneous exchange of information for tax purposes requires that the foreseeable relevance standard is at least be complied with at the time of spontaneous exchange, so at least *at the moment of sharing* the ma³tch filter. A specific *investigation or examination* of a person generally assumes a minimum of relevance, as it implies a reasonable suspicion of non-compliance with a specific legal obligation in the sending State, which may be indicative of any relevance for taxation in the receiving State. However, in the few cases where, for example, the receiving State requires *prior authorisation* from the sending State for the use of information for *non-tax purposes* or for its *disclosure to third parties*, the tax authorities in the sending State must be able to demonstrate that

173 Kroon 2021, p. 59.

174 Pels Rijcken & VKA Report 2023, Sec. 6.4.

175 Geelhoed & Hoving 2021, p. 22.

176 Geelhoed & Hoving 2021, p. 23 and FCInet 2022, *User Protocol*, p. 8.

the condition of foreseeable relevance is met at the time prior authorisation is given. The use of a so-called *whitelist* for certain high-priority cases where prior consent is given could help to address this (Section 2.1.4). For the application of FCInet ma³tch it is important to know whether such requirements apply to the participating countries in the network. Creating an oversight of such requirements with respect to the organisations participating in the FCInet ma³tch network – for which the questionnaire to identify relevant aspects for the standard of foreseeable relevance as included in Section 3.3 can be used – is therefore recommended (see also Section 6.3). Although States themselves are responsible for meeting such requirements, this will have to be taken into account when applying the ma³tch technology.

4.3 Technical phases related to information exchange on request

A hit is only an indication that the sending State probably knows the person or suspect, but that is not a guarantee. If, after checking the filter, there is a hit, it means that there *may be an actual link* between the data present in the sending State and the receiving State. This degree of relevance is sufficient to meet the foreseeable relevance threshold for the follow-up *verification request* by the receiving State; any exchange of information must comply with the foreseeable relevance standard. Although a hit may contain sufficient information to start a follow-up request for tax information by the receiving State, it can only be determined that it is *actually* the same person (match) after *verification* and *validation* of the hit.[177] In other words, if the receiving State decides on the basis of the hit alone or is obliged by (domestic) law to share this determination with third parties (for instance with the criminal law domain or with other countries), then this State still runs the risk of a false positive, even though that chance is (very) small since FCInet ma³tch strives for the highest possible accuracy and precision. This risk can be minimised by requesting validation from the sending State.

Key takeaway:

FCInet ma³tch strives for the highest possible accuracy and precision, which makes the chance of a false positive report (very) small.

4.3.1 The verification phase

Verification request

Because only the receiving State can see the hit, this State will have to verify with the sending State whether it is not a false positive. It is important to note that from the point of submission the verification request by the receiving State onwards, the regular rules around the exchange of information on request will take place and *ma³tch technology* no longer plays a role. Verification of the hit means that the receiving State checks with the sending State whether the hit between the filter and the information in its own database is accurate. Therefore, the receiving State must send a *verification request* to

177 Geelhoed & Hoving 2021, p. 23 and 28.

the sending State. Currently, the receiving State can choose to use the *FCInet network* to make a verification request, but the receiving State can also choose to use *another appropriate (traditional) channel*. The receiving State will request information on the individual to verify that the sending State does indeed know the person or suspect in question. Since there is at least a 'reasonable possibility' that the requested validation will be relevant for tax purposes in the receiving State, also at this stage of the technical operation the threshold for foreseeable relevance has been met.

The issue of a false positive

Since the chance of a false positive when applying FCInet ma³tch is quite small, the receiving State can assume with some certainty that a hit concerns the same person as in the database of the sending State. However, there are two ways to get a hit without it being the same person[178]:

> *"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 a match while this is not correct. The amount* [read: number] *of false positives that are randomly produced depends on the* [FCInet: configured precision of the filter, which is controlled by the data owner.] *(…) Secondly, a match* [read: hit] *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."*

Validation of the hit

The greater the reliability of the algorithm used to build the filter, the smaller the chance that a false positive will occur, i.e. the higher the accuracy and precision, the greater the chance that a hit will lead to validation. It is therefore important to pursue the highest possible accuracy and precision with the ma³tch technology. However, only the sending State can confirm that it is a *true hit* and use the FCInet network or another appropriate channel to validate the hit. Since it is evident that the validation will be relevant for tax purposes in the receiving State – in fact it implies actual relevance – also at this stage of the technical operation the threshold for foreseeable relevance has been met.

Pseudonymised data in retrospect

Even though the FCInet ma³tch filter consists of hashed and irreversible data, if the person behind the data can be traced after validation of a hit (and is therefore identifiable), this data should be considered pseudonymised data in retrospect (see Section 4.4.1). In the event of a validated hit, in hindsight, the *data protection rules* for the application of FCInet ma³tch must be complied with during the period in which the sharable filter is made available spontaneously.

178 Geelhoed & Hoving 2021, p. 23.

4.3.2 The completion phase

Requesting and providing tax information

After validation of the hit by the sending State, the receiving State may file a *substantive tax information request* to collect the underlying information and personal data of the taxpayer concerned.[179] Each participating State is autonomous, governed by its respective domestic law regarding exchange of information, and is in control of its decisions on whether to respond when a *match* is generated.[180] The receiving State will make this information request through its formal channels of mutual legal assistance. During this process, the sending State can check whether the request for information *adheres to its rules* before deciding to send the requested tax information. Since there is *actual relevance* between the person in question and the taxation in the requesting State, also in this stage the follow-up request meets the foreseeable relevance standard (Section 2.2). However, again, under certain circumstances, the receiving State may use it for *other than tax purposes* or provide the data received to a *third State* based on (local) legislation and/or other information-sharing tools. It should be noted that such transfers to third countries are in principle outside the scope of FCInet ma^{3}tch technology, but may have implications for *when* the foreseeable relevance principle must be met and may therefore influence how the technology needs to be designed to be effective in certain countries (see Section 4.2.2).

4.4 Assessment against the universal right to privacy and data protection

Privacy by design principles have been around since 1995, but the number of government initiatives to use PETs seems to be lagging behind.[181] The underlying reason seems to be inexperience and therefore unfamiliarity with the legal framework to be used. Ma^{3}tch technology can be used in a privacy-friendly manner to check for the presence of individuals in external sources, i.e. data collections that are not under their own control but with another competent authority. The autonomy of parties in the management of their own data collections is, however, fully maintained with ma^{3}tch. Only in the event of a hit will the receiving State consider requesting further information. To retrieve the information from the sending State, human intervention is always required. If the FCInet network is used for a verification request, instead of another channel, privacy safeguards will have to be observed here. Also, a verification request is handled in a privacy-friendly manner, so that no more individuals' data is processed than strictly necessary. Instead of providing privacy-sensitive information about an individual in the traditional way, the ma^{3}tch technology helps to spontaneously share data that *may be able to be relevant* to the receiving organisation with minimal violation of privacy and data protection rights.

179 Pels Rijcken & VKA Report 2023, Sec. 6.4.

180 FCInet 2022, *User Protocol*, p. 8.

181 See Pels Rijcken & VKA Report 2023, Sec. 3.3.

To assess whether the use of FCInet ma³tch complies with the right to privacy and data protection within the meaning of Article 17 ICCPR, Article 8 ECHR and Articles 7 and 8 of the Charter as a general framework (see Section 2.4), at least six questions will have to be answered[182]:

1. Is there any processing of personal data?
2. Do the privacy regulations apply?
3. Is the infringement provided by law?
4. Is the infringement necessary?
5. Is the infringement proportionate?
6. Is the infringement subsidiary?

We answer these questions in six steps, each of which will be explained first. This is a general assessment; applicable (treaty) provisions, local differences in interpretation and factual circumstances may lead to different outcomes. Where possible, the steps will be translated into the application of the FCInet ma³tch technology.

4.4.1 Is there any processing of personal data?

First, it must be determined whether there is a processing of personal data. To this end, it is important to assess whether the data provided through the ma³tch filter qualify as 'personal data' and whether such data are subject to 'processing'. Personal data can include any information about an *identified* or *identifiable* natural person.[183] A natural person is someone who can be identified based on, for example, a name or date of birth. Tax data, such as data on income and capital, as included in the OECD-MC, of natural persons are personal data. The processing of personal data involves, for example, the collection, recording and standardising thereof.

FCInet ma³tch uses names and, for example, dates of birth that can be used to identify natural persons. The hashing of names and dates of birth to create the ma³tch filter can be considered as an independent phase of *data processing* (start-up phase).[184] If the aggregated data should be qualified as *anonymised* data, the provision of the filter *cannot* be regarded as the processing of personal data.[185] However, if we assume that the aggregated data in the filter should be qualified as *pseudonymised* personal data, the provision of the filter as well as the comparison with a recipient's own data can be considered as an independent phase of *data processing* (execution phase).

182 See E.A.M. Huiskers-Stoop & M. Nieuweboer (2018), 'De Mandatory Disclosure-regels in het licht van het recht op privacy en de bescherming van persoonsgegevens (authors' translation: The Mandatory Disclosure rules in light of the right to privacy and the protection of personal data)', *Fiscaal tijdschrift vermogen* 2018(12): 6-17 (*FTV* 2018/45) (hereinafter: Huiskers-Stoop & Nieuweboer 2018), p. 12-15.

183 See for instance Article 4(1) EU GDPR.

184 See Pels Rijcken & VKA Report 2023, Sec. 4.

185 See Pels Rijcken & VKA Report 2023, Sec. 4.

The qualification as anonymised or pseudonymised personal data is important for the assessment of whether *personal data is processed or not*, and thus whether *privacy and data protection rules apply*. Data can be considered pseudonymised, if there is a possibility that the person behind the data can be identified in some way (*identifiable*).[186] This qualification is often related to the local legal assessment in different countries of the nature of the data. Identifiable does not necessarily mean *reversable*. Identifiable can also mean that a person is *identified indirectly*. As discussed in Section 1.6 the terms anonymised and pseudonymised are legal concepts, so their interpretation may vary from country to country. It should be noted that the qualification of the data as being pseudonymised or anonymous may vary also between the sending State and the receiving State.[187]

When applying ma^{3}tch, the receiving State does *not* gain *access to the underlying data*, as it remains solely available at the local source. Because the receiving State does not have access to this local source, it is impossible to retrieve the information used to build the filter.[188] Searching the filter by the receiving organisation will not disclose personal data, as the data made available is not only an *aggregation of compressed non-reversible double hashed data*, but the underlying personal data is at the *local source*. In principle, there is no way to trace back to the original dataset, and it should therefore be considered *irreversible*.

However, after validation of a hit, it should be stated *afterwards* that the data shared by the filter has *identified* the individual behind it. So initially, when the filter was generated, personal data is converted into *hashed* data – and even if this could be classified as anonymous within the ma^{3}tch technology (Balboni & Macenaite 2013) – the person behind the data can still be identified *indirectly* after validation of the hit. The person behind the initially 'anonymised' hashed data is still matched via the system. In our opinion, therefore, the hashed data in the filter should be regarded as *pseudonymised data*. Although the data in the filter *cannot* be traced back to the original content of the filter, it can be traced back indirectly to the *individual* behind.

186 See Pels Rijcken & VKA Report 2023, Sec. 8.18.

187 See Case T-557/20, *SRB/EDPS*, 26 April 3023, ECLI:EU:T:2023:219, at 76-83. For a further discussion on the qualification, please refer to Geelhoed & Hoving 2021, p. 26-27 with reference to Balboni & Macenaite 2013, p. 334-338. According to Geelhoed & Hoving conclude Balboni & Macenaite on the one hand "that it is unlikely that a motivated intruder can re-identify the individuals on which the filter was based". Geelhoed & Hoving conclude on the other hand: "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".

188 FCInet 2022, *User Protocol*, p. 6.

Data that directly or indirectly identify an individual, should in our view be considered personal data for tax information exchange purposes.[189] The distinction between anonymous data and personal data depends on the *possible connection to an identified or identifiable individual*, whereby "the test of identifiability is a dynamic one and should consider the state-of-the-art in technology at the time of the processing".[190] Although Balboni and Macenaite argued in 2013 that as long as the data in the filter cannot be traced back to the original content, the data qualifies as anonymous and the data protection rules do not apply, we believe that a *match* in retrospect involved the *provision of identifiable personal data*.

4.4.2 Do the privacy regulations apply?

Although the FCInet ma^{3}tch filter contains an aggregation of compressed non-reversible double hashed personal data and this hashed data cannot be traced back to the data in the local database of the sending State directly, the receiving State can determine whether there is a 'hit' between the filter and its own database, which can be validated by the sending State as belonging to a specific person. In the event of a *no-hit*, it can be stated that only *anonymised* hashed data has been processed to the receiving State, while personal data remained with the sending State. After a hit between the filter and the receiving State's own database, the receiving State starts *processing personal data* by verifying the hit with the sending State. In response, the sending State will start *processing personal data* by validating the hit. The verification phase therefore involves the processing of personal data and both States must take into account an infringement of the privacy of the person concerned, for which the exchange for the purpose of achieving proper taxation will generally be considered the justification.

In case of a verified match between the shared filter and the receiving State's database, it could be stated that the validation by the sending State *confirms afterwards* that *pseudonymised data* has been sent through the filter from the sending State to the receiving State.[191] In our opinion, in the event of a match, in hindsight, privacy

189 Balboni & Macenaite 2013, p. 334: "(…) any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

190 Balboni & Macenaite 2013, p. 335: "A natural person can be 'identified' when, within a group of persons, he or she is 'distinguished' from all other members of the group. When the identification has not taken place, but it is possible to do so, the individual is 'identifiable'", and p. 336: "Data are considered anonymous when an unreasonable effort (amount of time and manpower) is required to (re)turn the data into personally identifiable data. In other words, the likelihood of making a connection between data and a data subject is measured in relation to the time, cost and technical means necessary to do so".

191 Geelhoed & Hoving 2021, p. 29.

and data protection rules apply as from the time the filter was made available.[192] In fact, this only applies to the pseudonymised data that ultimately leads to a match. Because it seems impossible to select the data in the filter accordingly, privacy and data protection rules *should be considered to apply* to the provision of the filter. Only if no hit results from the provision of the filter, it can be said that privacy and data protection rules did not apply from a preliminary point of view.

Suppose that the data in the filter should be qualified as pseudonymised data. An advantage of using FCInet ma^{3}tch compared to traditional methods, is that the pseudonymisation of the personal data limits the breach of privacy or potentially avoids any breach at all. Given that privacy regulations apply to the processing of the filter, it is important that the data be *protected as part of private life* within the meaning of the framework we have determined based on Article 17 of the ICCPR, Article 8 of the ECHR and Articles 7 and 8 of the Charter and further elaboration in the EU GDPR. The term privacy should be judged by the circumstances and interpreted broadly.[193] The regular collection and processing of (tax) personal data in the ma^{3}tch filter (start-up phase), the provision of pseudonymised data through the ma^{3}tch filter (execution phase), the validation of a hit (verification phase) and the fulfilment of a tax information request (completion phase) constitute an interference in the private life of taxpayers by the sending State. The information provided for the request for verification as well as the information provided for the validation itself (verification phase) constitute an interference with the private life of the taxpayers. The information provided for the request for tax information and the submission of this tax information itself (completion phase) also constitute an interference with the private life of the taxpayers. Here too, the exchange for the purpose of achieving proper taxation will serve as a justification.

Key takeaway:

In the event of a validated hit, in hindsight, the data protection rules for the application of FCInet ma^{3}tch must be complied with during the period in which the sharable filter is made available spontaneously.

192 See in this respect EU GDPR 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".

193 See ECHR 4 December 2008, *S. and Marper v. United Kingdom*, ECLI:CE:ECHR:2008:1204JUD003056204 and ECHR 16 February 2000, *Amann v. Switzerland*, ECLI:CE:ECHR:2000:0216 JUD002779895.

4.4.3 Is the infringement provided by law?

The third question to be answered is whether the interference with private life is regulated by law that provides sufficient safeguards to ensure a careful weighing of interests.[194] For example, the law must be sufficiently *accessible* to those involved.[195] The legislation must also be foreseeable, which means that the legislature must have expressly intended the infringement. This means that the law must be *sufficiently clear* so that the person concerned has insight into the circumstances and conditions under which the government is authorised to breach on his or her private life and what the consequences are.[196] In answering the question of whether legislation is sufficiently accessible and clear, the way in which the information is *processed* and who has *access* to the data may also be important.[197] If there is virtually unlimited access to the data or if the data is stored systematically, additional safeguards may be required. New techniques make it possible to collect large amounts of information and store it for years. To determine whether certain obligations (still) have a sufficient legal basis for a breach of privacy, technological and social developments must also be taken into account. Furthermore, the purposes and conditions under which the data are processed must be *specified*. The legislation must also contain sufficient safeguards to *prevent arbitrariness and abuse*, for example regarding retention periods, access and security.[198] A *legitimate aim* must also be formulated, for example the prevention of tax evasion.

The safeguards to prevent arbitrariness and abuse are often left to the States themselves. This is problematic if the instruments of exchange and local legislation allow information and documents to be used for *non-tax purposes* and, moreover, to be submitted to third countries. A taxpayer whose rights have been violated in this regard is expected to have to invoke the *local protection rules*, which may be lacking.[199]

The use of FCInet ma^{3}tch is considered to involve data processing in the execution phase, i.e. while sharing the filter. In addition, both the sending State (in the start-up, the verification and the completion phase) and the receiving State (in the verification and the completion phase) have to do with the processing of personal data. This processing

194 ECHR 12 January 2010, *Gillan and Quinton v. United Kingdom*, ECLI:CE:ECHR:2010:0112JUD000415805, at 77.

195 ECHR 12 May 2000, *Khan v. United Kingdom*, ECLI:CE:ECHR:2000:0512JUD003539497.

196 ECHR 2 August 1984, *Malone v. England*, ECLI:CE:ECHR:1984:0802JUD000869179.

197 CJEU 8 April 2014, *Digital Rights v. Ireland*, Cases 293/12 and 594/12, ECLI:EU:C:2014:238: In the light of the aim of Directive 2006/24 on the storage of telecommunications data for the purposes of the prevention and prosecution of criminal offences, the use of electronic communications is "a valuable tool in the prevention of offences and the fight against crime" and "genuinely satisfies an objective of general interest". However, the Directive seeks to constitute a far-reaching and particularly serious interference with fundamental rights, while failing to lay down sufficient safeguards, as required by Articles 7 and 8 of the Charter, to ensure "effective protection of retained data against the risk of abuse and against any unlawful access to and use of such data".

198 ECHR 1 July 2008, *Liberty et al. v. United Kingdom*, ECLI:CE:ECHR:2008:0701JUD005824300 and ECHR 29 June 2006, *Weber and Saravia v. Germany*, ECLI:CE:ECHR:2006:0629JUD005493400.

199 Boei & Van Dam 2022.

of personal data is *only permitted* insofar as such processing can be based on a *legal basis*. Generally, the competency to levy taxes or to initiate a criminal investigation is regarded as a sufficient legal basis to breach the right to privacy and data protection for a specific domain, i.e. tax or criminal domain (Article 8 ECHR).

Key takeaway:

Both the spontaneous exchanges within the FCInet ma³tch technology and exchanges on request through the FCInet network in the verification and completion phase – if of course applicable since other appropriate channels can be used as well – are legally based. However, this does not mean that a legal basis for one domain, for instance for the criminal domain, is also a legal basis for another domain, for instance the tax domain. Moreover, the exchange from one domain to another must also be based on a legal authority.

As an example of a case in which the legal basis for (a cross-domain) exchange of information was lacking, we refer to the *Automatic Number Plate Recognition* (ANPR) case, in which the Dutch tax inspector used camera images – taken by cameras hanging above public roads – made by the Dutch National Police to apply tax corrections for private use of a company car, without there being an *independent tax legal basis* for this.[200] Following this case, the Dutch legislator subsequently created a legal tax basis to use camera images to make such corrections. Information about applicable rules in this context is often only available locally.

4.4.4 Is the infringement necessary?

In addition, the question must be answered whether interference in private life is necessary in a democratic society. To that end, it is important to determine whether the interference is in the interest of, for example, the economic well-being of a country.[201] Interference is necessary when there is an urgent social need. Violation of privacy is therefore almost always necessary in a democratic society. In view of Article 1 of Protocol No 1 to the ECHR, the payment of taxes is deemed to serve the public interest and a (European) State has far-reaching rights to achieve that objective, even if this requires a violation of the right to privacy and data protection under Article 8 ECHR. Article 17 ICCPR has a similar scope. The violation, however, must be limited

200 Dutch Supreme Court 24 February 2017, ECLI:NL:HR:2017:286: Article 8 of the ECHR provides that interference by any public authority is permitted only to the extent provided for by law and is necessary in the interests of security, economic well-being, the prevention of disorder or crime, or the protection of the health, morals or rights and freedoms of others.

201 CJEU 9 November 2010, *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen*, Cases 92/09 and 93/09, ECLI:EU:C:2010:662, at 77.

to what is strictly necessary.[202] The question of whether the interference is necessary must therefore also be determined based on the requirements of *proportionality* and *subsidiarity* to be discussed under steps 5 and 6.

4.4.5 Is the infringement proportionate?

To answer the question whether the interference in private life is proportionate, it is important to assess whether the violation is proportionate *to the aim pursued*. For example, in the light of increasing international cooperation in the fight against tax avoidance, the spontaneous provision of information to a tax authority of another State seems to be justified. In the case of the provision of the ma^{3}tch filter with aggregated and double hashed data, an assessment must be made of whether the processing of the – with hindsight pseudonymised – data are proportionate to the purpose intended by the regulation on exchange of tax information. The main objective of the exchange of information regulation is combating of tax fraud, corruption, money laundering, terrorism financing and other (tax) crime. The implicit sub-goals of the spontaneous exchange are, among others, to allow other tax authorities to obtain information that they would otherwise not be able to obtain or would be very difficult to obtain, to speed up the exchange of information and to limit it to necessary information, et cetera. Similar to the objective of information exchange instruments, such as Article 26 of the OECD-MC, FCInet ma^{3}tch aims to assist other States in achieving proper taxation, to prevent bulk requests and limit further investigation to cases where there is a 'match' between a person in the database of the sending State and the database of the receiving State. When it comes to combating tax fraud, a breach of privacy or data protection such as in the application of FCInet ma^{3}tch is generally accepted as proportionate.

4.4.6 Is the infringement subsidiary?

To answer the question whether the interference with private life is subsidiary, it is important to establish that the purpose for which the data are processed cannot reasonably be achieved in any other way, which is *less detrimental* (i.e. less infringing) to the person concerned by the processing of personal data.

There is no doubt that a spontaneous provision of the ma^{3}tch filter contributes to improving the *effectiveness and efficiency* of taxation by the receiving tax authorities. In doing so, there must be a balance between, on the one hand, the processing of pseudonymised data and, on the other hand, the possibility for tax authorities to become aware of tax-relevant data that would otherwise not be obtainable or would be difficult to obtain in the traditional way. Since the processed data is minimised, aggregated and double hashed, the breach of the protection of personal data is minimal, while, as far as we can see, there is no less disadvantageous way to obtain the information, since the

202 CJEU 11 December 2014, *Ryneš*, Case 212/13, ECLI:EU:C:2014:2428, at 28: "In that connection, it should be noted that, according to settled case-law, the protection of the fundamental right to private life guaranteed under Article 7 of the Charter of Fundamental Rights of the European Union ('the Charter') requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (…)".

exchange in the traditional way has a greater impact on privacy because more visible personal data is exchanged.

Key takeaway:

Although the infringement of privacy and data protection rules by the application of FCInet ma³tch is minimal, the foreseeable relevance principle must be complied with for the legality of this and it is therefore important for the application of FCInet ma³tch to know whether rules like prior authorisation (or prior notification) apply to countries – more specifically for the countries that participate or want to participate in FCInet ma³tch.

4.5 Additional assessment against the EU GDPR

Since the introduction of the EU GDPR in 2018, local European laws and regulations on the processing of personal data must also comply with the additional requirements for the protection of personal data contained therein.[203] The EU GDPR does not apply if personal data is anonymised, because anonymous data does not qualify as personal data. However, the EU GDPR does apply to pseudonymised data, because it qualifies as personal data.

It is important to note that even if the data provided through the filter should be considered anonymous data, this does not mean that the foreseeable relevance standard of Article 26 OECD-MC does not apply to the spontaneous exchange of the filter.[204] In this case, compliance with the foreseeable relevance standard is not a condition for the lawfulness of a possible *infringement of the right to privacy and the protection of personal data*, but for the lawfulness of the *spontaneous exchange of information* itself.

