

Exchange of Information, Tax Confidentiality, Privacy and Data Protection from an EU Perspective

Esther Huiskers-Stoop, Almut Breuer & Mark Nieuweboer*

Abstract

The call for more transparency in the (tax) world can hardly be overstated. One of the most prominent ways to achieve tax transparency is the exchange of information between countries. Achieving a proper balance between the exchange of information, tax confidentiality and privacy is however quite a challenge. In this article, the authors investigate some of these challenges. For the purposes of this contribution, confidentiality means that the information exchanged is used and disclosed only in accordance with the legal basis on which it was exchanged, while privacy focuses on the right to respect private life and communications, as well as the protection of personal data. More specifically, the authors elaborate on the question as to what extent do the international and European data exchange obligations deserve particular attention in the light of the privacy provisions of Article 8 ECHR and Articles 7 and 