To the extent that Union law applies, the following additional three questions follow from the EU GDPR[205]:

7. Is the data processed in a lawful, fair and transparent manner?
8. Have the data been collected for specified, explicit and legitimate purposes?
9. Is the right of access to and rectification of the personal data provided?

203 For an analysis of the protection of privacy rights in EU law, see F. Debelva, 'The impact of the right to privacy and nemo tenetur on tax information exchange', in: M. Serrat Romaní, J. Korving & M. Eliantonio (red.), *Exchange of Information in the EU*, Cheltenham: Edward Elgar Publishing (2024): 67-84 (hereinafter: Debelva 2024).

204 This is contrary to FCInet 2022, *User Protocol*, p. 5: "The sender does not send any protected or sensitive information, because a filter does not contain any, and thus the question of foreseeable relevance does not arise."

205 Huiskers-Stoop & Nieuweboer 2018, p. 15-16.

If FCInet's activities fall within the scope of the EU GDPR, the operation must be set up in such a way that it complies with these provisions. We will discuss these three provisions below. Where possible, the steps will be translated into the application of the FCInet ma^{3}tch technology.

4.5.1 Is the data processed in a lawful, fair and transparent manner?

According to the EU GDPR personal data must be processed in a manner that is lawful, fair and transparent with regard to the data subject, for instance a taxpayer.[206] Any processing of personal data must be lawful and fair.[207] In addition, it must be transparent to individuals that their personal data is collected, used, accessed or otherwise processed and to what extent. Besides, information and communication related to the processing of personal data should be easily accessible and understandable and clear language should be used.[208] In view of Article 6 of the EU GDPR, the processing of personal data is *presumed to be lawful*, among others, if a person has given consent to its processing[209], if the processing is necessary for compliance with a legal obligation or if it is necessary for the performance of a public-law task. In cross-border cases within the EU Article 6 of the EU GDPR provides for a legal basis.

Pursuant to Article 23 of the EU GDPR, it is possible to restrict the right of information of individuals and the right of access. The most far-reaching restriction is the full *right of cancellation* of individuals. In general, the EU GDPR allows for limitations in the scope of the rights of individuals, to the extent that they are necessary to safeguard, among others, important public interest objectives of the Union or of a Member State, including tax matters.[210] While the EU GDPR aims to establish common rules for the exchange of tax information, it leaves room for the Member States to decide on the limitation of the rights of individuals.

Given the condition of lawful, fair and transparent data processing, the organisation of data processing must be adapted to the rights of individuals. For the application of FCInet ma^{3}tch it must be taken into account, as discussed, that although hashed data is made available via the filter, this data must still be classified as pseudonymised data after validation of a hit and data protection safeguards subsequently apply (Section 4.4.1), which must therefore be taken into account in the technical and organisational set-up. However, since the processed data is already minimised, aggregated and double hashed, the breach of privacy in the processing of personal data can be considered *minimal*, so that the technical and organisational aspects already seem to be in order.

206 Article 5(1)(a) EU GDPR.

207 EU GDPR, Preliminary consideration 39.

208 Huiskers-Stoop & Nieuweboer 2018, p. 15.

209 Article 7 EU GDPR.

210 Article 23(1) EU GDPR.

4.5.2 Have data been collected for specified, explicit and legitimate purposes?

According to the EU GDPR, the personal data may only be collected for specified, explicit legitimate purposes and may not be further processed in a manner incompatible with those purposes.[211] Further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be considered incompatible with the original purposes.[212] However, every person should have the right to know and be informed of the purposes for which personal data are processed, if possible, for how long they are stored, who receives the personal data and the consequences of such processing.[213] Furthermore, the EU GDPR contains provisions on data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.[214] Appropriate technical and organisational measures must ensure that only data that is necessary for the processing is carried out for each specific stage of the processing. The principle of necessity is expressed, among others, in[215]:

- the amount of personal data collected (i.e. *as little as possible*);
- the extent to which they are processed (i.e. *the less often, the better*);
- the period for which they are stored (i.e. *the shorter, the better*), and;
- its accessibility (i.e. *the fewer people have access, the better*).

Since the data processed through the ma³tch filter is minimised, aggregated and double hashed and it is the source State that determines which data the filter is built with, to which State a filter is made available and when the data in the filter is renewed, the source State retains control over the data made available and additional tax information is only provided upon request by the receiving State after a validated hit.

4.5.3 Is the right of access to and rectification of the personal data provided?

Finally, the right of access to and rectification of data relating to the personal data provided must be safeguarded.[216] To that end, it is important to establish that a taxpayer has access to the data collected about him or her and that it is possible to rectify the collected data.[217] Individuals have the right to access and correct and, in a few countries, to object to the processing of personal data (in the rare case of prior notification).[218] Individuals also have the right to be 'forgotten', which means that they must be able to have all personal data erased under certain circumstances.[219] When applying the FCInet ma³tch technology the owner of the local filter is the designated organisation

211 Article 5(1)(b) EU GDPR.

212 Article 89(1) EU GDPR.

213 EU GDPR, Preliminary consideration 63.

214 See Articles 5(1)(c) to (f) and Article 5(2) EU GDPR.

215 See Pels Rijcken & VKA Report 2023, Sec. 8.9.

216 Article 8(2) Charter.

217 See CJEU 13 May 2014, *Google Spain*, Case 131/12, ECLI:EU:C:2014:317, at 72.

218 Article 15, 16, 19 and 21 EU GDPR.

219 Article 17 and 19 EU GDPR.

to provide access, to rectify or to remove inaccurate personal data before building and sharing the filter. This is beyond the scope of the FCInet ma³tch technology.

Key takeaway:

The application of FCInet ma³tch operates within the boundaries of existing international legal frameworks and does not impose additional obligations on participating States. Although the technology uses double-hashed data, privacy and data protection rules become relevant if a hit is identified and validated. Each phase of the process, from data preparation to verification, may constitute an interference with privacy, but is generally considered proportionate given the public interest in effective tax enforcement. The design of ma³tch limits data exposure and supports compliance with legal standards. As such, its use aligns with the foreseeable relevance requirement and respects data protection principles.

4.6 Preliminary conclusion

FCInet aims to eliminate as many hurdles as possible to facilitate the smooth and effective exchange of information between countries, making it more attractive and lowering the threshold for countries to join an exchange of information network. The matching process does not commence with the establishment of a local filter, but only when a State decides to share a filter. Every State will have its own local filter, and they can choose to connect with other States that also use FCInet. From the point of submission the verification request onwards after a hit, the regular legal rules around the exchange of information on request will take place and ma³tch technology no longer plays a role.

Although ma³tch contains an aggregation of compressed non-reversible double hashed data and this data cannot be traced back to the personal data in the local filter of the sending State directly, the receiving State can determine whether there is a 'hit' between the filter and its own database, which can be validated by the sending State as belonging to a specific person. The terms 'anonymised' and 'pseudonymised' are legal concepts, so their interpretation may vary from country to country. In the event of a verified match between the filters and the receiving State's database, it can be argued that the validation by the sending State subsequently confirms that pseudonymised personal data has been sent through the filter from the sending State to the receiving State. In our opinion, in the event of a match, in hindsight, privacy and data protection rules apply while sharing the filter. In fact, this only applies to the pseudonymised data that ultimately leads to a match. Since it is impossible to select the data in the filter accordingly, privacy and data protection rules should be considered to apply to the provision of the filter. Only if no match results from the provision of the filter, it can be said that privacy and data protection rules did not apply from a preliminary point of view.

The regular collection and processing of personal data in the ma³tch filter (start-up phase), the provision of pseudonymised data through the ma³tch filter (execution phase), the validation of a hit (verification phase) and the fulfilment of an information request (completion phase) constitute an interference in the private life of taxpayers by the *sending* State. The information provided for the request for verification as well as the request for tax information constitute an interference with the private life of the taxpayers by the *receiving* State. However, in view of Article 1 of Protocol No 1 to the ECHR, the payment of taxes is deemed to serve the public interest and a (European) State has far-reaching rights to achieve that objective, even if this requires an interference with the right to privacy and data protection under Article 8 ECHR. Article 17 ICCPR has a similar scope. For tax purposes, a breach is generally considered as justified.

To answer the sub-question *whether the way in which FCInet ma³tch is applied, influences the assessment of whether the foreseeable relevance requirement is met*, we have tested the technical operation of FCInet ma³tch against data protection requirements and assessed whether the foreseeable relevance threshold is still met. Table 3 (overleaf) shows the technical phases of FCInet ma³tch in the light of personal data protection and the foreseeable relevance threshold.

The table shows, among other things, that the spontaneous provision of data resulting from an examination or investigation shall be deemed to be relevant to taxation in the receiving State provided that there is a *minimal link* (minimal nexus) between the information and the taxation in that country. Consequently, it can be assumed that the standard of foreseeable relevance, as laid down in Article 26 of the OECD-MC, is met. Since information must be exchanged between countries to the 'widest extent possible', a link can easily be assumed. If, after checking the filter, there is a hit, it means that there may be an actual link between the data present in the sending organisation and the receiving organisation. This means that in this phase of the technical operation, the foreseeable relevance standard for the exchange of information on request has also been met. After a hit has been determined, the sending State must validate the hit to determine that it is a match. Only after verification and validation of the hit can the actual relevance of the exchanged information – both in spontaneous information exhange and in exchange on request – be confirmed. However, actual relevance is not a requirement to meet the foreseeable relevance threshold.

There is no doubt that a spontaneous provision of the filter contributes to improving the effectiveness and efficiency of taxation by the receiving tax authorities. In doing so, there must be a balance between, on the one hand, the processing of pseudonymised data and, on the other hand, the possibility for tax authorities to become aware of tax-relevant data that would otherwise not be obtainable or would be very difficult to obtain in the traditional way. Since the processed data is minimised, aggregated and double hashed, the breach of the protection of personal data is minimal, while, as far as we can see, there is no less disadvantageous way to obtain the information.

Table 3: Technical phases of FCInet ma³tch in the light of personal data protection and the foreseeable relevance standard

FCInet ma³tch technology	Four technical phases			
Sending State	**1. Start-up**	**2. Execution**	**3. Verification**	**4. Completion**
Selection of personal information	Selection of *structured* personal data			
Standardisation and optimalisation of selected data	Basically the *name* and *date of birth* are used			
Processing the data	Data are *aggregated compressed* and *double hashed* and cannot be traced back			
Creating the ma³tch filter	The filter with aggregated compressed double hashed data has *no link back* to the original data in the source data base			
Spontaneous Exchange	**1. Start-up**	**2. Execution**	**3. Verification**	**4. Completion**
Sharing the ma³tch filter		• This is the start of the spontaneous exchange of information • If the data in the filter *may be able to be of interest* the foreseeable relevance standard is met		
Receiving State	**1. Start-up**	**2. Execution**	**3. Verification**	**4. Completion**
Checking the ma³tch filter		• The sending organisation is *not aware* that the filter is *being queried* by the receiving organisation • *Human intervention* by the receiving organisation is required to judge if there is a hit		
Exchange on request	**1. Start-up**	**2. Execution**	**3. Verification**	**4. Completion**
Verification of a hit (request for information)			• A hit means: there *may be an actual link* between the data present in the sending organisation and the receiving organisation • Verification of the hit means the start of exchange of information *on request* and the processing of personal data by the receiving organisation	
Sending State	**1. Start-up**	**2. Execution**	**3. Verification**	**4. Completion**
Validation of the hit (response to request)			• Validation of the hit means: there is an *actual link*, and processing of personal data by the sending organisation • Actual link is, however, *no requirement* to meet the foreseeable relevance standard	

FCInet ma³tch technology	Four technical phases			
Receiving State	**1. Start-up**	**2. Execution**	**3. Verification**	**4. Completion**
Tax information request after validation of a hit				Regular rules of information exchange *upon request* apply
Sending State	**1. Start-up**	**2. Execution**	**3. Verification**	**4. Completion**
Tax information provision after validation of a hit				Regular rules of information exchange *upon request* apply
Assessment of the right to privacy and data protection	**1. Start-up**	**2. Execution**	**3. Verification**	**4. Completion**
Is there personal data processing?	Yes	• In case of *anonymised* data: no • In case of *pseudonymised* data: yes	Yes, from the point of hit verification onwards	Yes, in case of requesting and providing tax information
Do privacy rules apply?	Yes	In case of pseudonymised data: yes	Yes	Yes
Is the infringement provided by law?	• An infringement by the competent authorities must have a *legal basis* • The competency to *levy taxes* or to initiate a criminal *investigation* is generally regarded as a sufficient legal basis	• An infringement by the competent authorities must have a *legal basis* • The competency to *levy taxes* or to initiate a criminal *investigation* is generally regarded as a sufficient legal basis • Foreseeable relevance: 'may be able to be of interest' is *prerequisite* for 'lawfulness' under spontaneous exchange for data protection rights	• An infringement by the competent authorities must have a *legal basis* • The competency to *levy taxes* or to initiate a criminal *investigation* is generally regarded as a sufficient legal basis • Foreseeable relevance: 'may be an actual link' is *prerequisite* for 'lawfulness' under exchange on request for data protection rights	• An infringement by the competent authorities must have a *legal basis* • The competency to *levy taxes* or to initiate a criminal *investigation* is generally regarded as a sufficient legal basis • Foreseeable relevance: 'actual link' is *no prerequisite* for 'lawfulness' under exchange on request for data protection rights, 'may be an actual link' is sufficient
Is the infringement [...]?	**1. Start-up**	**2. Execution**	**3. Verification**	**4. Completion**
Proportionate?	It is proportionate to the aim of *combating tax fraud*	It is proportionate to the aim of *combating tax fraud*	It is proportionate to the aim of *combating tax fraud*	It is proportionate to the aim of *combating tax fraud*
Subsidiary?	There is an alternative in traditional exchange, but that is *'no less infringing'*	There is an alternative in traditional exchange, but that is *'no less infringing'*, since personal data are processed aggregated compressed and double hashed	There is *no (less infringing) alternative* to verify and validate a hit than filing a request	There is *no (less infringing) alternative* than filing a request based on an actual link between data in the sending and receiving organisation
Additional assessment to EU GDPR data protection rules	**1. Start-up**	**2. Execution**	**3. Verification**	**4. Completion**
Is the data processed in a lawful, fair and transparent manner?	• Regular legal rules apply • Guidance in *User Protocol*	• Regular legal rules apply • Minimal breach, if any	• Regular legal rules apply • Via FCInet network or another appropriate (traditional) channel	• Regular legal rules apply • Via appropriate (traditional) channel
Have data been collected for specified, explicit and legitimate purposes?	• Collection and processing in connection with the public-law task (taxation)	• Collection and processing in connection with the public-law task (taxation)	• Collection and processing in connection with the public-law task (taxation)	• Collection and processing in connection with the public-law task (taxation)
Is the right of access and rectification of the personal data provided?	• Regular legal rules apply • Sending State retains control over (tax) data	• Regular legal rules apply	• Regular legal rules apply	• Regular legal rules apply

Chapter 5

Interdisciplinary reflections from a criminal law perspective

In view of the increasing globalisation of economic relations, transnational tax and other financial crimes, States have an increasing need for the reciprocal provision of information on the basis of which national tax and criminal law should be applied and/or enforced.[220] FCInet especially plays an important role in the stadium of the *pre-inquiry/detection phase*. Information gathered in administrative investigations, such as tax investigations, may be used for criminal investigations too and may even enter case files in criminal proceedings. Moreover, administrative proceedings based on tax investigations may culminate themselves in sanctions that are criminal in nature, following the so-called *Engel/Bonda*[221] criteria.

As mentioned in Chapter 1, the concept of foreseeable relevance, analysed in Chapter 2, is not used as such in criminal law legal instruments. There are, however, other, comparable requirements to be met for the exchange of information in criminal matters. Therefore, this Chapter intends to establish what criteria for the exchange of information are applicable in criminal law matters and subsequently assesses how those requirements relate to the foreseeable relevance principle. The following question will be answered: *how does the concept of foreseeable relevance compare to requirements for information exchange in criminal proceedings?* Sub-questions in this context are: what issues may this create from a criminal law perspective given that information gathered by tax authorities often is admitted as evidence in criminal proceedings?

To address these questions, the applicable legal instruments for the exchange of information in criminal matters will be discussed (Sections 5.1 and 5.2) and the requirements comparable to that of foreseeable relevance will be examined (Section 5.3). Further, this Chapter evaluates to what extent the ma^{3}tch technology, if applied to criminal investigations, has the potential to affect individual rights, including the right to privacy and data protection, and other balances necessary in criminal law dynamics (Sections 5.4 and 5.5).

5.1 Examinations and investigations in criminal matters

In the context of this research, we understand criminal investigations of tax fraud as those investigations against tax offences that are classified as criminally relevant by criminal laws applicable at a national level. While national legislations are not identical and may present differences in terms of what specific conduct falls under the definition of tax fraud, one can generally include the act of wilfully and intentionally falsifying

220 FCInet 2022, p. 1.

221 ECHR 8 June 1976, *Engel and others v. the Netherlands*, ECLI:CE:ECHR:1976:0608JUD000510071; CJEU 5 June 2012, *Bonda*, Case 489/10, ECLI:EU:C:2012:319. In these cases, the Court sets out the criteria for defining the criminal nature of a penalty.

or withholding information on a tax return to avoid paying taxes under the concept of tax fraud. Such investigations have the goal to gather information and evidence to be used to formalise an accusation and, in case, to prosecute the case in front of a judge competent in criminal matters.

To note and as mentioned in Chapter 3, national legal systems may differ regarding in the way they distinguish between the (administrative) tax domain is separated and the criminal domain. Depending on the jurisdiction, tax fraud investigations are carried out by *LEAs* and the *public prosecution service* or by an *administrative authority* competent not only for supervising taxpayers, but also to investigate offences, whether of an administrative or criminal in nature.

This is the case, for instance, in the Netherlands where the Fiscal Intelligence and Investigation Service (*Fiscale inlichtingen- en opsporingsdienst*, hereinafter: FIOD) is competent to investigate financial crimes.[222] Similarly, in Germany, tax fraud investigations are undertaken by the tax authority (*Finanzamt für Steuerstrafsachen und Steuerfahndung*). Although such tax authority is an administrative authority within the province of the executive, for this kind of offence it assumes the powers and responsibilities of the public prosecution service, including investigation and prosecution.

This shows, once more, how the matter of tax investigations straddles the fields of administrative law and of criminal law. As mentioned above, this is suggested already by the criminal nature of the sanctions that may be imposed (even where proceedings are formally administrative), and by the possible transfer of evidence and reports from an administrative investigation into the case file of the criminal investigation. Moreover, it appears that the connection between these two fields is emphasised by the fact that in various jurisdictions, such as the Netherlands and Germany, fraud investigations are carried out by one and the same authority, regardless of whether the investigation has an administrative or criminal nature.

With this in mind, the analysis included in this Chapter intends to give an overview of the legal instruments that may be relied upon to share information in criminal investigations for tax fraud. The Chapter aims at assessing the requirements of information sharing in criminal investigations set out in these legal instruments to allow for a comparison with the foreseeable relevance principle. Considering also the applicable data protection provisions, the possible impact of applying the ma^{3}tch technology to information sharing in criminal (tax) investigations is evaluated too (Section 5.5).

222 The FIOD is a governmental agency that is part of the Dutch *Tax and Customs Administration*, which in turn is under the responsibility of the Dutch *Ministry of Finance*.

5.2 Legal instruments governing the cross-border exchange of information

In the field of judicial cooperation in criminal matters the last decades have seen the adoption of supranational legal instruments that entail provisions regarding both the information exchange on request and the spontaneous exchange of information. Instruments to be mentioned, in this regard, include the CoE Conventions on Laundering, Search, Seizure and Confiscation of Proceeds from Crime;[223] the CoE Criminal Law Convention on Corruption;[224] and the CoE Convention on Cybercrime.[225] Furthermore, at an international level, the UN Convention against Transnational Organised Crime[226] and the Protocols supplementing this Convention equally contain provisions on the exchange of information.[227]

While these instruments introduce the exchange of information (with and/or without prior request) as a cooperation tool to counter the specific categories of offences covered by them, there are also generally applicable instruments – adopted by the CoE by the EU legislator and, beyond that, among the governments of several American countries – that may be relied on to tackle cross-border crime. These are also applicable to investigations against tax fraud and form, thus, the focal point of this analysis. As mentioned in the introduction (Chapter 1), even considering just the generally applicable cooperation instruments, there is a multitude of legal instruments with varying scopes of application. A more detailed discussion of the respective scopes of application is included in Annex 2.

A first distinction in this regard must be made between instruments enabling cooperation (including the exchange of information) among judicial authorities, on the one hand, and among LEAs, on the other: instruments of judicial cooperation versus instruments of police cooperation.

223 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (adopted 8 November 1990, entered into force 1 September 1993) 141 ETS 1 (hereinafter: 1990 Strasbourg Convention); CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (adopted 16 May 2005, entered into force 1 May 2008) 198 ETS 1 (hereinafter: 2005 Warsaw Convention).

224 Criminal Law Convention on Corruption (adopted 27 January 2005, entered into force 1 July 2002) 173 ETS 1 (hereinafter: Convention on Corruption).

225 Convention on Cybercrime (adopted 23 November 2001, entered into force 01 July 2004) 185 ETS 1 (hereinafter: Budapest Convention).

226 UN Convention against Transnational Organized Crime (adopted 15 November 2000, entered into force 29 September 2003) 2225 UNTS 209 (hereinafter: 2000 Palermo Convention).

227 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the UN Convention against Transnational Organized Crime (adopted 15 November 2000, entered into force 25 December 2003) 2237 UNTS 319; Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the UN Convention against Transnational Organized Crime (adopted 15 November 2000, entered into force 28 January 2004) 2241 UNTS 480.

5.2.1 Judicial versus police cooperation

Police cooperation includes all kinds of cooperation between national police forces for which the use of coercive measures is not needed.[228] Judicial cooperation, on the other hand, refers to the cooperation between national judicial authorities such as judges, courts, investigating judges and public prosecutors, as well as customs authorities and other specialised LEAs.

Judicial cooperation may require the deployment of police officers but qualifies as judicial cooperation because it involves the use of coercive measures that can only be applied under the authority of prosecutors, investigative judges, et cetera. Some modalities of cooperation are exclusive either to police cooperation or to judicial cooperation. For instance, cross-border pursuit can only be performed by police authorities. Conversely, a transfer of a judgement will take place at judicial level without involving the police. As far as the exchange of information is concerned, however, this can occur both between police authorities and between judicial authorities.[229]

Whether the exchange of information occurs through police cooperation or through judicial cooperation depends on the structure of national criminal justice systems and on the distribution of competence, power and responsibility therein. Moreover, also the stage in which the proceedings are may play a role. In this sense, it should be considered that police cooperation, unlike judicial cooperation, may extend also to the prevention of criminal offences.[230]

Generally applicable legal instruments of judicial cooperation on which the exchange of information can be based include the 1959 CoE MLA Convention, whose scope was extended by its 1978 Additional Protocol to cover also the cooperation of fiscal offences (previously excluded from many cooperation agreements along political offences)[231]; its Second additional protocol adopted in 2001; the 2000 EU MLA Convention; and the EIO Directive 2014/41/EU. While the 1959 CoE MLA Convention and its Second

228 Coercive measures are investigative activities that entail the immediate interference with fundamental rights of an individual. For example, the search of a private domicile (or of a computer or of a phone) interferes with the right to private and family life; the seizure of any goods found in the course of such a search interferes, among others, with the right to property. Searches and seizures can therefore be considered coercive measures. The hearing of a witness, conversely, may be considered as a non-coercive measure as it does, in principle, not interfere with any individual right. The gathering of information or evidence that is already in the possession of another authority is generally also considered to be non-coercive because, while the original collection may have interfered with an individual right, the further sharing is not considered to cause a new and autonomous interference. It must, nevertheless, be considered that even though information sharing is a non-coercive measure, fundamental rights that may be affected by the processing of this information and its following use must be appropriately protected.

229 A. Klip, *European Criminal Law. An Integrative Approach*, Cambridge: Intersentia 2021 (hereinafter: Klip 2021), p. 457–458.

230 Klip 2021, p. 458.

231 Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (adopted 17/03/1978, entered into force 12704/1982) 99 ETS 1 (hereinafter: Additional Protocol to the 1959 MLA Convention).

additional protocol as well as the 2000 EU MLA Convention include provisions both on the exchange of information on request and on spontaneous exchange of information, the EIO Directive only provides for the possibility of requesting information from authorities of another EU Member State. Looking beyond the European landscape, the 1992 Inter-American Convention on Mutual Assistance in Criminal Matters includes provisions on exchange of information with and without prior request between the competent authorities of several American jurisdictions.[232] The 1993 Optional Protocol[233], similarly to the 1978 Additional Protocol to the 1959 CoE MLA Convention, extends for some of these jurisdictions the scope of application of the Inter-American Mutual Assistance Convention also to tax offences.[234]

The applicable legal instrument for the exchange of information through police cooperation is Directive (EU) 2023/977 on the exchange of information between the LEAs of Member States (repealing Council Framework Decision 2006/960/JHA). This Directive, which builds upon the Schengen acquis, represents the first component of the new EU Police Cooperation Code to have been adopted. In addition to this instrument, there is a newly adopted Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"),[235] and a Council Recommendation on operational police cooperation.[236] The EU Police Cooperation Code seeks to streamline, enhance, develop, modernise and facilitate law enforcement cooperation between relevant national agencies. Further, the Europol Regulation (EU) 2016/794 serves as a legal basis for data processing by Europol and for information exchange between Europol, on the one hand, and Union bodies and national authorities, respectively on the other hand.

5.2.2 Formal versus informal exchange

A second distinction may be drawn between formal and informal ways of exchanging information. At the outset, it must be clarified that the distinction drawn between formal and informal exchanges is specific to criminal law. It is important to consider that in criminal law both types of exchanges have a basis in legal instruments. However, they differ with regard to the intensity of legal requirements that must be met in order to proceed with the exchange of information.

232 Antigua and Barbuda; Argentina; Bahama; Bolivia; Brazil; Canada; Chile; Colombia; Costa Rica; Dominica; Czech Republic; Ecuador; El Salvador; Grenada; Guatemala, Guyana; Honduras; Jamaica; Kazakhstan; Mexico; Nicaragua; Panama; Paraguay; Peru; Suriname; Trinidad and Tobago; Ukraine; United States; Uruguay; Venezuela.

233 Optional Protocol Related to the Inter-American Convention on Mutual Assistance in Criminal Matters (adopted 11/06/1993, entered into force 07/04/2002) 77 OAS 1.

234 To date, the Optional Protocol has been ratified by Brazil; Chile; Colombia; Czech Republic; Ecuador; Honduras; Paraguay; Ukraine; and the United States.

235 Regulation (EU) 2024/982 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (hereinafter: the Prüm II Regulation) (13/03/2024) OJ L.

236 Council Recommendation (EU) 2022/915 on operational law enforcement cooperation (9 June 2022) OJ L 158/53.

The category of formal exchanges of information covers those forms of exchange that are subject to detailed legal requirements (concerning necessary conditions, forms and procedural steps to follow) because they are geared towards the collection of evidence abroad and its judicial use.[237] The exchange of information upon request between judicial authorities, either based on the request model (Inter-American Mutual Assistance Convention; 1959 CoE MLA Convention; 2000 EU MLA Convention) or on the mutual recognition model (EIO Directive) are examples for formal exchanges.

Informal exchanges refer to ways of sharing information through *simplified channels* upon which LEAs or judicial authorities rely to reinforce each other's investigations, to increase the efficiency of such investigations. Informal exchanges in criminal matters distinguish themselves from formal exchanges for being, on the one hand, subject to fewer procedural rules and, on the other hand, for being geared towards the exchange of information and intelligence. Such information and intelligence are useful for investigations, but they are, in principle, not suited to become evidence upon which a judge may directly base their decision.

This category includes *spontaneous* exchanges of information between police authorities or between judicial authorities. Exchange of information *upon request* among police authorities as regulated under Directive (EU) 2023/977 can equally be included in this category. Although they are *enshrined in a legal framework* accompanied by more detailed provisions than those established for the spontaneous exchange of information, they maintain traits of informal exchanges. This becomes clear when comparing the exchange of information upon request between police authorities to the above-mentioned forms of exchange of information on request between judicial authorities. As observed in the existing literature on the topic, the exchange of information between police authorities is still based on only minimal procedural requirements, and it has a much less defined object. Furthermore, the exchange of information upon request among police authorities is geared towards advancing investigations and intelligence operations rather than to gather evidence for judicial use. This reinforces the argument that such exchanges may still be considered as informal in nature.[238]

Table 4 on p. 107 offers an overview over the main instruments examined in this Chapter and indicates whether these are to be classified as instruments of judicial cooperation or of police cooperation and whether they contain rules on formal cooperation and/or informal cooperation.

237 M. Panzavolta, 'Formal and Informal Circulation of Cross-Border Evidence in Europe and Possible Improvements. Toward an "Annex E" of the European Investigation Order?', *European Criminal Law Review* 2024(2): p. 191-212 (hereinafter: Panzavolta 2024), p. 199.

238 Panzavolta 2024, p. 196.

Table 4: Categorisation of legal instruments generally applicable to the exchange of information in criminal investigation

Legal instrument	Judicial cooperation	Police cooperation	Formal cooperation	Informal cooperation
1992 Inter-American Mutual Assistance Convention	✓		✓	✓
1959 CoE MLA Convention	✓		✓	
2001 Second Protocol to 1959 CoE MLA Convention	✓		✓	✓
2000 EU MLA Convention	✓		✓	✓
Directive (EU) 2014/41 on EIO	✓		✓	
Directive 2024/977		✓		✓
Europol Regulation (EU) 2016/794		✓		✓

As mentioned in the introduction in Chapter 1, these instruments do not seem to use the concept of foreseeable relevance *per se* as a criterion to enable information exchange. However, the rules that they enshrine set out under which conditions information may be exchanged. These requirements entail an evaluation of the relevance of the information in question and may therefore be compared to the foreseeable relevance principle used in matters of tax law. The focus will lie on such similar/equivalent criteria that are used for information exchange between competent authorities in criminal investigations. The preconditions to exchange information will be assessed and evaluated considering the need to protect the involved parties' data and, so far relevant, their privacy. The risk of interference with other fundamental rights will equally be considered.

5.3 Concepts comparable to the foreseeable relevance standard

The above-mentioned legal instruments regulating mutual legal assistance – the 1992 Inter-American Convention on Mutual Assistance in Criminal Matters, the 1959 CoE MLA Convention, the Second additional protocol to the 1959 MLA Convention and the 2000 EU MLA Convention, the EIO Directive and Directive (EU) 2023/977 on the exchange of information between LEAs – include provisions on information exchange upon and/or without prior request. Starting with provisions governing the exchange of information upon request, the requirements set out therein will now be analysed.

5.3.1 Exchange of information on request

The exchange of information on request through judicial cooperation in criminal matters within the EU is primarily based on the EIO Directive. This instrument is based on the principle of mutual recognition and consists, according to Article 1 EIO Directive, in a judicial decision issued or validated by a judicial authority of a Member State to have one or several specific investigative measures carried out in another

Member State to obtain evidence.[239] According to Article 10(2) EIO Directive, among the 'measures' that must always be available in the executing Member States is the obtaining of information which is already in the possession of the executing authority.

Pursuant to Article 6 EIO Directive, an exchange of information may only be issued if its issuing is necessary and proportionate for the purpose of the proceedings, considering the rights of the suspected or accused person. Moreover, as established under Article 5(1) EIO Directive, the issuing authority must indicate in the exchange of information: (a) data about the issuing authority and, where applicable, the validating authority; (b) the object of and reasons for the exchange of information; (c) the necessary information available on the person(s) concerned; (d) a description of the criminal act, which is the subject of the investigation or proceedings, and the applicable provisions of the criminal law of the issuing State and (e) a description of the investigative measures(s) requested and the evidence to be obtained. This suggests that when issuing an exchange of information, including when this is aimed at obtaining information already in the possession of the executing authority, the issuing authority must provide the executing authority with sufficient elements to establish that the information requested is linked to an ongoing proceeding (usually in the investigation stage).

Article 5(1)(b) EIO Directive, in particular, indicates that the issuing authority must give reasons as to why the information is needed for the purposes of their investigation. This, arguably, resembles the provision of elements needed to establish that the required information is 'foreseeably relevant'.

In cases that lie outside the scope of the EIO Directive, the 1959 CoE MLA Convention or the 2000 EU MLA Convention may apply. These include a traditional mutual legal assistance principle according to which the so-called requesting Party may request the so-called requested Party to procure evidence or to transmit articles to be produced in evidence, records or documents. According to Article 3(1) 1959 CoE MLA Convention information may be requested through letters rogatory.

Similarly to what is required under the EIO Directive, Article 14(1) and (2) of the 1959 CoE MLA Convention provides that letters rogatory must indicate: (a) the authority making the request; (b) the object of and the reason for the request; (c) where possible, the identity and the nationality of the person concerned and (d) where necessary, the name and address of the person to be served. Moreover, they shall also state the offence and contain a summary of the facts. Here a similar reasoning could be followed as just laid out regarding to the exchange of information. The need for the requesting authority to indicate object and reasons of the request hints to the fact that also here elements are sought to establish the relevance of the requested information for the criminal proceeding in question. The 2000 EU MLA Convention does not include a

239 Article 82(1) Treaty on the Functioning of the European Union (hereinafter: TFEU) establishes that, on the basis of the principle of mutual recognition, judgments and judicial decisions adopted in one EU Member State are recognised by the competent authorities in another EU Member State as if they had been adopted by a competent authority of their own jurisdiction.

similar list of requirements. As this instrument must, however, be considered to be supplementing the 1959 CoE MLA Convention, it is reasonable to assume that the same requirements apply for the purposes of mutual legal assistance under the 2000 EU MLA Convention.

Pursuant to Article 7(h), the scope of application of the 1992 Inter-American Mutual Assistance Convention includes the transmittal of information. According to Article 24 of the 1992 Inter-American Mutual Assistance Convention, there is an obligation for the competent authority of a State party to make available information held by government agencies or departments of its State upon request of the competent authorities of another State party. Article 26 of the Inter-American Mutual Assistance Convention establishes that such request must include indications concerning: a) the crime to which the procedure refers; a summary description of the essential facts of the crime, investigation, or criminal proceeding in question; and a description of the facts to which the request refers; b) the proceeding giving rise to the request for assistance, with a precise description of such proceeding; c) where pertinent, a description of any proceeding or other special requirement of the requesting State and d) a precise description of the assistance requested and any information necessary for the fulfilment of that request.

Although there is no explicit reference to the need to lay out the reasons for the request, as in the case of an exchange of information or a request pursuant the 1959 CoE MLA Convention and, arguably, the 2000 EU MLA Convention, the necessary transmission of details concerning the description of the facts to which the request refers, set forth in Article 26(1)(a) Inter-American Mutual Assistance Convention, could be considered to absorb the need to outline a certain degree of foreseeable relevance of the information in question.

As far as exchange of information on request between LEAs of EU Member States is concerned, Directive (EU) 2023/977 includes provisions on this matter, that were introduced for the first time by the so-called *Swedish Framework Decision*.[240] Article 4(3) Directive (EU) 2023/977 establishes that Single Points of Contact (established or designated by the Member States) or designated LEAs of one Member State may submit requests for information to the Single Point of Contact of another Member State only where there are objective reasons to believe that (a) the requested information is necessary for and proportionate to prevent, detect, or investigate criminal offences, and (b) the requested information is available to that other Member State. The requesting authority must, according to Article 4(5) Directive (EU) 2023/977, indicate the objective reasons for which it is believed that the requested information is available to the requested Member State and it must give an explanation of the connection between the purpose for which the information is requested and any natural or legal person or entity to which the information relates, where applicable.

240 See Panzavolta 2024, p. 195. The general rules for cross-border exchange of law enforcement information are laid down in the Council Framework Decision (2006/960/JHA), known as 'Swedish Framework Decision' or 'Swedish initiative'.

Article 5 Directive (EU) 2023/977 provides that the requested Member State has strict time limits to follow-up on the request and provide the information. Only in cases in which under the national law of the requested Member State the information may only be provided after having obtained a judicial authorisation the time limits may be extended for the time necessary to obtain such an authorisation.

Refusals of requests for information are governed by Article 6 Directive (EU) 2023/977 and may only occur where (a) the information is not available to the Single Point of Contact and the competent LEAs of the requested Member State; (b) the requirements set forth in Article 4 Directive (EU) 2023/977 are not met; (c) the above-mentioned judicial authorisation is refused; (d) the information constitutes personal data other than those that may be collected and processed for the purpose of analyses of a strategic or thematic natures, for the purpose of operational analyses or for the purpose of facilitating the exchange of information pursuant to the Europol Regulation; (e) the requested information has been found to be inaccurate, incomplete or no longer up to date and cannot be provided in accordance with the Law Enforcement Directive; (f) there are objective reasons to believe that the provision of the requested information would be contrary or would harm the essential interests of the national security of the requested Member State, would jeopardise the success of an ongoing investigation of a criminal offence of the safety of an individual; unduly harm the protected important interest of a legal person; (g) the request pertains to a criminal offence punishable by a maximum term of imprisonment of one year or less under the law of the requested Member State, or to a matter that is not a criminal offence under the law of the requested Member State; (h) the requested information was initially obtained from another Member State or from a third country and that State has not consented to the provision of the information.

The requirement sub (b) seems to include the possibility for the requested Member State to evaluate to what extent the objective reasons of connection – which may be compared to a relevance assessment – are substantiated in the request. Moreover, Directive (EU) 2023/977 mandates that the requested Member State must exercise due diligence in carrying out this assessment and evaluate whether there is a manifest breach of fundamental rights.

Furthermore, the exchange of information between national authorities and between them and Europol is regulated by the Europol Regulation (EU) 2016/794 which equally indicates the conditions under which information may be exchanged.[241] The Europol Regulation (EU) 2016/794 refers to the exchange of information in general, without specifying whether only the exchange of information upon request or also

241 Regarding the cooperation between Europol and competent authorities of the United Kingdom, the Trade and Cooperation Agreement stipulates under Article 569 that personal data shall be processed only for the specific purposes set out in the Europol Regulation. The purpose must be clearly indicated by the moment data are transferred. If this is not the case, the receiving competent authority shall, in agreement with the transferring authority, process the personal data to determine their relevance as well as the purpose(s) for which it is to be further processed. Processing data for purposes other than those for which the data has been provided is only possible with the authorisation of the transferring competent authority.

spontaneous exchange of information are included. However, in the description of the tasks of the agency, Article 4 of the Regulation includes activities of information exchange. As there is no indication as to the necessity for such exchange to occur based upon a prior request, it seems that both forms of information exchange – upon request and without such request – are included. More specifically, Article 4 (1) mentions among others the performance of the following tasks: the exchange of information by Europol directly, the support of EU Member States in information exchange activities and the cooperation of Europol with FIUs, i.a. through the exchange of information.

Specific conditions to proceed with the exchange of information are not indicated. However, according to Article 18 Europol Regulation, the processing of personal data may only occur for the purpose of cross-checking to identify connections or relevant links between information related to persons suspected of or convicted for an offence for which Europol is competent (i.e. serious crime affecting at least two Member States or a list offence as enshrined in Article 2(2) FD 2002/584/JHA on the European arrest warrant[242]) or related to persons for whom there are factual indications or reasonable grounds to believe that they will commit such an offence.

Personal data may further be processed:

- for the purposes of analyses of a strategic or thematic nature;
- for operational analyses;
- to facilitate the exchange of information between Member States, Europol and other Union bodies, third countries, international organisations and private parties;
- for research and innovation projects and to support Member States, upon their request, in informing the public about suspects or convicted individuals who are wanted based on a national judicial decision relating to a crime that falls within Europol's objectives;
- and to facilitate the provision by the public of information on those individuals to the Member States and Europol.

Overall, also the basis upon which information may be exchanged upon request in criminal matters seem more stringent than those required to proceed with an own-initiative provision of information, which are discussed below (Section 5.3.2). The requesting/ordering authorities are in any case obliged to substantiate that (at least objective reasons to believe that) the preconditions (i.e. an ongoing investigation/proceeding or the need to prevent or detect a criminal offence) exist and that the information sought is necessary and proportionate for this purpose. As in the context of information exchange upon request a foreign competent authority is entrusted with the competence to decide on the request, an additional layer of control comes into play. Indeed, the competent authority in the other jurisdiction may refuse to provide the requested information if a ground for refusal is applicable. Directive (EU) 2023/977 includes among the grounds for refusal failure to comply with the provisions

242 Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States (13 June 2002) OJ L 190/1 as amended by Council Framework Decision 2009/299/JHA.

of its Article 4.[243] However, as a recent study on the judicial scrutiny in cross-border evidence gathering through exchange of information suggests, the control by the executing (or: requested) authority is necessarily an epidermic one and, as such, limited to macroscopic irregularities. Indeed, in EU cooperation in criminal matters, the principle of mutual trust mandates that the issuing/requesting authority is best placed to assess the preconditions and the necessity of a request, while the executing/requested authority in principle accepts this assessment.[244]

5.3.2 Spontaneous exchange of information

Spontaneous exchange of information is widely used also in cooperation in criminal matters in the EU and beyond.[245] Initially developed as a practice to make the cooperation of LEAs swifter and more efficient, it has been translated also to the realm of judicial cooperation in criminal matters.[246]

Among the above-mentioned, generally applicable legal instruments that may be relied upon to spontaneous exchange of information between judicial authorities the Second additional protocol to the 1959 MLA Convention and the 2000 EU MLA Convention must be mentioned. Moreover, also the 1992 Inter-American Mutual Assistance Convention contains provisions on the spontaneous exchange of information.

Article 11 Second additional protocol to the 1959 MLA Convention indirectly includes the requirement that the information to be shared might assist the receiving Party initiating or carrying out investigations or proceedings or might lead to a request for information. Article 7 of the 2000 EU MLA Convention only identifies the type of information that may be shared (must be relating to serious crime affecting at least two EU Member States, terrorism and list offences; and the competence for the handling and punishment must lie with the receiving Party).

It is debatable whether the two requirements are equivalent. While the first provision (Article 11 Second additional protocol to the 1959 MLA Convention) can be considered to be including elements of a relevance evaluation to be made by the sending authority, this does not seem to be the case for the second one. Article 7 of the 2000 EU MLA Convention does not seem to require an *ad hoc* evaluation as it merely sets out objective

243 Article 4 includes the indication and explanations of the objective reasons to believe that the information could be useful to prevent, detect and/or investigate criminal offences and that such information is likely to be found in the requested Member State. N.B. in matters of judicial cooperation in criminal matters, the lack of indication of the reasons of an EIO would not amount to a refusal ground but, rather, trigger consultation between the involved authorities to solve the issue and fill the gaps.

244 See, for instance, A. Mosna, 'Judicial Protection in EU Cross-Border Evidence-Gathering: the EIO as a Case Study', *European Criminal Law Review* 2024(2): p. 148-176 (hereinafter: Mosna 2024); M. Daniele, 'Scope of Judicial Review in the Executing State in EIO Proceedings', *European Criminal Law Review* 2024(2): p. 177-190 (hereinafter: Daniele 2024).

245 M. Simonato, 'The "Spontaneous Exchange of Information" Between European Judicial Authorities From the Italian Perspective', *New Journal of European Criminal Law* 2011(2): p. 220-229 (hereinafter: Simonato 2011) p. 224.

246 Simonato 2011, p. 221.

requirements the information must present, thus implying a presumption of relevance once the information fulfils the above-mentioned criteria. At the same time, the width of the criteria for the relevance evaluation under Article 11 Second additional protocol to the 1959 MLA Convention ('might assist' and 'might lead to a request') raises doubts as to whether any meaningful *ad hoc* relevance-evaluation can take place. In any case, as Article 1 of the 2000 EU MLA Convention establishes, the two Conventions are linked to each other as the 2000 EU MLA Convention is intended to supplement the provisions and facilitate the application between the Member States of the EU of the 1959 CoE MLA Convention. Its provisions must thus be read in light of those of the Council of Europe Convention as well as in light of its goal to facilitate cooperation.

Looking beyond the European sphere, the 1992 Inter-American Mutual Assistance Convention does not include a provision for the spontaneous exchange of information in general. However, in connection to the search, seizure, attachment and surrender of property, it includes the possibility for a spontaneous exchange of information. Article 14 of that Convention, governing measures for securing assets, provides that the central authority of any Party may convey to the central authority of any other Party information it has on the existence of proceeds, fruits, or instrumentalities of a crime in the territory of that other Party. The relevance requirement implied in the provision in question consists in the necessity that the information relate to the existence of property linked to crime and located in the territory of the Party receiving the information.

As far as spontaneous information exchange in cross-border police cooperation is concerned, as of 2024 this field is regulated by Directive (EU) 2023/977 on the exchange of information between the LEAs of the Member States. Spontaneous information exchange in cross-border police cooperation under Article 7 Directive (EU) 2023/977 requires objective reasons to believe that information could be relevant to the other Member State for the purpose of preventing, detecting or investigating criminal offences (spontaneous information sharing is obligatory in case of serious criminal offences). Based on the principle of availability, the intent also for this new instrument is to make simplified, informal (because they lie outside the mutual recognition mechanism) exchanges.[247]

Interestingly, the *new legal framework* presents some modifications with respect to the Swedish Framework Decision.[248] The latter only provided a compulsory exchange of information and intelligence where the competent LEA has factual reasons to believe that the information or intelligence could assist in the detection, prevention or investigation of list offences. The Swedish Framework Decision also included a limitation clause that stated that the provision of information and intelligence shall be limited to what is deemed relevant and necessary for the successful detection,

247 Panzavolta 2024, p. 195-196; pursuant to Article 3, the exchange of information under Directive (EU) 2023/977 is governed also by the principle of equivalent access, by the principle of confidentiality, by the principle of data ownership and by the principle of data reliability.

248 This new legal framework is effective as from 12 December 2024.

prevention or investigation of the crime/criminal activity in question. The Swedish Framework Decision included a two-step relevance assessment: first, a consideration of the existence of factual reasons to believe that information could be useful for detecting, preventing and investigating a list offence and, second, an evaluation of the relevance and necessity of the exchange for doing so successfully. The provision of this second step seems to require a more careful/selective assessment by LEAs, although no further criteria are indicated to ensure that this evaluation would follow a standardised pattern.

No such limitation clause is included in the recently adopted Directive (EU) 2023/977. Not only does this provision have a broader scope of application, being available for optional information exchange regarding any type of criminal offence and imposing obligatory information exchange for serious offences. This latter category includes not only "list offences", but also other types of serious offences if they affect more than one Member State (with potential national differences).

The provision in question contains a limitation to the obligation to exchange information. This limitation applies in instances that would allow to refuse request for information in procedures of exchange of information upon request: refusal of judicial authorisation (if required under national law); potential harm to the essential interest of national security; jeopardy of the success of an ongoing investigation or of the safety of an individual; or undue harm to the protected important interests of a legal person. This limitation does however not appear to affect that relevance evaluation required under Article 7 Directive (EU) 2023/977.

The result seems to be a considerably more *flexible notion of relevance* and of its assessment, especially because the concept of 'objective reasons' is not further explained. This concept was already part of the provision on spontaneous information exchange included in the Proposal of the Directive in question. The Explanatory Memorandum accompanying the Proposal, however, does not include any indication as to how 'objective reasons' should be interpreted. A hint could be taken from a comparison of Article 7 Directive (EU) 2023/977 with the provision regulating the same matter in the Swedish Framework Decision. One could argue that the previous phrasing relating to 'factual reasons' suggests the necessity of a more solid base of background information to reach the decision to spontaneously transfer information than 'objective reasons' seems to imply.

As the Europol Regulation does not specifically limit the scope of application of its provisions on the exchange of information to the exchange of information on request, its rules arguably apply also to the spontaneous exchange of information. These have been discussed in Section 5.3.1.

Overall, legal instruments applicable to spontaneous information exchange in criminal investigations, be this at the judicial level or at the level of LEAs, while they are not using the concept of 'foreseeable relevance' strictly speaking, they mostly do require an evaluation concerning the *link* of the information in question with the

law enforcement tasks of the foreign counterpart. Thereby the reference to 'objective reasons' (Directive (EU) 2023/977) or to the mere requirement of a factual connection, such as the one included in the 2000 EU MLA Convention suggests a tendency to limit the degree of relevance of the information that forms the object of spontaneous information exchange to a link of material pertinence to ongoing or potential investigations in the foreign Member States.

5.4 Relation between relevance criterion and applicable data protection

As far as criminal investigations are concerned, the requirement of a minimum degree of relevance of the information at stake for the purposes of the fulfilment of the tasks of competent authorities in other Member States is intended to provide a basis for the legality of an exchange of information consisting in the sharing of personal data. The applicable legal framework in the field of data protection in criminal proceedings is represented by Directive (EU) 2016/680 (Law Enforcement Directive, hereinafter: LED). Article 1(1) establishes that the LED lays down the rules relating to the protection of natural persons regarding 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. To note, Article 3(2) LED defines 'processing' as any operation or set of operations performed on personal data or on sets of personal data including also the disclosure of data by transmission. This allows to subsume the concept of exchange of data (information) as used in this study under the concept of 'disclosure by transmission' and thus under the concept of 'processing'.

Under Article 4, the LED requires Member States to process data lawfully and fairly; to collect data for specified, explicit and legitimate purposes and not to process data in a manner that is incompatible with those purposes. Moreover, data must be adequate, relevant and not excessive in relation to the purposes for which they are processed. According to Article 4(2) LED, the purposes for the collection and for the processing of data do not necessarily have to coincide. Processing of data for purposes (included in Article 1(1) LED) other than those for which such data was collected is allowed as long as the conditions set forth in the provision in question are fulfilled. These conditions require that the competent authority which determines the purposes and means of the processing of personal data is authorised to process such personal data for such a purpose in line with EU or national law. It is, further, necessary that the processing is necessary and proportionate to the original purpose in accordance with EU or national law. This has been confirmed by the CJEU in its case C-180/21.[249]

Pursuant to Article 20, the LED requires Member States to implement data protection by design and by default. Thus, Member States must protect the data subject, on the one hand, by pseudonymising data and by thereby achieving their minimisation (data

249 CJEU 8 December 2022, *VS v Inspektor v Inspektorata kam Visshia sadeben savet*, Case 180/21, ECLI:EU:C:2022:967, at 63.

protection by design) and, on the other hand, by ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

A combined reading of the provision of the LED and of the different provisions applicable to information exchange in criminal proceedings arguably suggests that – even considering the more flexible requirements that the latter provisions establish – the justification and condition for the lawfulness of the data sharing consists not only in a clearly identified purpose (i.e. facilitation of contrasting certain offences) for the exchange. There is also a need to evaluate the relevance and the necessity of the data in light of the purpose of the exchange in question. Looking specifically at information exchange between LEAs, this second step seems to recall aspects of Article 7(2) FD 2006/960/JHA. While this part has not been included in the new provision on spontaneous information exchange set forth in Article 7 Directive (EU) 2023/977, the combined reading allows for the reasoning according to which this second step is still implicitly required in light of the applicable data protection legislation. In short: this analysis suggests that the combination of the requirements of the LED with that of the specific instruments allowing for the exchange of information on request or without prior request reinforces protection of individual rights from the perspective of the principle of legality, necessity and proportionality.

Key takeaway:

Criminal law instruments generally apply flexible relevance criteria, particularly in the context of spontaneous information exchange. The design of FCInet ma³tch, which only reveals identifiable information upon a validated hit, does not appear to be incompatible with these standards and may even offer enhanced protection for individual rights. The technology shifts the moment of data access to the receiving authority, and thus prevents untimely disclosure of information. However, to avoid discriminatory use, common rules establishing how data ought (or ought not) to be selected within the entities participating in the network before they are used to create filters and hashes, should be adopted.

5.5 Preliminary conclusion

The aim of this assessment was to lay out what kind of relevance criteria are applied in information exchange in criminal matters and to draw a parallel to the concept of foreseeable relevance applied in administrative tax exchanges. The legal instruments discussed in this Chapter present a rather *flexible approach* to the link between the information and the aim for the transmission (preventing, detecting or investigating/prosecuting criminal offences). This applies in particular to those instruments that regulate spontaneous forms of information exchange.

Focussing on the ma³tch technology and the sharing of filters, the question arises whether in this instance of own-initiative provision of information, the lack of a relevance evaluation may be justified by the privacy-enhanced effect of this technology and by the fact that the receiving authority is only able to access the data on the identity of a person shared if it experiences a hit (confirmation that this basic data is not the result of a false positive occurs at a later stage, through validation from the sending authority, if this is sought by the receiving authority). Such a hit occurs when the receiving organisation is able to detect a hit as a result of the shared filter, which again is only possible if that organisation already has a file on the person in question. The potentially broad interpretation of the relevance criteria suggests that the different criminal law instruments concerning information exchange that have been discussed above do not preclude the use of the ma³tch technology. This argument is reinforced if one relies on a teleological interpretation of these instruments according to which the relevance criterion is meant to ensure an appropriate balance between the public interest in efficient and effective information sharing, intelligence and investigation, on the one hand, and the individual rights to privacy and data protection, on the other.

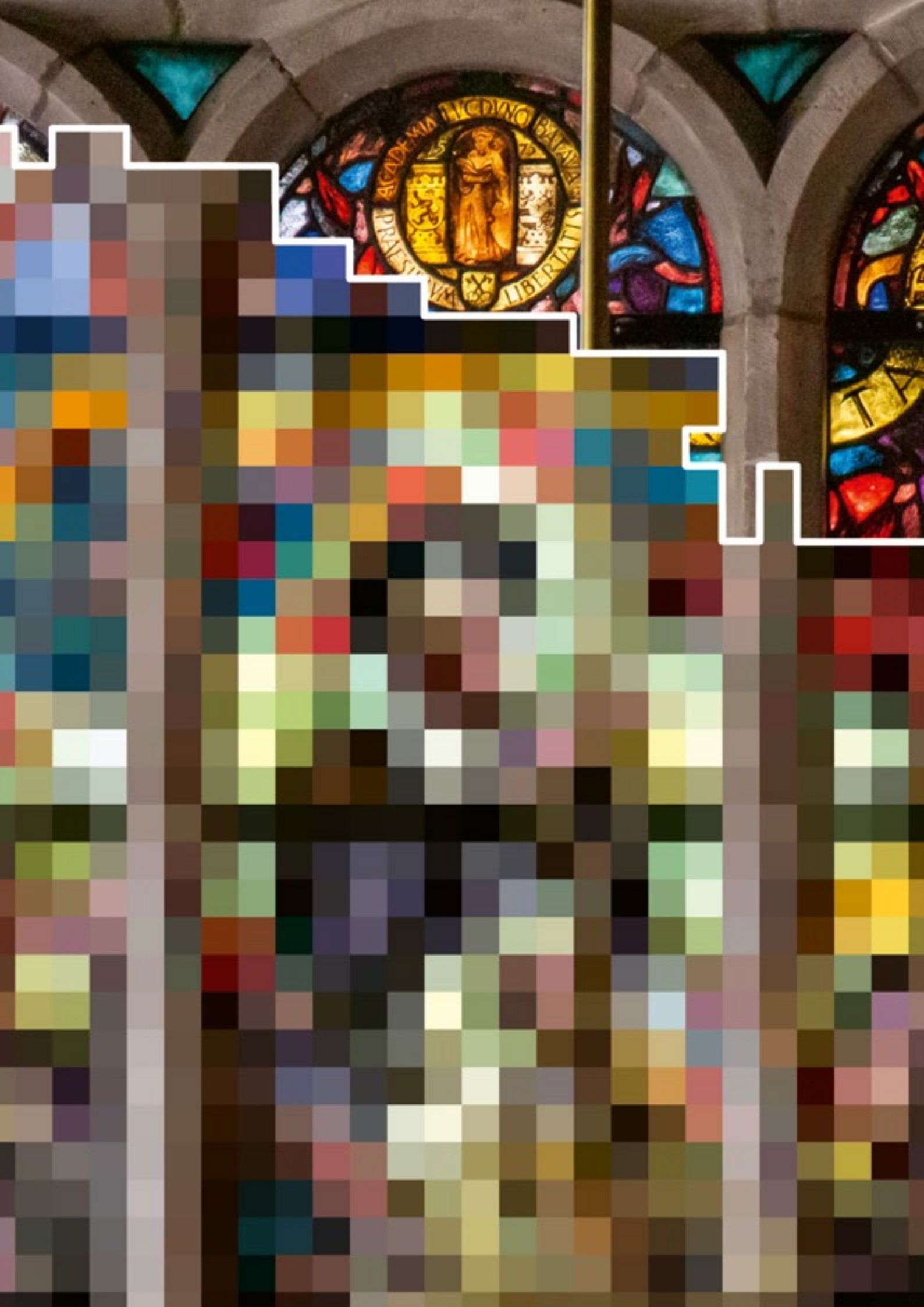
More precisely: the dynamic of spontaneous exchange of information seems to be altered through the ma³tch technology in a way that the moment in which the filter is shared is not the moment in which the providing authority sends/discloses tax information, but the (only potential) moment in which the receiving authority is able to access such information by detecting a hit and a subsequent validation and tax information request. The validation replaces the actual relevance evaluation. In principle, the technology at issue does not seem to raise any issues of incompatibility with criminal law standards. To the contrary, it appears to be even more protective towards individual rights that are typically interfered with, such as the right to the respect for private life and data protection. Nevertheless, considering what has been described in Chapter 4, the *User Protocol* does not completely preclude the use of potentially discriminatory characteristics (see Section 4.2.1). It could, thus, be beneficial to establish common rules that determine how data ought (or ought not) to be selected within the entities participating in the network before they are used to create filters and hashes that go beyond what is currently enshrined in the *User Protocol* to ensure even more effectively that any discriminatory use is avoided.

Finally, a more general reasoning could be added. As a form of spontaneous and, for criminal matters considered informal information exchange, this 'hit/no-hit mechanism' is conceived to increase the efficiency of information sharing. In this perspective, this could lead to an increasing reliance on what for criminal law purposes is considered to be an informal way of exchanging information, even in cases in which formal channels, such as the issuing of a *European investigation order* for an exchange of information, would be an option.[250] While there is theoretically a clear divide between formal and informal channels of exchange, the first conducive to share *evidence* and the second to

250 See, in this sense, S. Allegrezza, 'Critical Remarks on the Green Paper on Obtaining Evidence in Criminal Matters from One Member State to Another and Securing Its Admissibility', *Zeitschrift für Internationale Strafrechtsdogmatik* 2010: p. 569-579 (hereinafter: Allegrezza 2010).

share *information and intelligence* (on the basis of which evidence may be gathered in the following), in practice these lines are often blurred. Given the national differences concerning rules on the admissibility of evidence, in many countries information and intelligence has the potential of turning into evidence used for judicial purposes. Considering the different type and intensity of safeguards for individuals respectively in formal and informal exchanges of information between authorities, concerns about the appropriate protection of individual rights (beyond privacy and data protection), such as the right to a fair trial and the right to interact with the counterpart on the way evidence is gathered, are understandable.[251] As mentioned, these concerns are directed towards a more general dynamic within the realm of judicial cooperation in criminal matters. While the use of ma^{3}tch also enables informal exchange of information in criminal matters, it must be stressed that this technology provides for a considerable minimisation of the interference with the right to privacy and to data protection and therefore represents a positive development in this field.

251 Panzavolta 2024, p. 198-199.


ACADEMIA LUGDUNO BATAVA
LIBERTATIS

Chapter 6

Summary and conclusion

Since the turn of the century, the exchange of information has become a vital tool in the fight against tax evasion and aggressive tax avoidance. A strong information position of governments worldwide is needed to tackle tax fraud, financial crime, and other crimes that undermine society. At the same time, these governments must uphold and safeguard public values, in particular the protection of taxpayer data and privacy. This creates a challenging dual role for government organisations that collect and use data for the proper execution of their work. The *Forum of Heads of Tax Crime Investigation*, held under the auspices of the OECD, recognised this duality and initiated the FCInet-platform, which houses a built-in privacy enhancing technology named 'ma^{3}tch', to meet this challenge. FCInet is focused on 'getting the right information, at the right time, in the right way, from and to the right place'. Organisations that use this instrument must comply with the legal requirements for international cooperation and information exchange, and the associated data protection and privacy laws.

Although tax authorities have a range of legal instruments for the exchange of information at their disposal, the OECD-MC, UN Model Tax Convention, OECD-TIEA, the MAAC, and the DAC are regarded as the principal instruments for tax purposes. Since the DAC, like the MAAC, is predominantly multilateral in nature, whereas the application of FCInet ma^{3}tch technology involves bilateral exchanges, this study has focused on the application of Article 26 of the OECD-MC in the context of bilateral information exchange (Chapter 2, Legal interpretation). Where relevant, we also discussed some valuable insights into the development of other instruments, such as the more precise definition of foreseeable relevance in DAC7 and the use of information for other than tax purposes or transmission to third parties as set out in the Explanatory Report to Article 22(4) of the MAAC.

Article 26 of the OECD-MC provides three methods to exchange information: spontaneous, automatic and on request. States engage in spontaneous exchange of information when they discover – often in the course of their own investigations – information that may be relevant and useful to a tax treaty partner. In addition, States have the option to designate certain information that will be shared with a treaty partner on an automatic basis, without the need to file a request. Finally, States may exchange information on request; the competent authority of the requesting State makes the request to the competent authority of the requested State, which shall assess whether the requested information can be provided.

Article 26(1) of the OECD-MC sets out the basic obligation to exchange information 'foreseeably relevant' to the implementation of a tax treaty, the administration or enforcement of a State's domestic tax law or political subdivisions or local authorities. For bilateral tax treaties, the relevant actors in each State are the competent authorities. They are responsible for handling the requests for information, which may also involve other actors, such as those involved in the investigation that gave rise to the request, mostly someone in the tax administration. The competent authority of the requesting

State makes the request to the competent authority of the requested State, who will then work through its internal procedures to confirm the information request to be appropriate under the treaty, secure the requested information and transmit it to the competent authority of the requesting State. States are, however, not at liberty to engage so called 'fishing expeditions'.

Since Article 26(2) of the OECD-MC allows a State to use information for *other than taxpayer-specific purposes* – if the information may generally be used for such purposes under the national laws of both States and the sending State authorises such use – the receiving State may share this information with other LEAs, for example, in the area of money laundering and (tax) fraud and with third parties (i.e. supervisory bodies/oversight institutions). In the latter case, the exchange may be subject to other restrictions (domestic law or tax treaty). For instance, the competent authority of a receiving State can only share with other authorities/supervisory bodies information received from the sending State provided prior authorisation has been granted and/or prior notification has been given by the competent authority of the sending State. In the few cases where prior authorisation and, in rare cases, notification are required, the competent authority of the sending State will have to demonstrate the foreseeable relevance prior to the disclosure. Such provisions may, in few cases, require an adjustment in the use of the FCInet ma³tch technology, resulting in the principle of foreseeable relevance having to be satisfied earlier than the time the ma³tch filter is made available. Such differences between States are highlighted in the comparative analyses of Chapter 3.

As the protection of personal data has become an increasingly important issue, some States have included provisions to limit the exchange of information to countries subject to an equivalent level of privacy and data protection. The ma³tch technology enables competent authorities to comply with their international obligations to share information that could assist a peer organisation in their investigation into criminal offenses or tax fraud. In today's world, technologies like ma³tch, when used under the appropriate legal basis, can conduct such a qualification process in a more efficient and privacy-friendly manner. A question under debate is whether all data used for ma³tch must have an explicit link to the jurisdiction of the peer organisation prior to sharing the filter, or whether this is unnecessary, given that a match or commonality involving a person under investigation by the peer organisation, based on the data in the filter, is in any case considered relevant. The research shows that both parts of this question must be answered in the negative: (1) the data used for ma³tch does not need to have any visible relationship with the receiving jurisdiction before the filter is shared, except in some cases where certain jurisdictions, for example, require *prior authorisation* by the sending State for the use of the data for *purposes other than taxation* or *transmission to third parties* by the receiving State; (2) a hit or commonality on a person under investigation by a peer organisation cannot be considered 'relevant' as long as this hit has not also been validated by the source country of the data. Another question under debate is whether – given the specific characteristics of the technology – the sharing of filters constitutes a form of 'fishing', where one seeks to determine whether certain individuals are active in other jurisdictions. This question must also be answered in

the negative. The fact that the persons included in the filter have been subjected to an investigation for a specific fraudulent typology or scheme, is generally a sufficient reason to escape the qualification of fishing expedition: "An ongoing examination or investigation to a person(s) is generally accepted as proof of foreseeable relevance". The data protection and privacy rights related to the application of FCInet ma^{3}tch technology are discussed in Chapter 4 (Technical assessment). As data can be shared between different levels of government, for instance within the criminal domain (Chapter 5, Criminal perspective), it is essential to strike a balance between the effective exchange of information and the protection of taxpayers' privacy rights. Many countries therefore emphasise the importance of maintaining a minimum standard of privacy protection in the domestic legislation of the partner State with which they intend to exchange information. To ensure that taxpayer data is adequately protected in the receiving State, these countries carefully evaluate the domestic legislation of that State regarding taxpayer privacy. Such legislation can be found in multiple sources, including the constitution, procedural tax law, standalone privacy laws, or decrees, et cetera.

This research concerns a case study on FCInet ma^{3}tch technology, more specifically on its functioning within the legal context of the international exchange of tax information. It maps out the meaning of the requirement of 'foreseeable relevance' in relation to the application of the technology, identifies differences in interpretation between countries involved in the research, and highlights some challenges in the protection of personal data. The main research question is:

> *"How should the principle of foreseeable relevance be interpreted in relation to the spontaneous exchange of information via FCInet's ma^{3}tch from a tax law perspective, what criteria do the competent authorities in jurisdictions (involved in the underlying study) distinguish to assess whether the principle has been met, how is this principle related to the right to privacy and the protection of taxpayers' personal data, and how does the concept of foreseeable relevance compare to requirements for information exchange in criminal proceedings?"*

6.1 Reply to the research question

The main research question is divided into four sub-questions, which we answer as follows.

1. *What is the reasoning and legal context behind the principle of foreseeable relevance from a tax law perspective and how is this related to the protection of personal tax data (Chapter 2)?*

From a historical perspective it is important to note that between 1998 and 2005, the nature of the concept evolved from 'necessary' to 'foreseeably relevant', to align with developments in the international exchange of information. It is also important to note that in 2005 the scope of the taxes covered by the Convention was extended from taxes imposed on 'income and capital' to taxes of *every kind*. In addition, it is important that

the information to be exchanged is *not limited to taxpayer-specific data*. Competent authorities may also exchange other *sensitive information*, for example, with a view to improving tax compliance. Furthermore, the information provided must be treated as *secret* in the receiving State, in the same manner as information obtained locally, under the domestic law of that State. The maintenance of secrecy in the receiving State is governed by domestic law, and at the national level, States may provide for exceptions to tax secrecy.

Since 2005, information may also be disclosed to 'oversight bodies', including authorities responsible for supervising tax administrations and enforcement agencies that operate within the general administrative framework of a contracting State. Thus, data collected by tax authorities and exchanged with other tax authorities should, in principle, be used solely for the administration and enforcement of tax law. However, some tax treaties and other international agreements on the exchange of information, such as the MAAC and the DAC, permit the use of exchanged information for *non-tax purposes* or its *disclosure to third parties*. Article 26(3) OECD-MC contains limitations which dictate a State's ability to refuse to provide information.

Although the wording of Article 26 of the OECD-MC does not distinguish between the spontaneous exchange of information and the exchange upon request, the research shows a difference in its application. To comply with the principle of foreseeable relevance in *spontaneous* exchange of information, such as in the application of ma^{3}tch, there must be a *minimum link* (minimum nexus) between the information to be provided about a taxpayer and its relevance for the taxation in the other State. This means that the information *must be able to be of interest*. In the case of spontaneous exchange about a group of taxpayers, this minimum link must be met regarding each taxpayer in relation to a particular receiving State. The link must be there at least *at the time of spontaneous provision* of the information. In principle, all persons whose hashed data is included in the ma^{3}tch filter are involved in an investigation, which may facilitate the assumption of a minimal link with the receiving State. If this minimal link is missing, the foreseeable relevance principle is not met.

In order to comply with the principle of foreseeable relevance in the exchange of information *on request*, Article 26 OECD-MC obliges States in principle to cooperate with such a request, but there is no obligation to cooperate in *fishing expeditions* or requests which are *unlikely to contribute to taxation* in the other State. Although the principle of foreseeable relevance has a broad interpretation, information requests should not be made without reason, there should at least be *some degree of knowledge* of an examination or investigation (nexus), the request must allow the *identification of a specific individual* and be *sufficiently concrete*, and the standard must at least be met *at the time the request is made*. In the application of FCInet ma^{3}tch, the presence of a 'hit' after checking the filter is sufficient for the receiving State to meet the requirement of foreseeable relevance for the follow-up verification request. The subsequent validation of the hit by the sending State confirms the actual link, but that is not a requirement for the application of the foreseeable relevance principle.

Furthermore, following the analysis of the protection of taxpayer information, it is important to keep in mind that the standard of foreseeable relevance must be interpreted in the light of the general principle that taxpayers must be protected against arbitrary or disproportionate interference by public authorities in the course of their private activities. In any case, the principle of foreseeable relevance must comply with the right to privacy and protection of personal data, because the absence of this detracts from the lawfulness of the exchange. Important aspects of the protection of personal data are the *lawfulness* of and *transparency* in the collection and processing of the information, the specification of the *purpose* for which the data is collected, the *accuracy* and *control* of the quality of the data, as well as the *security* and *prevention* of the data.

The spontaneous exchange of information requires that the foreseeable relevance standard is at least be complied with at the time of spontaneous exchange. In the application of FCInet ma³tch this means at least the moment of *sharing the filter*. In the few cases where a State is required to obtain prior authorisation from the source State for the use of information for *non-tax purposes* or for its *disclosure to third parties* – or in the rare cases where a State is required under its national law to inform taxpayers of the exchange before the information is provided to a receiving State – the tax authorities must be able to demonstrate that the condition of foreseeable relevance is met at the time of obtaining prior authorisation or informing the taxpayer. For the purposes of FCInet ma³tch, this prior authorisation or prior notification obligation means that the data used for ma³tch must have a minimum link with the receiving State prior to sharing the filter. A specific *investigation* or *examination* of a person based on well-founded suspicions generally assumes a minimum of relevance, as it implies a reasonable suspicion of non-compliance with a specific legal obligation in the source State, which may be indicative of any relevance for taxation in the receiving State. The threshold of foreseeable relevance in the case of spontaneous exchange of information must be interpreted as meaning that the information to be provided is *supposed to be of interest* to the receiving State, in the sense that the information must *at least be able to be of interest*, which may be qualified as a *less onerous requirement* than the requirement of some degree of knowledge of an examination or investigation in the case of an exchange of information on request.

2. *What criteria do jurisdictions (involved in the study) distinguish to assess whether the principle of foreseeable relevance has been met in the case of bilateral exchange of information (Chapter 3)?*

To answer this sub-question, we have assessed the application of the principle across various jurisdictions by comparative analyses of eleven countries inside and outside the EU (see Annex 1 for a description of the country analyses). As far as possible, we have made a distinction between spontaneous exchange of information and exchange on request. In reviewing the current international framework for information exchange – particularly in the context of spontaneous exchanges and the standard of foreseeable relevance – several insights have emerged. Legislation typically places greater emphasis on information exchanges made upon request rather than spontaneous exchanges.

This focus is rational, as the requesting country is better positioned to articulate the relevance of the information needed, given its familiarity with the specifics of the request. In contrast, spontaneous exchanges occur without prior request, which limits the sending State's ability to fully assess the relevance of the information within the recipient State's tax system. As a result, the threshold for what qualifies as relevant in spontaneous exchanges tends to be lower than in requested exchanges.

States with more developed information exchange frameworks, such as the U.S. and France, demonstrate a *higher frequency of information exchanges*. These States have established comprehensive systems that support both requested and spontaneous exchanges. For instance, the U.S. has detailed legislation governing these exchanges, including specific procedures for determining the usefulness of the information. France similarly maintains a structured approach that aligns with both national and international standards.

Globally, most States adopt the OECD standard for the principle of foreseeable relevance, resulting in a generally consistent application across various jurisdictions. This alignment indicates that significant interpretation deviations – which could affect the implementation of technologies like FCInet ma^{3}tch – are rare. The standardisation provided by the OECD facilitates a uniform approach to information exchange, thereby minimising potential barriers to the integration of advanced PETs. However, we have also observed significant variations in how the use of exchanged information for purposes beyond taxation is addressed in different DTCs. This could present challenges regarding the competence of the authorities involved in the exchange of information, and their possibility to use the received information. States generally adopt one of the three following approaches: restricting the use of received information solely to tax matters; allowing its use for additional purposes, subject to authorisation by the competent authority of the sending State; or permitting its use for non-tax purposes without requiring prior authorisation of the sending State (by using for instance a whitelist), provided it complies with the laws of both States.

Article 26(4) of the OECD-MC, encountered in the DTC between Colombia and Canada, mandates the exchange of information even if it is not relevant to the domestic tax interests of the requesting State. This raises an important question regarding spontaneous information exchange: does such a provision require States to spontaneously share information, even when it is not directly related to their own tax assessments? Since the amendment of Article 26 of the OECD-MC in 2005 (Section 2.1.1), this question must be answered in the affirmative for the exchange of information on request. In our view, this question does not play a role in the case of spontaneous exchange of information, since the relevant information has already been obtained in the course of a State's own investigation. Information already obtained should be exchanged with other countries spontaneously if an exchange instrument requires so.

Privacy and secrecy regulations may pose challenges in relation to information sharing. Some States are reluctant to share information with jurisdictions that do not adhere to equivalent standards of privacy and secrecy. This caution reflects a priority for protecting sensitive data and ensuring that international partners uphold comparable confidentiality levels. Such concerns highlight the importance of maintaining privacy and secrecy, by for example applying the EU GDPR standards to enable effective international collaboration. The need for similar privacy and secrecy standards can be viewed as an aspect of reciprocity as well, which has proven to be a significant consideration for States when exchanging information.

Additionally, laws governing the exchange of information between different levels of government can create barriers. In certain jurisdictions, prior authorisation is required before information can be used for purposes beyond tax administration and/or submission to third countries. This requirement may complicate the use of networks like FCInet, since in the spontaneous exchange with some countries, the data used for FCInet ma^{3}tch must have a visible relationship with the jurisdiction of the peer organisation beforehand, i.e. before the filter is shared. Creating an oversight is therefore important for the well-functioning of integrated information exchange systems (see the questionnaire in Section 3.3).

Adherence to OECD standards and the established frameworks of States like the U.S. and France, provide a strong foundation for effective information exchange. Notably, these States apply the principle of foreseeable relevance, though with a generally lower threshold for spontaneous exchanges compared to those requested. This reflects the practical difficulty of assessing relevance spontaneously, as the sending State may not fully grasp the recipient country's tax system. Despite these developments, challenges related to foreseeable relevance, privacy, secrecy, and domestic regulations remain. Addressing these issues will be important for improving the information exchange process within an international context.

3. *Does the way in which FCInet ma^{3}tch is applied, more specifically in the light of the right to privacy and the protection of personal data, have an impact on the assessment of whether the requirement of foreseeable relevance is met (Chapter 4)?*

As the use of FCInet ma^{3}tch is based on the existing international legal framework, it does not entail any additional obligations, and all information exchanged is treated in accordance with the applicable international legal framework. FCInet aims to eliminate as many hurdles as possible to facilitate the smooth and effective exchange of information between countries, making it more attractive and lowering the threshold for countries to join an exchange of information network. The matching process does not commence with the establishment of a local filter, but only when a State decides to share a filter (bilaterally). Every State will have its own local filter, and they can choose to connect a shareable filter with other States that also use FCInet. From the point of submission the verification request onwards after a hit, the regular legal rules around the exchange of information on request will take place and ma^{3}tch technology no longer plays a role.

Although ma³tch contains an aggregation of compressed non-reversible double hashed data and this data cannot be traced back to the personal data in the local filter of the sending State directly, the receiving State can determine whether there is a 'hit' between the filter and its own database, which can be validated by the sending State as belonging to a specific person. Key terms such as 'anonymised' and 'pseudonymised' data are legal concepts, so their interpretation may vary from country to country. In the event of a verified match between the filters and the receiving State's database, it could be argued that the sending State has subsequently validated that pseudonymised personal data were sent through the filter from the sending State to the receiving State. In our opinion, in the event of a match, in hindsight, privacy and data protection rules apply while sharing the filter. In fact, this only applies to the pseudonymised data that ultimately leads to a match. Since it is impossible to select the data in the filter accordingly, privacy and data protection rules should be considered to apply to the provision of the filter. Only if no match results from the provision of the filter, it can be said that privacy and data protection rules did not apply from a preliminary point of view.

The regular collection and processing of personal data in the ma³tch filter (start-up phase), the provision of pseudonymised data through the ma³tch filter (execution phase), the validation of a hit (verification phase) and the fulfilment of an information request (completion phase) constitute an interference in the private life of taxpayers by the *sending* State. The information provided for the request for verification as well as the request for tax information constitute an interference with the private life of the taxpayers by the *receiving* State. However, in view of Article 1 of Protocol No 1 to the ECHR, the payment of taxes is deemed to serve the public interest and a (European) State has far-reaching rights to achieve that objective, even if this requires an interference with the right to privacy and data protection under Article 8 ECHR. Article 17 ICCPR has a similar scope. For tax purposes, a breach is generally considered as justified.

The spontaneous provision of data resulting from an examination or investigation shall be deemed to be relevant to taxation in the receiving State provided that there is a minimal link between the information and the taxation in that country. Consequently, it can be assumed that the standard of foreseeable relevance, as laid down in Article 26 of the OECD-MC, is met. Since information must be exchanged between countries to the 'widest extent possible', a link can easily be assumed. If, after checking the filter, there is a hit, it means that there may be an actual link between the data present in the sending organisation and the receiving organisation. This means that in this phase of the technical operation, the foreseeable relevance standard for the exchange of information on request has also been met. However, after a hit has been determined, the sending State must validate the hit to determine that it is a match. Only after verification and validation of the hit can the actual relevance of the exchanged information – both in the spontaneous information exchange and the exchange on request – be confirmed. However, actual relevance is not a requirement to meet the foreseeable relevance threshold.

There is no doubt that a spontaneous provision of the filter contributes to improving the effectiveness and efficiency of taxation by the receiving tax authorities. In doing so, there must be a balance between, on the one hand, the processing of pseudonymised data and, on the other hand, the possibility for tax authorities to become aware of tax-relevant data that would otherwise not be obtainable or would be very difficult to obtain in the traditional way. Since the processed data is minimised, aggregated and double hashed, the breach of the protection of personal data is minimal, while, as far as we can see, there is no less disadvantageous way to obtain the information.

4. *How does the concept of foreseeable relevance compare to requirements for information exchange in criminal proceedings (Chapter 5)?*

In Chapter 5, the relevance criteria applicable to the exchange of information in criminal matters are assessed. Since the concept of foreseeable relevance as described in the tax law analysis is not used by the legal instruments applicable in criminal matters, the criteria enshrined in those instruments are compared to the foreseeable relevance concept to evaluate whether the use of the ma^{3}tch technology would be problematic for the purposes of information exchange in criminal matters.

The analysis suggests that as the criteria applicable to the exchange of information in criminal cases are quite flexible and potentially subject to broad interpretation, it can be concluded that the ma^{3}tch technology does not appear to be incompatible with the *applicable legal framework*. This technology seems to minimise the interference with individual rights such as the right to privacy and data protection since, in principle and by design, even basic information is only shared to the extent that the receiving authority already has a file about the person concerned and, thus, that the information is relevant.

While this mechanism appears to ensure an appropriate balance between investigative efficiency and fundamental rights protection, a general remark may be added according to which this 'hit/no-hit mechanism' could lead to an increasing reliance of both judicial authorities and LEAs to *prefer informal ways* (according to the criminal law concept of informality) of exchange even in cases in which formal channels, such as the issuing of a European investigation order for an exchange of information, would be an option. Informal exchanges in criminal matters distinguish themselves from formal exchanges for being, on the one hand, subject to *fewer procedural rules* and, on the other hand, for being geared towards the exchange of *information* and *intelligence* rather than sharing *evidence*. A growing preference for informal ways of exchange in criminal matters fosters general concerns about an overall lowering of another set of fundamental rights, including fair trial rights and procedural safeguards in criminal proceedings. While the use of ma^{3}tch also enables informal exchange of information in criminal matters, this technology provides for a considerable minimisation of the interference with the right to privacy and to data protection and it therefore represents a positive development in this field.

Based on the above we give the following reply to the principal research question:

> *"In relation to the spontaneous exchange of (tax) information via FCInet's ma³tch the principle of foreseeable relevance should be interpreted as the information to be exchanged is supposed to be of interest to the receiving State, in the sense that the information must at least be able to be of interest, which may be qualified as a less onerous requirement than the requirement of some degree of knowledge of an examination or investigation in the case of an exchange of information on request. The way in which competent authorities in jurisdictions (involved in the study) assess whether the principle has been met has emerged several insights, such as that legislation tends to place greater emphasis on the exchange of information on request than on spontaneous exchanges, that countries with more developed frameworks demonstrate a higher frequency of information exchange, that globally most countries adopt the OECD standard for the principle of foreseeable relevance, that privacy and secrecy regulations may pose challenges in relation to information sharing, whereas laws governing exchanges between various public administrative bodies can create barriers and, finally, adherence to OECD standards and other established frameworks provide a strong basis for effective exchange of information. The requirement of foreseeable relevance is not only a prerequisite for the lawfulness of the information to be provided, but also for complying with data protection rules for tax purposes. Although the concept of foreseeable relevance, as it has been described in tax law, does not apply to the exchange of information in criminal proceedings, the criminal law instruments examined present relevance criteria too. The way in which these are formulated suggests that spontaneous exchange of information could occur also through the ma³tch technology without raising issues of incompatibility with the relevant criminal legal instruments."*

6.2 Other conclusions

In the introduction to the research in Chapter 1, several related 'other questions' arose, which were answered in the course of the research. Here's a recap:

1. *Can the sharing of the filter be considered as some form of 'fishing', i.e. does the filter represents bulk data?*

The research shows that States are not at liberty to engage *fishing expeditions* or to request information that is unlikely to be relevant to the tax affairs of a given taxpayer (no bulk data sharing). A fishing expedition can be defined as a random or speculative request for incriminating information that has no apparent link to an examination or investigation (Section 2.1.1). Fishing expeditions refer, for example, to information requests that do not identify a specific taxpayer but have a broader scope to find information about taxpayers who do not comply with the rules or that do concern a *specific taxpayer*, but where the information request is addressed

to a very large number of countries. In the light of data protection rules, a fishing expedition qualifies as an arbitrary or disproportionate intervention by the public authorities and is impermissible (Section 2.2). In our view the sharing of the filter cannot be considered as a form of fishing expedition: 'wherever there is fishing, there is bycatch'[252], while FCInet ma³tch only identifies the *specific taxpayer*, which may also be involved in tax offences in another country. The foreseeable relevance standard should deter tax administrations from sharing unspecified bulk data with other States and sharing information that is not relevant for tax purposes or an investigation in another country. This is what FCInet ma³tch technology does: to prevent bulk requests and to limit follow-up to cases where there is a hit.

2. *How minimal must the individualisability of the person for the taxation by the receiving State be in order to meet the foreseeable relevance standard? Must each individual in the filter be mentioned by name?*

To meet the foreseeable relevance standard in spontaneous exchange, there must be a minimal link between each taxpayer in the filter and its interest for tax purposes in the receiving State (Section 2.3). It is not necessary that the name of each person in question is shared, which allows the use of hashed names to protect personal data. To meet the link, the persons in the filter must, however, be 'identifiable'. This means that the information provided is sufficient to identify a person. With FCInet ma³tch, hashed data is made available in the filter, but after a validated hit, that data must be classified as pseudonymised, because the person behind has become identified. It is up to the State that spontaneously makes the filter available to assess whether the data in the filter may have any relevance for taxation in the receiving country. In a specific investigation or examination of a person, there is usually a minimum level of relevance because there is a reasonable suspicion of non-compliance with a specific legal obligation in the source State, which may indicate relevance for taxation in the receiving State. When using ma³tch, in principle all persons whose hashed data is included in the filter are involved in an investigation, so that a minimum link with the receiving State will be assumed to be present quite easily.

3. *Need all data used for FCInet ma³tch also have relevance (to the peer organisation) in advance, so before sharing the filter?*

In principle the data used for FCInet ma³tch need relevance to the peer organisation at the time of sharing the filter (Section 2.3). The data used for ma³tch does not need to have relevance with the receiving jurisdiction before sharing, except in some rare cases where certain jurisdictions, for example, require *prior authorisation* by the sending State for the use of the data. This requirement of prior authorisation can play a role in, for instance, the use of exchanged information for other than tax purposes, disclosure to non-tax administrative bodies (for instance in criminal matters) or in case of transmission to third countries. In a few cases the standard of foreseeable relevance

252 See for instance *World Wide Fund for nature* (WWF), 'What is Bycatch? Understanding and Preventing Fishing Bycatch', retrieved from https://www.worldwildlife.org/threats/bycatch.

should therefore be met at the moment of obtaining this authorisation. The use by the sending State of a so-called 'whitelist' of cases in which prior authorisation for the use of exchanged data no longer needs to be obtained, for example in high-priority cases, can help to meet this requirement. In addition, in a rare number of States the competent authorities are obliged, based on domestic laws, to notify their residents of a spontaneous exchange of information prior to the exchange. In such cases, the competent authorities will have to demonstrate at the time of notification the taxpayer that the standard for foreseeable relevance has been met, which is earlier than the moment of the spontaneous sharing of the filter. For the application of FCInet ma³tch it is important to know whether such requirements apply to the participating countries in the network. To gain this insight, use can be made of the questionnaire as included in the preliminary conclusion of Chapter 3.

4. *Does the presence of a 'hit' after checking the filter by the receiving organisation implies relevance?*

A hit means that some characteristics in the sent filter are most likely also present in the system of the receiving State, though there is a chance of a so-called 'false positive', where the filter detects a hit, but the data match does not concern the same individual. If after checking the filter, there is a hit, it means that there may be an actual link between the data present in the sending organisation and the receiving organisation. The algorithms of the ma³tch software ensure that there is a standard chance of a random false positive hit when checking the filter. This is the result of the precision of the ma³tch filter. This precision can be set high, which means that the chance of a random false positive hit is very low (Section 4.2.1). However, the hit implies sufficient relevance for the receiving organisation to file a verification request to the sending State. It should be noted that this verification request contains personal data, which is subject to data protection rules for the receiving State. If the sending State validates the hit, this implies actual relevance. Also, this validation contains personal data, for which data protection rules apply for the sending State. So, a hit itself does not imply relevance, because it can also be a false positive. However, the greater the reliability of the algorithm used to build the filter, the smaller the chance that a false positive will occur. In other words, the higher the accuracy and precision, the greater the chance that a hit will lead to validation. It is therefore important to pursue the highest possible accuracy and precision with the ma³tch technology. Only after verification and validation of the hit can the actual relevance of the data exchanged be confirmed. However, actual relevance is not a requirement to meet the foreseeable relevance standard. A no match means that there are no common characteristics with the dataset on which the shared filter is built, at least not under the name under which the receiving organisation knows the person or suspect. Even in the event of a hit, no tax-relevant information is exchanged yet. This is done only after the receiving State requests it.

6.3 Recommendations

In light of the above, this study provides some recommendations to improve the effectiveness of the exchange of information, considering the need to exchange information efficiently as well as the use of new technologies, such as FCInet ma[3]tch.

A first more general recommendation resulting from Chapter 2 is two-fold: to review the concept of foreseeable relevance in the OECD-MC considering the use of digital technologies and to update the privacy and data protection rules to facilitate the exchange of information between States. More specifically, this means that, in view of the current developments in the use of digital technologies by tax administrations, the OECD will have to review Article 26 and the interpretation of foreseeable relevance according to these developments. Following this review, countries will need to also introduce Protocols to their tax treaties or change their domestic rules to facilitate exchange of information for instance with other non-tax authorities such as money laundering authorities and/or supervisory bodies. This can be arranged bilaterally by countries or via a protocol at, for example, the MAAC or the DAC.

Furthermore, countries will need to revisit the definition of foreseeable relevance to ensure that exchange of information takes place in a swift and efficient way. For this purpose, the definition of the DAC7 on foreseeable relevance can be regarded as a good practice for countries to introduce in their tax treaties. Article 5a of DAC7 states that the requested information is foreseeably relevant where, at the time the request is made, the requesting authority (receiving State) considers that, in accordance with its national law, there is a reasonable possibility that the requested information will be relevant to the tax affairs of one or several taxpayers, whether identified by name or otherwise, and be justified for the purposes of the investigation. The restriction introduced by the OECD on the minimum link in case of spontaneous exchange is left to the interpretation of the sending State and the reasonable possibility to be assessed by the receiving State that the information can be of use for purposes of an investigation.

A second recommendation concerns the few cases where prior authorisation from the source State for the use of (tax) information for purposes other than taxation or for the transmission of the information to third parties is required and, in rare cases, prior notification to the taxpayer (Chapters 2 and 3). The requirement of prior authorisation can play a role in exchanges for other than tax purposes, to non-tax administrative bodies (for instance in criminal matters, Chapter 5) or in case of submission to third countries. In such cases the standard of foreseeable relevance should be met at the moment of obtaining prior authorisation. The use by the sending State of a whitelist of cases in which prior authorisation for the use of exchanged data no longer needs to be obtained could fulfil this requirement. In a rare number of States the competent authorities are obliged, based on domestic laws, to notify their taxpayers of a spontaneous exchange of information. In such cases, the competent authorities will have to demonstrate at the time of notification that the standard for foreseeable relevance has been met, which is earlier than the moment of the spontaneous exchange

itself. For the application of FCInet ma³tch, it is important to know whether such provisions apply to the participating countries. Therefore, creating an oversight of such requirements with respect to the organisations participating in the FCInet ma³tch network is recommended. The questionnaire to identify relevant aspects for the standard of foreseeable relevance in Chapter 3 can be used for this purpose. However, given the global drive for international exchange of tax information 'to the widest possible extent', such provisions are rare and will continue to decline in number.

In addition, privacy and tax secrecy regulations may pose challenges in relation to information sharing. Tax secrecy concerns provisions in national legislation that are intended to ensure that information about a taxpayer remains confidential and is protected against unauthorised disclosure. Some States are reluctant to share information with States that do not adhere to equivalent standards of privacy and tax secrecy. This caution reflects a priority for protecting sensitive data and ensuring that international partners maintain comparable levels of confidentiality. For (participating) countries – including countries outside the EU – it is important to align their local privacy rules with those of the EU GDPR to (continue to) guarantee privacy and data protection. At the time of writing, countries are adopting this regulation in their domestic laws, and replacing the previous rules based on the EU GDPR.

To conclude, the use of FCInet ma³tch contributes to data minimisation and privacy protection. However, there is also a point of attention in the technical process that should not be lost sight of. For the exchange of information by means of ma³tch it is necessary to the peer organisation to create a local filter with corresponding fields and high-quality data, e.g. first name, last name, date of birth, to be able to test whether the characteristics of an individual in the local filter are also present in the received filter. In addition, it is important to pursue the highest possible accuracy and precision with the ma³tch technology. Although the chance of a false positive after checking the filter is small, in rare cases a receiving State may be obliged under (tax exchange) provisions to share, for example, the detection of a 'hit' with a third party (as in Italy, where the *Guardia di Finanza* acts as both a tax authority and a criminal investigative body). Such a provision may violate the individual's right to privacy and data protection, if it subsequently turns out that this is not the person in question. To reduce this risk as much as possible, FCInet could consider obliging participating countries – for example by including this in the *User Protocol* – to always first request validation *within the FCI network*, before providing personal information to a third party. Furthermore, peer organisations are required to have established the legal framework, policies and procedures concerning exchanges of information. They may only request and exchange information via FCInet ma³tch if this is allowed under the applicable international and domestic laws, including relevant (mutual legal assistance) treaties and international agreements, of both the sending and receiving organisation. Consider that the data in the filter qualify as pseudonymised data and that the use of FCInet ma³tch constitutes an interference with the private life of taxpayers, an advantage of using FCInet ma³tch compared to the traditional way, is that the breach of the protection of personal data is minimal or does not breach at all, in the absence of a hit.

Although the technology in question does, in principle, not seem to be incompatible with criminal law standards – it appears to be even more protective compared to individual rights, such as the rights to privacy and data protection, that are usually affected – it could be useful to establish common rules to *prevent possible discriminatory elements* in the filters (Section 5.5). As a first step, FCInet might consider including such rules in the *User Protocol*. The cooperation in the exchange of information means, that there is an interdependence between peer organisations regarding the reliability of the data in the filter and the compliance with international and domestic regulations. Maintaining the 'equality in the cooperation' is of great importance for the proper functioning of the FCInet ma³tch network for the international exchange of tax information. From a criminal law perspective, it is also desirable to continue to draw attention to the need for common rules for the participating organisations in order to prevent even unconscious discriminatory elements in the filters.

6.4 Final remarks

Despite an increase in the number of information exchanges, in the amount of information to be exchanged and in the use of data exchanged for non-tax purposes, since 2010 only the Commentary on Article 26 OECD-MC has been changed, not the wording itself. However, the 2024 update to Article 26 of the OECD Commentary shows that the OECD aims to ensure a more swift and efficient exchange of information among States, and to facilitate the use of the information exchanged by competent authorities of other States and by third countries, without the need for prior authorisation (or notification) from the sending State. So even though under certain circumstances the application of FCInet ma³tch will have to take into account the requirements of prior authorisation (or notification) for certain countries, the global trend is towards a more flexible exchange of information.

It is not easy to strike the right balance between respect for the fundamental rights of taxpayers and the need for tax authorities to have instruments at their disposal to effectively monitor compliance with tax obligations and to combat tax avoidance and evasion. FCInet ma³tch provides for the possibility to innovate regarding the development of an exchange of information system so that countries are not left behind. Similar to the purpose of the amendments to Article 26 of the OECD-MC, FCInet also aims to assist other States in achieving proper taxation, to prevent bulk requests and limit further investigation to cases where there is a 'match' between a person in the database of the sending country and the database of the receiving country. FCInet ma³tch aims to eliminate as many hurdles as possible to facilitate the smooth and effective exchange of information between countries, making it more attractive and lowering the threshold for countries to join an exchange of information network.

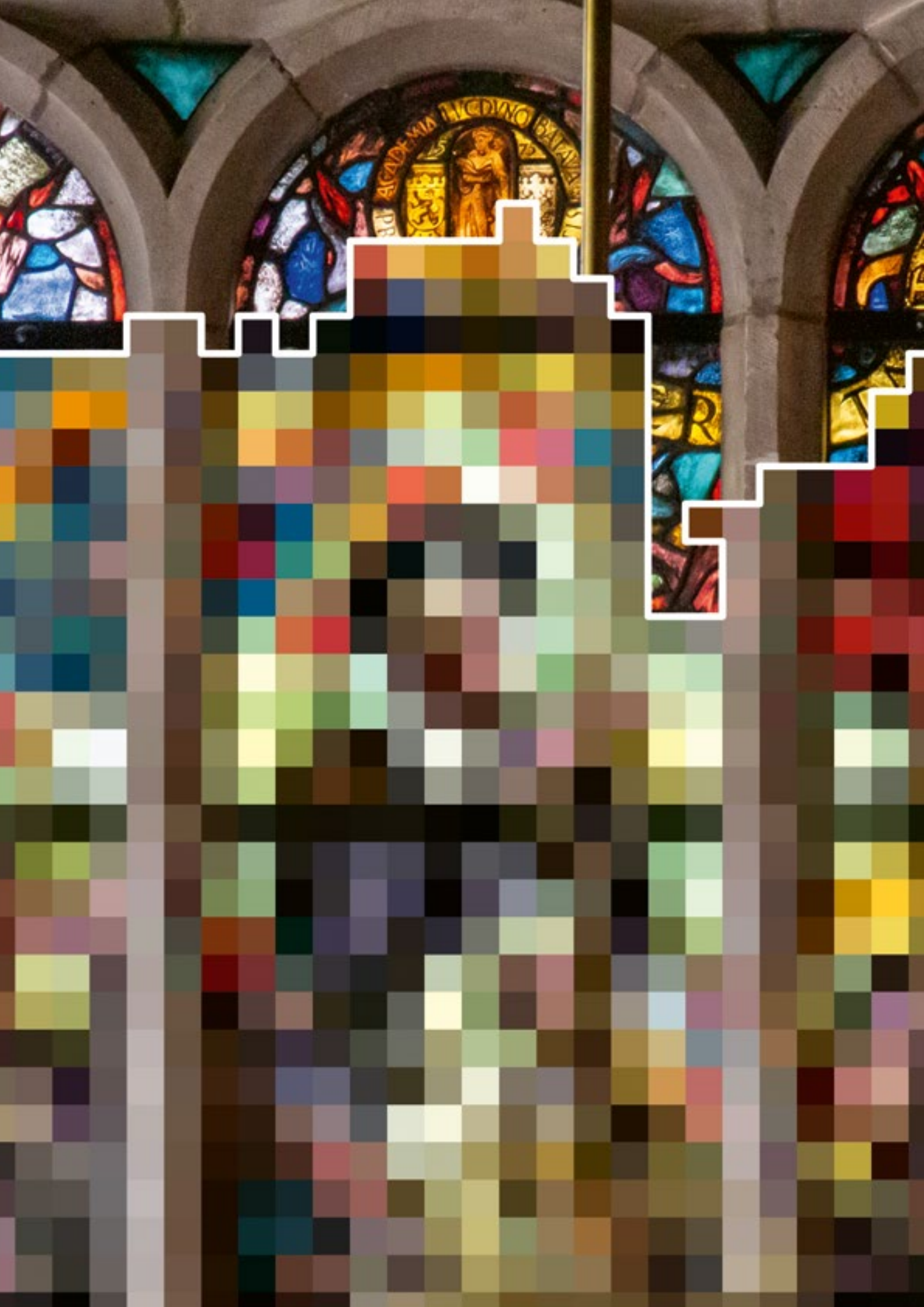
Balancing between privacy and knowledge is a continuous struggle. Collecting, combining and analysing information offers advantages, but it can also easily breach on the privacy of citizens when it comes to personal data. Benefits of sharing data include increasing knowledge and identifying trends and threats that would otherwise go unnoticed. Ma³tch helps to limit the amount of information to be exchanged.

Instead of providing privacy-sensitive information about an individual, the ma³tch technology can be used to spontaneously share data that may be able to be relevant to the receiving organisation. Also, in the event of a hit, a request is handled in a privacy-friendly manner, so that no more individuals' data is processed than strictly necessary.

Particular attention should be given to the role of tax officials as gatekeepers who manage the flow of information, both internationally and within domestic boundaries among associated public administrative bodies, under established legal frameworks. This gatekeeper role is crucial, as officials must ensure that data sharing adheres to legal requirements. Systems such as FCInet ma³tch could be well suited to support this role, by enhancing privacy and implementing controls that align with national and international regulations regarding the safeguarding of taxpayer rights and efficient exchange of information.

While the foreseeable relevance concept can be considered reactive in nature – because relevance is the assessment criterion – the FCInet ma³tch technique is also proactive in nature, by identifying links between countries in high-priority matters related to combating tax fraud, corruption, money laundering, terrorism financing and other (tax) crime. The shift from a more reactive to a more proactive nature can be considered time saving. FCInet tackles two problems that affect the efficiency of traditional methods of information exchange. Firstly, the challenges posed by the processing of the ever-increasing amount of data received by tax administrations, by enabling international organisations to identify individuals, whose activities may be able to be of interest to another country on the basis of aggregated compressed non-reversible 'double hashed personal data' and, in case of a validated hit, to request additional information. And secondly, the quickly and accurately identifying of specific individuals, after which a peer organisation can request targeted questions, which minimises the risk of providing bulk data or conducting fishing expeditions.

The foreseeable relevance standard should deter tax administrations from making unspecified bulk requests to other States and requesting information that is not relevant to the investigation in question. This is what FCInet mat³ch technology does: to prevent bulk requests and to limit follow-up to cases where there is a hit. Technologies like FCInet ma³tch offer the capability to implement and enforce specific limitations within both international and domestic systems of information exchange. This built-in flexibility allows for the establishment of tailored controls that respect each country's legal boundaries and institutional practices, rather than relying solely on manual legal application for each spontaneous information exchange.



Annex 1

Descriptions of States involved in the comparative analyses

1.1 The EU States

1.1.1 France

The applicability of domestic rules

The central competent authority in France for handling exchange of information (hereinafter: EOI) requests is the General Directorate of Public Finance (*Direction Générale des Finances Publiques,* hereinafter: DGFIP). The DGFIP is responsible for tax administration within the Ministry of Budget, Public Accounts, the Civil Service, and State Reform (*Ministère du Budget, des Comptes Publics, de la Fonction Publique et de la Réforme de l'État*). Specifically, these requests are managed by the International Affairs Office (*Bureau des Affaires Internationales*) within the Tax Examination Branch (*Sous-direction du Contrôle Fiscal, CF3*). According to Article 55 of the French Constitution, treaties take precedence over domestic laws.[253]

Article L.76B of the French Book for Tax Procedures (hereinafter: TPB) stipulates that the taxpayer only needs to be notified at some point before the actual tax collection, allowing the tax administration ample time to gather data without immediately notifying the taxpayer.[254] The collected data may be shared domestically within different branches of the tax administration, but it is prohibited to share this data with other domains of public administration, such as the administrative police.[255] An exception to this rule exists: taxpayer information may be shared with the criminal investigation police, as permitted by Article L.135L of the TPB.[256] It is also interesting to note that France utilises several mutual assistance agreements with overseas territorial communities, such as New Caledonia and French Polynesia, and employs Article 26 of the OECD standard to facilitate these territorial exchanges.[257]

253 Global Forum on Transparency and Exchange of Information for Tax Purposes, *Peer Reviews France 2011: Combined: Phase 1 + Phase 2*, Paris: OECD Publishing (2011), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews-france-2011_9789264114708-en.htm (hereinafter: Global Forum Peer Review France 2011), p. 48.

254 E. Kristofferson, M. Lang, P. Pistone, J. Schuch, C. Staringer & A. Storck, *Tax Secrecy and Tax Transparency*, Berlin, Germany: Peter Lang Verlag 2014 (hereinafter: Kristofferson et al. 2014), p. 413.

255 Kristofferson et al. 2014, p. 423-424.

256 Kristofferson et al. 2014, p. 423.

257 Kristofferson et al. 2014, p. 423.

The EOI mechanisms established by France therefore allow for the EOI for both criminal and civil (tax) purposes.[258] The OECD-TIEAs explicitly provide for this in their Article 1.[259] Regarding international exchanges of information, French domestic law explicitly authorises the tax administration to bilaterally send data to other States that have concluded an EOI agreement with France. This is based on Article L.114 of the TPB, provided that the other State has similar secrecy rules or respects French secrecy rules concerning the exchanged information, as outlined in Article R*114A-1 of the TPB. Several exceptions to the types of information France may exchange are specified in Article R114A-2 of the TPB. Additionally, France can exchange information with EU Member States without a specific EOI treaty, but only if the exchange is reciprocal, as stated in Articles L.114A, R114A-3, and R*114A-4 of the TPB. It is also noteworthy that, even without paragraphs 4 and 5 of Article 26 of the OECD-MC, the French competent authority can exchange all types of information, as French domestic law imposes no restrictions on information exchange with France's partners.[260]

Taxpayer rights and secrecy rules

Regarding secrecy, it is noteworthy that confidentiality in tax law has not been recognised by the Constitutional Council (*Conseil Constitutionnel*) in France as having constitutional value. However, it remains a crucial aspect of French tax law. For instance, 'the secrecy of taxation' is considered a fundamental principle. This principle, along with the 'professional secrecy' of tax officials, constitutes the two main elements of tax secrecy in France.[261] Here, article L.117 of the TPB is quite interesting, as it allows agents within the General Directorate of Public Finances to share information, either spontaneously or upon request.[262] To collect this data, the tax administration has various tools at its disposal, such as requests for additional information.[263] According to domestic case law (*Conseil d'État* (Supreme Court), 27 April 1987, *Menella*, 8/7 SSR, No. 63634), France is not required to inform the taxpayer when collecting information from these third parties.[264]

An important distinction in French DTCs lies in the obligations imposed on contracting States: some DTCs mandate the active procurement of certain information, while others merely require the transmission of information that is already available. Concerning the use of information for purposes beyond taxation, certain DTCs permit such use, but only if it is sanctioned by the domestic laws of both contracting States, as exemplified by the DTC with Bahrain in article 22A (2).

258 Global Forum on Transparency and Exchange of Information for Tax Purposes, *Peer Reviews France 2018 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2018), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-france-2018-second-round_9789264291058-en.html, (hereinafter: Global Forum Peer Review France 2018), p. 86.

259 Global Forum Peer Review France 2011, p. 68.

260 Global Forum Peer Review France 2018, p. 84-85.

261 Kristofferson et al. 2014, p. 411-412.

262 Article L.117 of the Tax Procedures Book and Kristofferson et al. 2014, p. 411.

263 Kristofferson et al. 2014, p. 413.

264 Kristofferson et al. 2014, p. 412-415 and CE 27 April 1987, 8/7 SSR, No. 63634 retrieved from: https://www.legifrance.gouv.fr/ceta/id/CETATEXT000007623542/.

Reciprocity in information exchange represents another reoccurring aspect of these treaties. Upholding this principle can be particularly challenging in the context of spontaneous exchanges. In some DTCs, such as the agreement with Belgium, reciprocity is unconditional. However, in other instances, such as with Germany and Finland, exceptions are permitted that allow for the refusal to exchange information reciprocally when it poses a threat to State sovereignty, public security, or the general interest of the State. These exceptions may impede the speed and efficiency of spontaneous exchanges, as it may limit the kinds of information to be exchanged.

Instrument on the exchange of information

France utilises both DTCs and OECD-TIEAs to exchange information, adhering to Article 26 of the OECD-MC. The EOI provisions in French DTCs generally apply only to the taxes covered by the DTC, as specified in Article 2 of the OECD-MC. In terms of personal scope, France exchanges information only concerning residents of one of the contracting States under the DTC. However, under French DTCs, information related to a permanent establishment in a third country that belongs to a French company is not exchanged. The French DTCs concluded with EU Member States are less restricted in many respects, as they are governed by a broader obligation to exchange information based on Directive 2011/16/EU (DAC).

France has also concluded multiple OECD-TIEAs, in which it also provides for spontaneous exchange of information. For example, the OECD-TIEA with Aruba provides for spontaneous exchange in Article 6, where it obliges the contracting parties to spontaneously exchange information that in relation to Article 1 of the agreement, could be relevant to the other contracting party. Generally speaking, the OECD-TIEAs concluded by France include all taxes existing within the contracting States within their scope. It is also notable that within most of these OECD-TIEAs contracting parties need to provide information even if the requested party does not need it to apply its own tax legislation (Article 5(2) OECD-TIEA between France and Aruba). Generally, the OECD-TIEAs concluded by France encompass all taxes levied within the contracting States under their scope.

The standard of foreseeable relevance

The study has not clarified how the State deals with the standard of foreseeable relevance. This requires further (local) investigation.

Concluding statement

In examining France's domestic law and international agreements, it is evident that the provisions for privacy and spontaneous information exchange align with the principles established in Article 26 of the OECD-MC. France's use of OECD-TIEAs and DTCs supports the principle of proactive data sharing, consistent with OECD standards.

1.1.2 Germany

The applicability of domestic rules

The BZSt is the designated authority in Germany for managing the international EOI related to taxation and serves as the primary contact for foreign administrations requesting information from German tax authorities. Within the BZSt, a specialised unit is responsible for handling EOI matters concerning direct taxation. The powers of German revenue authorities for investigation are delineated in Sections 88 to 140 of the Fiscal Code (*Abgabenordnung*, hereinafter: AO). Specifically, Section 93(1) mandates that "participants and other persons must provide the revenue authority with the information necessary to ascertain facts". Additionally, Section 117 of the AO allows the revenue authorities to offer international legal and administrative assistance based on national agreements, relevant European legal instruments, and the EC Mutual Assistance Act. This Section also states that the implementation of such assistance must adhere to the provisions applicable to taxes. Consequently, Section 93(1) applies to EOI purposes, indicating that Germany's domestic information-gathering procedures are applicable for both domestic and international information requests. However, Germany's search and seizure powers for criminal investigations cannot be utilised to address incoming EOI requests.

Taxpayer rights and secrecy rules

Regarding data collection and secrecy, the German tax administration has the discretion to gather evidence as stipulated in Section 92 of the AO. Both taxpayers and third parties are obligated to cooperate and disclose all relevant information related to taxation, as specified in Sections 90(1) and 93 of the AO. However, this authority is constrained by privacy rights and must adhere to the principle of proportionality. The data collected must be suitable for taxation purposes and necessary to ensure proper tax administration. Disproportionate data collection is restricted by Section 20(2) of the *Bundesdatenschutzgesetz* (hereinafter: BDSG) or Germany's Federal Data Protection Act.

The sharing of tax information with other authorities is governed by tax secrecy rules codified in Article 30 of the AO. This article emphasises that the purpose of the information exchange is critical for its legality when shared with other German authorities. Furthermore, tax information may also be disclosed outside of tax courts to entities such as criminal prosecutors and courts, but only to the extent necessary for the criminal proceedings, ensuring adherence to the principle of proportionality.

A notable feature of German law concerning the EOI is the provision for "unilateral discretionary sharing of information", as outlined in Section 117(3) AO. This provision allows the German tax authority to unilaterally disclose information if certain conditions are met, such as ensuring reciprocity with the foreign recipient country. This process closely resembles spontaneous exchange, as it does not require a formal request from another country and can be initiated at the discretion of the German tax authority.

The BZSt makes in its administrative assistance a clear distinction between automatic EOI and non-automatic EOI.[265] According to the BZSt, non-automatic EOI encompasses both spontaneous EOI and EOI on request (hereinafter: EOIR). The BZSt appears to apply the standard of foreseeable relevance equally to both spontaneous EOI and EOIR.

However, the BZSt distinguishes between spontaneous EOI to EU members and non-EU members. It broadly states that with respect to EU members, almost any information may be transmitted if it can aid in the accurate taxation of a taxpayer in the other EU Member State. This seems to allow for more flexibility than under the foreseeable relevance principle for exchanging information. Conversely, concerning non-EU members with which Germany has a DTC, it emphasises the importance of having an information clause and reciprocal arrangements to determine whether spontaneous EOI should be pursued. The leaflet then provides a list of indications for when spontaneous EOI should be conducted, such as suspicions of tax evasion or profit shifting. This approach mirrors the practice of the U.S. regarding EOI.

Instrument on the exchange of information

In its DTCs, Germany generally adheres to Article 26 of the OECD-MC, typically providing a narrow EOI clause that is restricted to the enforcement of the convention. This approach means that not all types of taxes are covered. Germany places significant emphasis on reciprocity and has expressed concerns that many countries fail to meet reciprocity standards due to ineffective tax administrations and enforcement practices. However, there are instances where Germany adopts a broader scope, extending EOI not only for the effective levying of the taxes mentioned in the convention, but also for combating tax evasion. Some DTCs allow for a wider use of the information exchanged. Use for purposes beyond taxation is then permitted, however only if such use is authorised under the laws of both States and with the consent of the competent authority in the supplying State. For example, the DTC between Germany and Sweden, as outlined in Article 29(2), permits such extended use under specified conditions.

The standard of foreseeable relevance

Germany's treaty policy is informed by principles derived from the OECD Commentaries on the OECD-TIEA and the OECD-MC. Germany's approach suggests that a prohibition on 'fishing expeditions' does not necessitate a strict requirement to provide specific identifying details, such as the name and address of an individual, to meet the foreseeable relevance standard. Instead, the OECD standard should be assessed in the context of the information exchange. For instance, if a request concerns the identity of an individual associated with a particular bank account, providing the bank account number may suffice for the request. Additionally, if a bank account is involved in multiple suspicious transactions, the OECD standard does not preclude

265 Bundeszentralamt für Steuern, *Merkblatt zur zwischenstaatlichen Amtshilfe durch Informationsaustausch in Steuersachen (Stand: 1. Januar 2019)*, BMF v. 29. Mai 2019 - IV B 6 - S 1320/07/10004 :008, BStBl. I 2019, 480, retrieved from: https://karriere.bzst.de/SharedDocs/Downloads/DE/intern_amtshilfe/merkblatt_zwischenstaatliche_amtshilfe.pdf?__blob=publicationFile&v=10.

the spontaneous EOI with a partner country without specifying the individual's name and address.

As an EU Member State, Germany has integrated Article 9 of Directive 2011/16/EU (DAC) into its national legislation. Consequently, Germany facilitates spontaneous exchanges of information with all EU Member States through Paragraph 8 of the EU-*Amtshilfegesetz*.

Concluding statement

In examining Germany's domestic law and international agreements, the provisions for data collection, privacy, and spontaneous information exchange align with the principles established in Article 26 of the OECD-MC. Germany's approach, including its implementation of unilateral discretionary sharing and adherence to both the OECD standards.

1.1.3 Italy

The applicability of domestic rules

Italy presents a unique situation in that it has two competent authorities for the EOI. The *Dipartimento delle Finanze* (hereinafter: DF), a Directorate of the Italian Ministry of Economy and Finance, serves as the primary competent authority for EOI in Italy, including in the fields of VAT, tax collection, and excises. Additionally, the *Agenzia delle Entrate* (hereinafter: AE) and the *Guardia di Finanza* (hereinafter: GDF), as operational revenue services, are both authorised to act as competent authorities.[266] In practice, this means that both the AE and the GDF are permitted to directly send outgoing requests to their counterparts and receive incoming requests from other jurisdictions, all under the supervision of the DF. The AE and the GDF share responsibilities in compliance functions, which can result in situations where one agency receives a request while the individual who is the subject of the request is under examination by the other. For the purposes of this discussion, both agencies will be collectively referred to as the 'tax authority'. Going forward, we will refer to both agencies together as the 'tax authority'.

The Italian tax authority has been granted extensive access powers, which, combined with stringent tax reporting and disclosure obligations imposed on taxpayers and third parties, create an environment conducive to a high level of tax transparency. Under Article 64 of the Presidential Decree of 1973 (hereinafter: PD 1973), the tax authority is authorised to collect data on taxpayers and various third parties.

All the gathered tax data is stored in the *Anagrafe Tributaria* (hereinafter: AT), the primary data warehouse of the Italian tax authority. Documentation of the authority's actions is also maintained within the AT. The information housed in the AT is protected by professional secrecy, as stipulated in Article 36 of PD 1973. Internal exchange of this information is governed by strict protocols.

266 Global Forum on Transparency and Exchange of Information for Tax Purposes, *Italy 2017 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2017), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-italy-2017-second-round_9789264283800-en.html, p. 20-21.

As previously mentioned, the Italian tax authority is unique in that it consists of two distinct entities, one of which, the GDF, also functions as a *fiscal police force with the authority to investigate tax crimes*. However, access to information in the AT is not uniform across departments. The GDF and the AE have different levels of access rights. When a department does not have direct access to specific information, it must file a formal request, justifying that the information is necessary to fulfil its institutional responsibilities.

According to Article 6 of Law 212 of the *Statuto Dei Diritti Del Contribuente* (The Taxpayer's Bill of Rights), taxpayers must be *notified* when information is being collected under domestic tax law, including when this information is gathered in response to an EOI request from another tax administration. Sharing information about a tax case with other authorities is prohibited under Article 63 of PD 1973, unless such disclosure is mandated by a court order or explicitly provided for by law. It is also important to note that information collected during a criminal investigation by the GDF, pursuant to Article 329 of the Italian Criminal Procedure Code, is subject to stricter confidentiality rules compared to those governing tax investigations.

Taxpayer rights and secrecy rules

The Italian Constitution provides that treaties take precedence over domestic law (as established by Constitutional Court judgments no. 348 and 349), meaning that EOI does not violate the confidentiality obligations under Article 68 of PD 1973. Italian law does not require the partner country in an EOI to uphold domestic tax secrecy, nor does it enforce a dual criminality principle. However, Italy reserves the right to withhold information from countries that do not meet a certain level of reciprocity in EOI. Information received under an EOI is sent to either the GDF or the AE. The data is not forwarded to local offices or units, and only the information relevant to the case is translated into Italian and transmitted to the requesting unit.

Italy includes provisions for spontaneous EOI in all its OECD-TIEAs, such as Article 4 in the OECD-TIEA with Lithuania. Additionally, Italy exchanges information spontaneously with EU Member States in accordance with Directive 2011/16/EU (DAC). This directive was incorporated into Italian law through Legislative Decree No. 29 of March 4, 2014, thereby also mandating spontaneous exchange of information.

Instrument on the exchange of information

As previously demonstrated, the Italian tax authority has broad access to various types of information relevant for tax purposes. While Italy, unlike Germany, does not permit unilateral EOI, it actively participates in EOI under DTCs and OECD-TIEAs. It also aims to align the wording of Article 26 OECD-MC in its DTCs, and it does not restrict EOI based on the wording from older versions of Article 26. Additionally, Italy incorporates paragraphs 4 and 5 of Article 26 OECD-MC in its treaties. These provisions ensure that information is shared even when it is not directly relevant to the State providing the information, and that bank secrecy cannot be invoked to limit the exchange of information (see in this respect Fort & Rust 2012). An example of this can be seen in Article 25 of the DTC between Italy and Liechtenstein.

The standard of foreseeable relevance

The study has not clarified how the State deals with the standard of foreseeable relevance. This requires further (local) investigation.

Concluding statement

In analysing Italy's domestic law and international agreements, it is evident that the provisions for data collection, privacy, and spontaneous information exchange are consistent with the principles set forth in Article 26 OECD-MC. Italy's approach reflects this alignment by adopting the OECD standards in its DTCs and OECD-TIEAs and shows no signs of major limitations to the EOI.

1.1.4 Spain

The applicability of domestic rules

The competent authority in Spain for handling EOI requests is the head of the Information Office of the Spanish Tax Administration (*Equipo Central de Información*, hereinafter: ECI). The scope of the ECI's authority to collect taxpayer data and information from third parties is outlined in Article 93 of the General Tax Code (*Ley General Tributaria*, hereinafter: LGT).

Taxpayer rights and secrecy rules

The Spanish Constitutional Court underscores that tax confidentiality, protection, and privacy are derived from the right to privacy and personal data protection, as enshrined in Article 18 of the Spanish Constitution (*Constitución Española*, hereinafter: CE). According to the Constitutional Court's jurisprudence (STC 45/1989), tax secrecy in Spain is grounded in the protection of economic privacy. However, the obligation to pay taxes (Article 31 CE) takes precedence over economic privacy, creating an exception that allows tax authorities to collect necessary information. Nonetheless, safeguards are in place to prevent misuse, including restrictions on using collected data for purposes other than those legally intended (Article 95 LGT).

Spain adheres to the principle of proportionality, ensuring that information collected by any government layer is used solely for purposes necessary to fulfil its legal authority. Notably, Spanish law addresses the collection of bank information explicitly; Article 93.3 of the LGT establishes that bank secrecy cannot prevent the tax authority from accessing information. The tax authority is permitted to share information domestically, that is with government authorities, only under the conditions specified in Article 95 LGT. In all other instances, tax information cannot be shared with other authorities without the taxpayer's prior consent.

Instrument on the exchange of information

Spain employs a network of DTCs and OECD-TIEAs and adheres to Directive 2011/16/EU (DAC) for EOI. In its DTCs, Spain consistently mirrors the language of the OECD-MC, particularly Article 26, adhering to the standard of foreseeable relevance. Spain has adopted the fourth paragraph of Article 26, thus mandating the EOI even if it is not required for its own tax purposes. Furthermore, Spain has incorporated

the fifth paragraph, which overrides bank secrecy rules. However, this provision is not universally applied across all partner countries; for instance, it is not included in the DTC with the Netherlands. Nevertheless, this restriction is mitigated by the incorporation of Directive 2011/16/EU (DAC) into national law, which addresses the limitation on the collection of banking information. However, challenges may persist with regard to non-EU countries.

Spain's OECD-TIEAs are predominantly concluded with jurisdictions deemed unsuitable for a DTC due to their low or negligible taxes on profits or income. These OECD-TIEAs are generally narrower in scope compared to DTCs but offer more specific provisions. For instance, the OECD-TIEA between Spain and Aruba outlines the procedure for spontaneous EOI in Article 6. Article 6(1) of this OECD-TIEA, details circumstances that necessitate the spontaneous EOI. This obligation arises if there is a suspicion of potential tax loss in the other contracting State, if a taxpayer obtains a tax reduction or exemption that could increase tax liability for the other party, if business transactions between taxpayers from different parties are structured to create tax savings, or if there are artificial profit transfers within corporate groups. Additionally, any information obtained because of an investigation based on previous data exchanged by one of the parties, that could be relevant for assessing tax liability in that party, must also be exchanged.

The standard of foreseeable relevance

Spain does not mandate specific information to demonstrate foreseeable relevance. However, the requesting jurisdiction must furnish the necessary elements to identify the taxpayer or group of taxpayers. Additionally, Spain does not prescribe a particular form for EOI requests, allowing flexibility in the submission process.

Concluding statement

In examining Spain's domestic law and international agreements, it is evident that Spain's provisions for data collection, privacy, and spontaneous information exchange are in alignment with the principles established in Article 26 of the OECD-MC. Spain's approach integrates the OECD standards through its network of DTCs and OECD-TIEAs, and it adheres to Directive 2011/16/EU (DAC) for effective exchange of information.

1.2 Non-EU States

1.2.1 Canada

The applicability of domestic rules

The Canada Revenue Agency (hereinafter: CRA) handles EOI requests, with the *Minister of National Revenue* as the competent authority. The CRA's authority comes from the *Income Tax Act* (hereinafter: ITA), allowing the Minister to access information for tax purposes, including EOIs.[267] These powers are delegated to CRA officials through the Commissioner of Revenue under Section 220 of the ITA.[268]

The CRA may collect data from residents and any individuals or entities conducting business in Canada, including information or documents located outside Canada that may be relevant to tax administration or enforcement, as stipulated in Section 231.6 of the ITA. The CRA's tax compliance enforcement powers are derived from Sections 231.1 and 231.2 of the ITA. In *Queen v. McKinlay Transport Ltd.* the Canadian Supreme Court determined that taxpayers should have a very low expectation of privacy.[269] This is notable given Canada's extensive privacy protections under the Constitution Act, the ITA, the Privacy Act (Revised Statutes of Canada 1985, c. P-21), and the Access to Information Act (hereinafter: AIA), among others.[270] A distinction is made between civil and criminal tax matters, with the latter subject to stricter search and seizure protections. Unlike the U.S., Canada operates under a principle of proportionality in data collection, resulting in a more constrained approach to data gathering.[271]

Taxpayer rights and secrecy rules

Data collected by the CRA may be shared internationally under subparagraph 241(4)(e)(xii) of the ITA, which stipulates that tax information can only be exchanged pursuant to a tax treaty or listed international agreement.[272] This exchange is also permissible under Section 8(2)(f) of the Privacy Act 1985 regarding privacy considerations. Such information may be shared internationally based on a tax treaty or international agreement, which, according to Section 3 of the Tax Convention Act, has the force of law in Canada and prevails over domestic law, even in cases of inconsistency, as confirmed in *TG Andison v. MNR*.[273]

267 Global Forum on Transparency and Exchange of Information for Tax Purposes, *Canada 2017 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2017), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-canada-2017-second-round_9789264280137-en.html, p. 67-75.

268 OECD Commentary 2019, p. 71.

269 Kristofferson et al. 2014, p. 219-221 and Canadian Supreme Court 29 March 1990, *R. v. McKinlay Transport Ltd.*, SCC: 20761, retrieved from: https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/585/index.do.

270 Kristofferson et al. 2014, p. 212-219.

271 Kristofferson et al. 2014, p. 224-225.

272 Subparagraph 241(4)(e)(xii) of the *Income Tax Act* (Canada).

273 Kristofferson et al. 2014, p. 233-234 and Canadian Supreme Court 9 January 1995, *T.G. Andison v. Minister of National Revenue*, [1995] 1 C.T.C. 203, retrieved from: https://www.uniset.ca/other/cs6/95DTC8085.html.

Instrument on the exchange of information

Regarding international treaties for information exchange, Canada aligns its income tax treaties with the OECD-MC, primarily following Article 26 for EOI provisions. While the CRA facilitates spontaneous exchanges, this is not explicitly stated in the income tax treaties. Canada has also entered several OECD-TIEAs, some of which explicitly provide for spontaneous exchange.

The standard of foreseeable relevance

For instance, the OECD-TIEA between Canada and Aruba includes provisions in Article 6 for spontaneous information exchange, requiring the sharing of "knowledge that may be foreseeably relevant".[274] The term 'knowledge' in this context implies that the sending State must understand the partner State's tax legislation and assess whether the information could be relevant to that jurisdiction's tax laws.

Another notable feature of Canada's international tax treaty network is its adoption of the fourth paragraph of Article 26 of the OECD-MC in some of its income tax treaties.[275] For example, the tax treaty with Argentina includes in Article 26(3), a provision stating that "the other Contracting State shall endeavour to obtain the information (…) notwithstanding the fact that the other State does not, at that time, need such information".[276] This means that Canada is required to share information even if it does not having an interest in collecting such taxes, as specified in the treaty with Argentina. This provision could present challenges for spontaneous information exchanges, as Canadian tax officials might not always be aware that they need to share information spontaneously, even when it is not in Canada's interest but is relevant to the other contracting State.

Concluding statement

It can be concluded that Canada's information exchange instruments do not in any significant way deviate from the foreseeable relevance standard outlined in Article 26 OECD-MC. Overall, Canada maintains alignment with international standards of foreseeable relevance. However, in cases of spontaneously exchanging information the wording of the Canadian OECD-TIEA's does differ from that used in relation to the OECD-MC.

1.2.2 Colombia

The applicability of domestic rules

The *Andean community*, a trade bloc of four countries – Bolivia, Colombia, Ecuador, and Peru – mandates contracting parties to exchange information necessary for resolving mutual difficulties or doubts arising from the Andean Community Directive's application. Additionally, it aims to establish administrative controls to prevent fraud and tax evasion, in line with the Convention's provisions. Colombian

274 Aruba – Canada, *Exchange of Information Agreement*, Signed: 20 October 2011.

275 OECD Commentary 2019, p. 71.

276 Argentina – Canada, *Income and Capital Tax Treaty*, Signed: 29 April 1993.

authorities interpret this directive as allowing for EOI concerning compliance with the directive and the enforcement of domestic laws on tax avoidance and fraud. However, recommendations suggest Colombia revise the EOI Article of the Andean Community Directive, to align more closely with Article 26 of the OECD-MC.

Taxpayer rights and secrecy rules

Colombia's DTC with Switzerland limits information exchange to that necessary for implementing the Convention and the respective domestic laws on fiscal fraud related to covered taxes. This limitation does not encompass all information potentially relevant to domestic law administration or enforcement, such as information on individuals or entities not involved in tax fraud. A protocol has been initiated between Colombia and Switzerland to amend this DTC accordingly. Both countries have also signed the MAAC, which facilitates the exchange of information in line with international standards once ratified by Switzerland. The study has not clarified how the State deals with data protection and confidentiality. This requires further investigation.

Instrument on the exchange of information

In the context of Colombia's international agreements on EOI, nine agreements with various countries and its OECD-TIEA with Barbados contain provisions in Article 1 that closely mirror the OECD-MC. These agreements stipulate the exchange of information deemed foreseeably relevant. During the Phase 2 OECD review process, Colombian authorities reported no instances of declining EOI requests based on foreseeable relevance, consistent with feedback from peers.

The standard of foreseeable relevance

Colombia's OECD-TIEA with the U.S. outlines that competent authorities will exchange information pertinent to tax determination, assessment, collection, as well as the enforcement of tax-related laws and regulations, including those pertaining to tax offences or violations of tax administration. This formulation is equivalently broad to the concept of foreseeable relevance.

Concluding statement

Considering the foreseeable relevance principle in EOI, Colombia's information exchange instruments vary in interpretation, with deviations observed, such as in the DTC with Switzerland and the Andean Community Directive, where limitations on information exchange could result in a narrower application of the principle.

1.2.3 Indonesia

The applicability of domestic rules

As indicated in the 2014 Peer Review Report, Indonesia's agreements with Germany, Singapore, and the United Arab Emirates (hereinafter: UAE) initially fell short of the international standard by only permitting the EOI as deemed necessary for fulfilling the agreements' provisions.

Taxpayer rights and secrecy rules

However, advancements have been made: EOI meeting the standard with Germany and Singapore is now facilitated through the MAAC. Although the MAAC offers the potential for exchanging 'foreseeably relevant' information with the UAE, its pending ratification status poses a hurdle. The study has not clarified how the State deals with data protection and confidentiality. This requires further (local) investigation.

Instrument on the exchange of information

Throughout the review period, Indonesia sought clarification on foreseeable relevance in two instances, without declining any requests. No objections were raised by peers regarding Indonesia's pursuit of clarification.

The standard of foreseeable relevance

Notably, Indonesia's recently established OECD-TIEA with The Bahamas incorporates language in line with the foreseeable relevance criterion.

Concluding statement

In light of the general indicators for interpreting the foreseeable relevance principle in the case of exchange on request, it can be concluded regarding the information exchange instruments used by Indonesia that they do not deviate from the principle as set out in Article 26 of the OECD-MC.

1.2.4 Mexico

The applicability of domestic rules

Despite the absence of explicit coverage of the foreseeable relevance principle in Mexico's internal EOI Manual, the Mexican competent authority adheres to the Manual on EOI for Tax Purposes by the *Global Forum* to apply this principle.

Taxpayer rights and secrecy rules

The 2014 peer review affirmed that Mexico's existing bilateral agreements conformed to the foreseeable relevance principle, employing terms such as 'foreseeably relevant', 'necessary', or 'relevant', which were deemed equivalent by Mexican authorities. The study has not clarified how the State deals with data protection and confidentiality. This requires further (local) investigation.

Instrument on the exchange of information

Subsequently, all new EOI instruments initiated by Mexico post-2014 adopt the language of foreseeably relevant. Notably, most of these agreements involve jurisdictions party to the MAAC, with the exception of the Philippines, which still adheres to the foreseeably relevant wording. Remarkably, Mexico has never rejected a request based on its failure to meet the foreseeable relevance principle. Throughout the review period, Mexico sent eight clarification requests, most of which were successfully addressed upon receipt of clarifications.

The standard of foreseeable relevance

During the current review period, feedback from peers corroborated Mexico's application of the foreseeable relevance concept in accordance with the established standard. All requests initiated by Mexico were found to meet this standard. In instances where clarification was required, the Mexican competent authority proactively sought clarification from peers, primarily to ascertain the identity of the individual subject to the request.

Concluding statement

In light of the general indicators for interpreting the foreseeable relevance principle in the case of exchange on request, it can be concluded regarding the information exchange instruments used by Mexico that they do not deviate from the principle as set out in Article 26 of the OECD-MC.

1.2.5 Nigeria

The applicability of domestic rules

Nigeria's tax system is regulated by laws such as the Companies Income Tax Act (hereinafter: CITA), the Personal Income Tax Act (hereinafter: PITA), and the Value Added Tax Act (hereinafter: VATA). Administered by the *Federal Inland Revenue Service* (hereinafter: FIRS) at the federal level and State revenue agencies, it encompasses corporate, personal, and value-added taxes.

Taxpayer rights and secrecy rules

Regarding practical application, Nigeria's EOI manual guides officials to assess requests for foreseeable relevance, although it lacks specific procedural details. Nigerian authorities assert that they adhere to the foreseeable relevance criterion in accordance with established standards. While no standardised template is provided for request formulation, Nigeria expects requesting jurisdictions to furnish adequate information demonstrating the foreseeable relevance of their requests. Clarifications may be sought when necessary. The study has not clarified how the State deals with data protection and confidentiality. This requires further (local) investigation.

Instrument on the exchange of information

Nigeria has established an extensive network for the EOI, facilitated through 21 bilateral agreements and its involvement in the MAAC since September 1, 2015. Additionally, Nigeria is a party to the African Tax Administration Forum agreement on Mutual Assistance in Tax Matters since September 23, 2017. Oversight of these EOI arrangements is centralised at the federal level, under the purview of the FIRS.

The standard of foreseeable relevance

The 2016 peer review assessment revealed that most of Nigeria's DTCs employed the term 'is necessary' in their language. This terminology aligns with the guidance provided in the Commentary 1998 to Article 26(1) of the OECD-MC, indicating flexibility in adopting alternative formulations of the 'is necessary' principle. As from 2005 the term 'is necessary' or 'is relevant' need to be replaced by 'foreseeably relevant'

to remain consistent with the Article's scope. In two DTCs this trend is followed by utilising the term foreseeably relevant. See Section 2.1.1.

Since the previous evaluation, Nigeria has entered three new DTCs with Singapore, Turkey, and the United Arab Emirates, all of which incorporate the term 'foreseeably relevant'. Additionally, a DTC with Qatar employs the term 'may be relevant'. Moreover, the ECOWAS Supplementary Act mandates the exchange of foreseeably relevant information among member States, including Nigeria.

Authorities in Nigeria have clarified that when terms like 'is necessary' or 'may be relevant' are employed, they interpret them to imply foreseeably relevant information exchange. This interpretation ensures consistency with international standards.

Concluding statement

Considering the general indicators for interpreting the foreseeable relevance principle in the case of exchange on request, it can be concluded regarding the information exchange instruments used by Nigeria that they do not deviate from the principle as set out in Article 26 of the OECD-MC.

1.2.6 South Africa

The applicability of domestic rules

EOI agreements signed by South Africa incorporate the term 'foreseeably relevant' in their EOI Articles. While some DTCs, such as those with Chile, Democratic Republic of Congo, Kenya, and Chinese Taipei, utilise language referring to information 'necessary' for the Convention's provisions, South Africa deems these formulations equivalent to foreseeably relevant. Consequently, no prohibitions impede EOI aligned with South Africa's domestic tax laws.

Taxpayer rights and secrecy rules

In practical application, South Africa adheres to the foreseeable relevance principle, with competent authority officials demonstrating proficiency in understanding this criterion. While no specific template is mandated for request formulation, South Africa expects requesting jurisdictions to furnish adequate information demonstrating foreseeable relevance, seeking clarification where necessary. The study has not clarified how the State deals with data protection and confidentiality. This requires further (local) investigation.

Instrument on the exchange of information

The 2013 peer review identified restrictions in the DTCs with Austria and Switzerland, prompting the need for amendments. Presently, South Africa enjoys full exchange with these jurisdictions through the MAAC, which is operational across all involved territories.

During the review period, South Africa requested clarification on three out of 154 requests. Clarifications were sought primarily to identify the subject in South Africa

and obtain unique identifiers for information holders. South Africa's EOI Standard Operating Procedures outline the process for determining compliance with foreseeable relevance criteria.

Over the review period, South Africa declined one EOI request due to inadequate foreseeable relevance. The request lacked essential details such as the period under investigation and tax type, instead focusing on vehicle chassis numbers. Given the request's focus on customs matters without tax implications, South African authorities advised the partner jurisdiction to seek information under the Customs Agreement. Peers did not raise any concerns regarding South Africa's application of the foreseeable relevance criterion.

The standard of foreseeable relevance

The 2013 assessment affirmed that South Africa's DTCs align with the OECD-MC, maintaining consistency in approach. In instances where treaties utilise 'as necessary' instead of 'foreseeably relevant', South Africa and its partners interpret these terms as synonymous with foreseeably relevant. Similarly, South Africa's OECD-TIEAs adhere to the 2002 OECD Model TIEA.

Concluding statement

In light of the general indicators for interpreting the foreseeable relevance principle in the case of exchange on request, it can be concluded regarding the information exchange instruments used by South Africa that they do not deviate from the principle as set out in Article 26 of the OECD-MC.

1.2.7 The United States of America

The applicability of domestic rules

In the U.S. the IRS is responsible for tax collection and preparing the international EOI, the competent authority for exchanging the information is the *Commissioner* of the LB&I Division. The IRS has broad authority to obtain and exchange information internationally without relying on other U.S. governmental agencies. The range of information the IRS may collect is extensive. Through its reliance on 'voluntary compliance,' the U.S. gathers data through tax return filings of its taxpayers, which are then verified using third-party filings to check the taxpayer's liability. The types of information the IRS can collect include social security numbers, marital status, names and social security numbers of dependents, and the existence of outstanding student loans. This is termed 'return information' and is broadly defined within the extensive privacy rules of the U.S. in Section 6103 of the Internal Revenue Code (hereinafter: IRC). Notably, the IRS has much broader access to return information and is not restricted by the principle of proportionality, as is the case in the EU, meaning the IRS faces fewer limitations in its efforts to enforce tax laws compared to the EU (see in this respect Oberson 2023).

The U.S. has codified the possibility of exchanging information with other countries in its national law. Under 26 U.S.C. § 6103(k)(4), tax return information can be shared

with a foreign government that has an income tax or gift and estate tax treaty, or another agreement for tax information exchange, with the U.S.. This sharing is allowed only within the scope and under the conditions specified by that treaty or agreement. Therefore, the EOI is codified in U.S. law, but it adheres to the applicable tax treaty with the country involved. Information will be supplied spontaneously by the U.S. only if the specific treaty allows for spontaneous exchange.

The IRS follows a preset approach regarding U.S.-Initiated Spontaneous EOI, as outlined in Section 4.60.1.3.1 of the IRM. According to this Section, IRS personnel send spontaneous tax-related information to foreign partners through the U.S. competent authority, the Commissioner of the LB&I Division. The authority to review and process these exchanges is delegated to the *Program Managers* of the EOI Program and Offshore Compliance Initiatives, as specified in Delegation Order 4-12. Spontaneous exchanges initiated by the U.S. typically occur when an IRS employee uncovers potential non-compliance with foreign tax laws during an examination, investigation, or other administrative procedure. From subpart (3) onwards, Section 4.60.1.3.1 of the IRM describes several examples of when information should be exchanged spontaneously and further specifies the required process for sending and following up on the spontaneous exchange. This procedure is described with unusual specificity compared to other countries, where the process for spontaneous exchange is less transparent.

Taxpayer rights and secrecy rules

The IRS, as the U.S. authority for tax collection and international information exchange, operates under extensive privacy rules. However, it has broad data collection methods to its disposal and ensures compliance and facilitates spontaneous exchanges through laws such as 26 U.S.C. § 6103(k)(4). Unlike other jurisdictions, the IRS assesses potential usefulness rather than proving foreseeable relevance, but it can deviate from this, as demonstrated in the OECD-TIEA with Argentina. The U.S. therefore seems to adopt the foreseeable relevance principle in spontaneous EOI in agreements but does not attach great weight to it during the facilitation of a U.S.-initiated spontaneous EOI.

Instrument on the exchange of information

The exchange itself is then facilitated by international conventions. The U.S. is a signatory to the 1988 MAAC. It also regularly applies Article 26 of the OECD-MC to its bilateral double taxation treaties and follows the wording of the MC. Additionally, the U.S. has entered several OECD-TIEAs. Examining the OECD-TIEA with Argentina reveals that Article 4-1-b(i) designates the Secretary of the Treasury (or his delegate) as the U.S. competent authority. According to the IRM, this authority is delegated to the LB&I Division.

The standard of foreseeable relevance

Article 7 of the same OECD-TIEA with Argentina, addresses spontaneous exchanges, but it appears to diverge from the IRM regarding foreseeable relevance. Specifically, Article 7 mandates the EOI that the competent authority deems to be foreseeably relevant, thereby the agreement reintroduces the foreseeable relevance standard. This

contrasts with the IRM rules, where the IRS does not seem to explicitly require the application of this standard. We highlight that Article 7 specifies that the competent authority *must suppose* the information *to be foreseeably relevant*. Although this represents a lower threshold than proving the information *is* foreseeably relevant, it nonetheless requires that the foreseeable relevance of the information to the receiving country be assessed by the sending State (see Section 2.3). This creates a situation in which the information-sending country must, to a certain extent, apply the domestic tax laws of the receiving country, to determine whether the information can be *supposed to be of interest* for tax assessment in that jurisdiction.

Concluding statement

Regarding the foreseeable relevance principle, it seems that the U.S. chooses not to apply the standard of foreseeable relevance as explicitly for spontaneous EOI as it does for EOIR. In EOIR, Section 4.60.1.2.1 (4)(J) of the IRM explicitly mentions foreseeable relevance as a requirement to request information from the IRS. In contrast, for spontaneous exchange, Section 4.60.1.3.1 of the IRM describes it as an exchange that "typically involves information discovered during a tax examination, (...) or that is otherwise determined to be potentially useful to a foreign partner for tax purposes". Here, the requirement is not a demonstration of foreseeable relevance, but a determination of potential usefulness to the partner for tax purposes. Thus, the IRS does *not need to prove* that the information *is useful* to the foreign tax administration but has the authority to determine that it *potentially could be*.


ACADEMIA LVGDVNO BATAVA
PRAESIDIVM LIBERTATIS

Annex 2

Legal instruments governing cooperation in criminal matters

Applicable legal instruments and respective scope

The legal instruments regulating judicial cooperation have different scopes of application with a considerable overlap. To delimit the scope of application of the different provisions, a first distinction must be made between rules on the information exchange on request and rules on spontaneous information exchange.

As far as information exchange on request is concerned, judicial cooperation in criminal matters is regulated by the 1959 CoE MLA Convention, by the 2000 EU MLA Convention and by the EIO Directive and functions, in essence, according to a request/order and execution mechanism. For the sake of clarity, the scope of application of the three instruments will be examined first.

Starting from the instrument applicable to the smallest circle of jurisdictions, the EIO Directive applies to all EU Member States except for Ireland and Denmark. Hence, the following EU Member States are bound by the EIO Directive when it comes to information exchange upon request: Belgium, Bulgaria, Czechia, Germany, Estonia, Greece, Spain, France, Croatia, Italy, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Malta, Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland and Sweden.

The 2000 EU MLA Convention is applicable to all EU Member States except for Croatia and Greece. Thus, the following EU Member States are bound by this Convention: Belgium, Bulgaria, Czechia, Denmark, Germany, Estonia, Ireland, Spain, France, Italy, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Malta, Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland, and Sweden. Furthermore, pursuant to Article 29 2000 EU MLA Convention, the Convention (including Article 7) applies also to Norway and Iceland.[277]

The 1959 MLA Convention applies to 50 States composed of Members of the Council of Europe (including but not limited to EU Member States) and Non-Member of Council of Europe. These include: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Republic of Moldova, Romania, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, Ukraine, and

277 Although these countries do not fall within the scope of the study, in some cases they are FCInet members and may therefore be of interest. While Norway is among the State Parties to the 1959 CoE Convention and to its Second additional protocol, Iceland has signed, yet not ratified the second additional protocol to the 1959 CoE Convention.

United Kingdom. Further, the 1959 CoE MLA Convention applies to Chile, Israel, Republic of Korea, and Russian Federation.

As the three lists above show, most EU Member States are covered by all three legal instruments in question. The relation between these legal instruments is set forth in Article 34 EIO Directive. According to that provision, the EIO Directive replaces for those Member States that are bound by that Directive the corresponding provisions, inter alia, of the 1959 CoE MLA Convention and of its protocols, as well as of the 2000 EU MLA Convention. Thus, for all EU Member State except for Denmark and Ireland, the EIO Directive applies when their authorities engage in judicial cooperation (including when this is for the purpose of requesting and obtaining information) with the authorities of another EU Member State to which the EIO Directive is applicable. This is coherent with the provisions set forth in Article 26(4) 1959 CoE MLA Convention.[278]

If the request for information is sent between authorities of Denmark and Ireland, respectively, or between the authorities of Denmark or Ireland, on the one hand, and the authorities of another EU Member State, on the other, it must be established whether the 2000 EU MLA Convention or the 1959 CoE MLA Convention applies. There are no doubts when in the EU Member State engaging with either Denmark or Ireland only one of the two Conventions is applicable. This would be the case of Croatia and Greece. As these two Countries have not adopted the 2000 EU MLA Convention, but they are Parities, as other EU Member States, to the 1959 CoE MLA Convention, the provisions of the latter will apply in case judicial cooperation aiming at the exchange of information upon request were to take place between Ireland or Denmark on the one hand, and Greece or Croatia, the other.

In cases in which authorities from Denmark and Ireland interact with authorities from other EU Member States, which have signed and ratified both Conventions, the solution must be found according to the relevant provisions enshrined in those Conventions. Pursuant to Article 26(1) 1959 CoE MLA Convention, the Convention supersedes the provision of any other treaty, convention or bilateral agreement governing mutual assistance in criminal matters between any two Contracting Parties. Article 26(3) 1959 CoE MLA Convention, however, allows Contracting Parties to conclude between themselves bilateral or multilateral agreements on mutual assistance in criminal matters to supplement the provisions of 1959 CoE MLA Convention or to facilitate the application of the principles contained therein. The 2000 EU MLA Convention establishes in Article 1(1) that the purpose of that Convention is to supplement the provisions and facilitate the application between the MS of the EU of, among others, the 1959 CoE MLA Convention.

278 Where, as between two or more Contracting Parties, mutual assistance in criminal matters is practised on the basis of uniform legislation or of a special system providing for the reciprocal application in their respective territories of measures of mutual assistance, these Parties shall, notwithstanding the provisions of this Convention, be free to regulate their mutual relations in this field exclusively in accordance with such legislation or system. Contracting Parties which, in accordance with this paragraph, exclude as between themselves the application of this Convention shall notify the *Secretary General* of the CoE accordingly.

As the provisions of the 2000 EU MLA Convention add to the provisions of the 1959 CoE MLA Convention, the provisions of the 2000 EU MLA Convention arguably prevail according to the *lex specialis* principle. This is confirmed also by Article 30(3) and (4) of the Vienna Convention on the law of treaties that regulates the application of successive treaties relating to the same subject matter. According to a combined reading of those two provisions, the earlier treaty (in this case, the 1959 CoE MLA Convention) applies only to the extent that these provisions are compatible with those of the later treaty (in this case, the 2000 EU MLA Convention).

Turning to the spontaneous exchange of information, the applicable provisions are enshrined in the Second additional protocol to the 1959 CoE MLA Convention and in the 2000 EU MLA Convention. As mentioned above, the provisions of the 2000 EU MLA Convention apply to 25 of the current 27 EU Member States.[279] Furthermore, pursuant to Article 29 2000 EU MLA Convention, the Convention (including Article 7) applies also to Norway and Iceland.

17 non-EU Member States have ratified the 1959 CoE MLA Convention and its Second additional protocol.[280] Except for the position of Iceland, to which Article 7 2000 EU MLA Convention – but not Article 11 Second additional protocol to the 1959 CoE MLA Convention – applies, the scope of application of the Second additional protocol also includes the jurisdiction to which the 2000 EU MLA Convention applies.

Where spontaneous exchange of information is to occur between the authorities of a State that has adopted the 2000 EU MLA Convention and the authorities of a State that has ratified the Second additional Protocol (but not the 2000 EU MLA Convention), the exchange will be regulated by Article 11 Second additional protocol to the 1959 CoE MLA Convention.

Where both the sending and the receiving authority belong to jurisdictions that have both adopted the 2000 EU MLA Convention and the Second additional protocol to the 1959 CoE MLA Convention, the applicable legal framework is identified pursuant to Article 28 Second additional protocol to the 1959 CoE MLA Convention, Article 26 1959 CoE MLA Convention and Article 1 2000 EU MLA Convention.

As mentioned above, a combined reading of these provisions establishes a prevalence of the relevant provisions of the 2000 EU MLA Convention. In addition, the Second additional protocol to the 1959 CoE MLA Convention, which was adopted in 2001, provides under Article 28 that its provisions are without prejudice to more extensive regulation in bilateral or multilateral agreements concluded between Parties according to the above-mentioned Article 26(3) 1959 CoE MLA Convention. Thus, when spontaneous exchange of information is to occur between the competent authorities of

279 Croatia has signed and ratified the 1959 CoE MLA Convention as well as its Second additional protocol. Conversely, Greece is a Party to the 1959 CoE MLA Convention, but it has not ratified the Second additional protocol.

280 Albania, Armenia, Bosnia and Herzegovina, Georgia, Liechtenstein, Montenegro, North Macedonia, Norway, Republic of Moldova, Serbia, Switzerland, Türkiye, Ukraine, United Kingdom, Chile, Israel, Russian Federation.

two States that have ratified the 1959 CoE MLA Convention and its Second additional protocol and that have adopted also the 2000 EU MLA Convention, the latter applies as the Second additional protocol to the 1959 CoE MLA Convention does not interfere with the provisions of instruments such as the 2000 EU MLA Convention.

This is in line with Article 30 of the Vienna Convention on the law of treaties that provides that when a treaty specifies that it is subject to, or that it is not to be considered as incompatible with the earlier treaty, the provision of that other treaty prevails. Moreover, the explanatory report of the 2001 Second additional protocol to the 1959 CoE MLA Convention establishes that with regard to the interpretation of its provisions that follow the EU 2000 MLA Convention one has to look at the explanatory report of the latter.[281]

As far as police cooperation between competent authorities of (any) EU Member State or Europol, on the one side, and the United Kingdom, on the other side, is concerned, the Trade and Cooperation Agreement applies. Article 563 Trade and Cooperation Agreement lays down the rules on cooperation on operational information between authorities from an EU Member State and from the United Kingdom. The Agreement establishes under Article 563(3) that information may be provided in response to a request or spontaneously, subject to the conditions of the domestic law which applies to the providing competent authority and within the scope of its powers. Hence, while authorities operating in jurisdictions of EU Member States will be bound by national law that implements the applicable EU legislation on cross-border police cooperation (from 12 December 2024: Directive (EU) 2023/977), competent authorities in the United Kingdom will conform to rules of their domestic law. Relating to the cooperation of Europol with competent authorities of the United Kingdom, Article 569 Trade and Cooperation Agreement sets out the legal coordinates for cooperation including the exchange of personal data.

281 After Brexit, as far as the United Kingdom is concerned, the Trade and Cooperation Agreement applies. Under Article 633, the Trade and Cooperation Agreement provides that it is the objective of Title VIII on mutual assistance to supplement the provisions and facilitate the application between Member States, on the one side, and the United Kingdom, on the other side, of the 1959 CoE MLA Convention and both its additional protocol (including the 2001 Second additional protocol). The provisions included in Title VIII, do not contain any rules on spontaneous information exchange. This allows for the conclusion that regarding this kind of operations the applicable provisions of the Second additional protocol to the 1959 CoE MLA Convention continue to apply.


ACADEMIA LVGDVNO BATAVA
PRAESIDIVM LIBERTATIS

Annex 3

Literature and Case Law

Literature

Allegrezza 2010

S. Allegrezza, 'Critical Remarks on the Green Paper on Obtaining Evidence in Criminal Matters from One Member State to Another and Securing Its Admissibility', *Zeitschrift für Internationale Strafrechtsdogmatik* (2010): 569-579.

Balboni & Macenaite 2013

P. Balboni and M. Macenaite, 'Privacy by design and anonymisation techniques in action: Case Study of Ma³tch technology', *Computer Law & Security Review* 29 (2013), p. 330-340.

Boei & Van Dam 2022

W. Boei and J. van Dam, 'Legal Protection in the Context of International Exchange of Information upon Request between Tax Authorities', *Erasmus Law Review*, 2, (2022):76-85, retrieved from: https://www.erasmuslawreview.nl/tijdschrift/ELR/2022/2/ELR-D-22-00033.

BZSt 2019

Bundeszentralamt für Steuern, *Merkblatt zur zwischenstaatlichen Amtshilfe durch Informationsaustausch in Steuersachen (Stand: 1. Januar 2019)*, BMF v. 29. Mai 2019 - IV B 6 - S 1320/07/10004 :008, BStBl. I 2019, 480, retrieved from: https://karriere.bzst.de/SharedDocs/Downloads/DE/intern_amtshilfe/merkblatt_zwischenstaatliche_amtshilfe.pdf?__blob=publicationFile&v=10.

Cannes 2022

F. Cannes, 'Tax Cooperation and Exchange of Information: The Issue of "Circulation of Evidences"', *Erasmus Law Review*, 2, (2022):125-135, retrieved from: https://www.boomportaal.nl/tijdschrift/ELR/ELR-D-22-00022.

CIAT 2006

CIAT, *Manual for implementing and carrying out Information exchange for tax purposes. General and legal aspects of information exchange*, CIAT Publishing (2006), retrieved from: https://www.ciat.org/Biblioteca/DocumentosTecnicos/Ingles/2006_CIAT_manual_information_exchange.pdf, p. 1-129.

CoE 2011

CoE, *Explanatory Report to the Convention on Mutual Administrative Assistance in Tax Matters as amended by the 2010 Protocol*, European Treaty Series (ETS) No. 127 (2011), retrieved from: https://rm.coe.int/16800cb345.

Daniele 2024

M. Daniele, 'Scope of Judicial Review in the Executing State in EIO Proceedings', *European Criminal Law Review* 2024(2):177-190.

Debelva 2024
F. Debelva, 'The impact of the right to privacy and nemo tenetur on tax information exchange', in: M. Serrat Romaní, J. Korving & M. Eliantonio (red.), *Exchange of Information in the EU*, Cheltenham: Edward Elgar Publishing (2024):67-84.

FCInet 2022, *User Protocol*
FCInet, *Protocol for Cooperation between FCInet participants*, The Hague (2022), Netherlands (not published).

Fort & Rust 2012
E. Fort and A. Rust, *Exchange of Information and Bank Secrecy*, Alphen aan den Rijn: Kluwer Law International (2012).

Geelhoed & Hoving 2021
W. Geelhoed and R.A. Hoving, *Enhanced Exchange of Information in Financial Investigations*, Groningen: University of Groningen (2021), retrieved from: https://pure.rug.nl/ws/portalfiles/portal/193148668/Enhanced_Exchange_of_Information_in_Financial_Investigations.pdf.

Global Forum Peer Review Canada 2017
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Canada 2017 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2017), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-canada-2017-second-round_9789264280137-en.html.

Global Forum Peer Review Colombia 2024
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Colombia 2024 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2024), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-colombia-2024-second-round_76d26379-en.html.

Global Forum Peer Review France 2018
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Peer Reviews France 2018 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2018), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-france-2018-second-round_9789264291058-en.html.

Global Forum Peer Review France 2011
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Peer Reviews France 2011: Combined Phase: 1 + Phase 2*, Paris: OECD Publishing (2011), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews-france-2011_9789264114708-en.html.

Global Forum Peer Review Indonesia 2018
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Indonesia 2018 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2018), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-indonesia-2018-second-round_9789264302754-en.html.

Global Forum Peer Review Indonesia 2014
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Peer Reviews Indonesia 2014 Phase 2: Implementation of the Standard in Practice*, Paris: OECD Publishing (2014), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews-indonesia-2014_9789264217737-en.html.

Global Forum Peer Review Italy 2017
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Italy 2017 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2017), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-italy-2017-second-round_9789264283800-en.html.

Global Forum Peer Review Mexico 2023
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Mexico 2023 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2023), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-mexico-2023-second-round_6fd9ab78-en.html.

Global Forum Peer Review Mexico 2014
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Mexico 2014 Peer Review Report Phase 2: Implementation of the Standard in Practice*, Paris: OECD Publishing (2014), retrieved from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/08/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews-mexico-2014_g1g45f14/9789264217751-en.pdf.

Global Forum Peer Review Nigeria 2023
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Nigeria 2023 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2023), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-nigeria-2023-second-round_90bade22-en.html.

Global Forum Peer Review Nigeria 2016
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Peer Reviews Nigeria 2016: Phase 2: Implementation of the Standard in Practice*, Paris: OECD Publishing (2016), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews-nigeria-2016_9789264250857-en.html.

Global Forum Peer Review South Africa 2022
Global Forum on Transparency and Exchange of Information for Tax Purposes, *South Africa 2022 (Second Round, Combined Review): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2022), retrieved from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/11/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-south-africa-2022-second-round-combined-review_56613ecb/0cb5c667-en.pdf.

Global Forum Peer Review South Africa 2013
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Peer Reviews South Africa 2013: Combined: Phase 1 + Phase 2, incorporating Phase 2 ratings*, Paris: OECD Publishing (2013), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews-south-africa-2013_9789264205901-en.html.

Global Forum Peer Review Spain 2019
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Spain 2019 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2019), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-spain-and-turks-2019-second-round_997a7b23-en.html.

Global Forum Peer Review United States 2018
Global Forum on Transparency and Exchange of Information for Tax Purposes, *United States 2018 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2018), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-united-states-2018-second-round_9789264302853-en.html.

González 2024
S.M. González, 'Transparency and foreseeable relevance in exchange of information procedures', in: M. Serrat Romaní, J. Korving & M. Eliantonio (red.), *Exchange of Information in the EU,* Cheltenham: Edward Elgar Publishing (2024):8-35, retrieved from: https://www.elgaronline.com/edcollchap/book/9781035314560/book-part-9781035314560-9.xml#:~:text=The%20purpose%20of%20this%20chapter%20is%20to%20analyse%20the%20evolution.

Huiskers-Stoop, Breuer & Nieuweboer 2022
E.A.M. Huiskers-Stoop, A.C. Breuer and M. Nieuweboer, 'Exchange of information, tax confidentiality, privacy and data protection from an EU perspective', *Erasmus Law Review,* 2, (2022):86-99, retrieved from: https://www.erasmuslawreview.nl/tijdschrift/ELR/2022/2/ELR-D-22-00030.

Huiskers-Stoop & Nieuweboer 2018
E.A.M. Huiskers-Stoop and M. Nieuweboer, 'De Mandatory Disclosure-regels in het licht van het recht op privacy en de bescherming van persoonsgegevens (authors' translation: The Mandatory Disclosure rules in light of the right to privacy and the protection of personal data), *Fiscaal tijdschrift vermogen* 2018(12):6-17.

Jeong 2013
Y. Jeong, 'Spontaneous Exchange of Information', in: O.C. Günther and N. Tüchler (red.), *Exchange of Information for Tax Purposes*, Vienna: Linde Verlag (2013):447-462, retrieved from: https://beckassets.blob.core.windows.net/product/toc/13113214/9783707324099_toc_003.pdf.

Klip 2021
A. Klip, *European Criminal Law. An Integrative Approach*, Cambridge: Intersentia 2021.

Kristofferson et al. 2014
E. Kristofferson, M. Lang, P. Pistone, J. Schuch, C. Staringer & A. Storck, *Tax Secrecy and Tax Transparency,* Berlin, Germany: Peter Lang Verlag 2014.

Kroon 2021
U. Kroon, *Smart Intelligence Beyond Borders: understanding FCInet and ma³tch technology, 'a blueprint for privacy by design'*, Thesis Master ICT in Business and the Public Sector, LIACS, Leiden University (2021), retrieved from: https://theses.liacs.nl/1773.

Kroon 2013
U. Kroon, 'Ma³tch: Privacy AND Knowledge: "Dynamic Networked Collective Intelligence"', *IEEE International Conference on Big Data* (2013):23-31.

Merkx 2022
M. Merkx, 'Exchange of Information and Administrative Cooperation between Countries in a Globalised and Digital Economy', *Erasmus Law Review*, 2, (2022):73-75, retrieved from: https://www.erasmuslawreview.nl/tijdschrift/ELR/2022/2/ELR-D-23-00001.

Mosna 2024
A. Mosna, 'Judicial Protection in EU Cross-Border Evidence-Gathering: the EIO as a Case Study', *European Criminal Law Review* 2024(2):148-176.

Mosquera Valderrama & Debelva 2017
I. Mosquera Valderrama and F. Debelva, 'Privacy and Confidentiality in Exchange of Information: Some Uncertainties, Many Issues, but Few Solutions', *Intertax* (2017) 45 (5): 362-381.

Mosquera Valderrama 2010
I.J. Mosquera Valderrama, 'EU and OECD Proposals for International Tax Cooperation: A New Road?', *Tax Notes International* (2010), Vol. 59, nr. 8, p. 609-622.

Oberson 2023
X. Oberson, *International Exchange of Information in Tax Matters: Towards Global Transparency*, Cheltenham: Edward Elgar Publishing (2023).

OECD Commentary 2024
OECD, *Update on the commentary on Article 26 of the OECD Model Tax Convention*, Paris: OECD Publishing (2024), retrieved from: https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-transparency-and-international-co-operation/update-commentary-article-26-oecd-model-tax-convention.pdf, p. 1-3.

OECD Commentary 2019
OECD, *Model Tax Convention on Income and on Capital: Full Version 2017*, Paris: OECD Publishing (2019), retrieved from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/model-tax-convention-on-income-and-on-capital-2017-full-version_g1g972ee/g2g972ee-en.pdf, on Article 26, p. 1295-1350.

OECD 2018
Global Forum on Transparency and Exchange of Information for Tax Purposes, *France 2018 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2018), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-france-2018-second-round_9789264291058-en.html, p. 86.

OECD 2017
Global Forum on Transparency and Exchange of Information for Tax Purposes, *Canada 2017 (Second Round): Peer Review Report on the Exchange of Information on Request*, Paris: OECD Publishing (2017), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-canada-2017-second-round_9789264280137-en.html, p. 67-75.

OECD Commentary 2017
OECD, *Model Tax Convention on Income and on Capital: Condensed Version 2017*, Paris: OECD Publishing (2017), retrieved from: https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2017_mtc_cond-2017-en#page30, on Article 26: p. 487-507.

OECD Commentary 2014
OECD, *Model Tax Convention on Income and on Capital: Condensed Version 15 July 2014*, Paris: OECD Publishing (2014), retrieved from: https://www.oecd.org/en/publications/model-tax-convention-on-income-and-on-capital-condensed-version-2014_mtc_cond-2014-en.html, on Article 26: p. 414-433.

OECD Commentary 2012
OECD, *Model Tax Convention on Income and on Capital: Full Version 2010 22 July 2010,* Paris: OECD Publishing (2012), retrieved from: https://www.oecd.org/en/publications/model-tax-convention-on-income-and-on-capital-2010_9789264175181-en.html#page1, on Article 26, p. 1010-1048.

OECD 2011
Global Forum on Transparency and Exchange of Information for Tax Purposes Peer Reviews, *France 2011: Combined: Phase 1 + Phase 2*, Paris: OECD Publishing (2011), retrieved from: https://www.oecd.org/en/publications/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews-france-2011_9789264114708-en.html.

OECD Commentary 2010
OECD, *Model Tax Convention on Income and on Capital: Condensed Version 22 July 2010*, Paris: OECD Publishing (2010), retrieved from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2010/08/model-tax-convention-on-income-and-on-capital-condensed-version-2010_g1g10b68/mtc_cond-2010-en.pdf, on Article 26: p. 397-410.

OECD Commentary 2005
OECD, *Model Tax Convention on Income and on Capital: Condensed Version 15 July 2005*, Paris: OECD Publishing (2005), retrieved from: https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2005_mtc_cond-2005-en#page1, on Article 26: p. 313-327.

OECD and CoE MAAC 2010
OECD and Council of Europe, *The Multilateral Convention on Mutual Administrative Assistance in Tax Matters: Amended by the 2010 Protocol*, Paris: OECD Publishing (2011), retrieved from: https://www.oecd.org/en/publications/the-multilateral-convention-on-mutual-administrative-assistance-in-tax-matters_9789264115606-en.html.

OECD Model TIEA 2002
OECD, *Agreement on Exchange of Information on Tax Matters*, Paris: OECD Publishing (2002), retrieved from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2002/05/agreement-on-exchange-of-information-in-tax-matters_g1gh2b36/9789264034853-en.pdf.

OECD 2000
OECD, *Improving Access to Bank Information for Tax Purposes*, Paris: OECD Publishing (2000), retrieved from: https://www.oecd.org/en/publications/improving-access-to-bank-information-for-tax-purposes_9789264181267-en.html.

OECD 1998 Commentary
OECD, *Model Tax Convention on Income and on Capital: Condensed Version 1998*, Paris: OECD Publishing (1998), retrieved from: https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-1998_mtc_cond-1998-en#page264, on Article 26: p. 260-266.

OECD 1998
OECD, *Harmful Tax Competition: An Emerging Global Issue*, Paris: OECD Publishing (1998), retrieved from: https://www.oecd.org/en/publications/harmful-tax-competition_9789264162945-en.html.

Panzavolta 2024
M. Panzavolta, 'Formal and Informal Circulation of Cross-Border Evidence in Europe and Possible Improvements. Toward an "Annex E" of the European Investigation Order?', *European Criminal Law Review* 2024(2):191-212.

Pels Rijcken & VKA Report 2023
Pels Rijcken & Verdonck Klooster & Associates, *De inzet van ma³tch-technologie door JenV ter uitvoering van inzage- en verwijderingsverzoeken* (*authors' translation: The use of ma³tch technology by JenV to carry out access and deletion requests*), Report 10 October 2023, retrieved from: https://realisatieibds.nl/file/download/fc3e7035-29e5-46df-b541-c8e78de65eef/20231003_rapport-ma3tch-use-case-def.pdf.

Ring 2016
D.M. Ring, 'Article 26: Exchange of information – Global Tax Treaty Commentaries', *Global Tax Treaty Commentaries IBFD* (2016).

Simonato 2011
M. Simonato, 'The "Spontaneous Exchange of Information" Between European Judicial Authorities From the Italian Perspective', *New Journal of European Criminal Law* 2011(2):220-229.

UN Model Double Taxation Convention 2021
United Nations, *Model Double Taxation Convention between Developed and Developing Countries*, New York (2021), retrieved from: https://financing.desa.un.org/sites/default/files/2023-05/UN%20Model_2021.pdf.

De Zeeuw 2021
C. de Zeeuw, *New Technologies and the Right to the protection of personal data: A study to the use of Ma³tch technology and the Principle of Proportionality in cross-border data sharing for the purpose of criminal prosecution and crime prevention*, Thesis Master International Technology Law based on a research internship at the Innovation Department of the Dutch Ministry of Justice and Security, Amsterdam: Vrije Universiteit (2021).

Case Law

- CJEU 26 April 2023, *SRB/EDPS*, Case T-557/20, ECLI:EU:T:2023:219.
- CJEU 8 December 2022, *VS v Inspektor v Inspektorata kam Visshia sadeben savet*, Case 180/21, ECLI:EU:C:2022:967.
- CJEU 25 November 2021, *État du Grand-Duché de Luxembourg*, Case 437/19, ECLI:EU:C:2021:953.
- CJEU 6 October 2020, *État luxembourgeois v. B and Others*, Cases 245/19 and 246/19, ECLI:EU:C:2020:795.
- CJEU 16 May 2017, *Berlioz*, Case 682/15, ECLI:EU:C:2017:373.
- CJEU 11 December 2014, *Ryneš*, Case 212/13, ECLI:EU:C:2014:2428.
- CJEU 13 May 2014, *Google Spain*, Case 131/12, ECLI:EU:C:2014:317.
- CJEU 8 April 2014, *Digital Rights v. Ireland*, Cases 293/12 and 594/12, ECLI:EU:C:2014:238.
- CJEU 22 October 2013, *Sabou*, Case 276/12, ECLI:EU:C:2013:678.
- CJEU 5 June 2012, *Bonda*, Case 489/10, ECLI:EU:C:2012:319.
- CJEU 9 November 2010, *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen*, Cases 92/09 and 93/09, ECLI:EU:C:2010:662.
- ECHR 12 January 2010, *Gillan and Quinton v. United Kingdom*, ECLI:CE:ECHR:2010:0112JUD000415805.
- ECHR 4 December 2008, *S. and Marper v. United Kingdom*, ECLI:CE:ECHR:2008:1204JUD003056204.
- ECHR 1 July 2008, *Liberty et al. v. United Kingdom*, ECLI:CE:ECHR:2008:0701JUD005824300.
- ECHR 29 June 2006, *Weber and Saravia v. Germany*, ECLI:CE:ECHR:2006:0629JUD005493400.
- ECHR 12 May 2000, *Khan v. United Kingdom*, ECLI:CE:ECHR:2000:0512JUD003539497.
- ECHR 16 February 2000, *Amann v. Switzerland*, ECLI:CE:ECHR:2000:0216JUD002779895.
- ECHR 2 August 1984, *Malone v. England*, ECLI:CE:ECHR:1984:0802JUD000869179.
- ECHR 8 June 1976, *Engel and others v. the Netherlands*, ECLI:CE:ECHR:1976:0608JUD000510071.
- Supreme Court (Canada) 9 January 1995, *T.G. Andison v. Minister of National Revenue*, [1995] 1 C.T.C. 203.
- Supreme Court (Canada) 29 March 1990, *R. v. McKinlay Transport Ltd.*, SCC: 20761.
- Supreme Court (France) 27 April 1987, *Menella*, 8 / 7 SSR, No. 63634
- Supreme Court (Netherlands) 24 February 2017, *ANPR*, ECLI:NL:HR:2017:286.

Credits

Graphic design: Robert van Sluis – https://www.opticnerve.nl
Image selection: Tofigh Hasen Nezhad Nisi, Esther Huiskers-Stoop, Robert van Sluis
Print: Drukmotief, Apeldoorn, The Netherlands
Photography: 3alexd/Getty Images (Cover), Jansen Yang (p. 12), Lori Ayre (p. 34), Engin Akyurt (p. 62), Umberto Ferrara (p. 76), Wesley Tingey (p. 100), Natalia Moroz (p. 120), _marqs/Getty Images/iStockphoto (p. 138), Roberto Moller (p. 158), Aravind Jay V. (p. 164), Anna Loh (pp. 7, 33, 119, 137, 157, 163, 175)


ACADEMIA LUGDUNO BATAVA
PRAESIDIVM LIBERTATIS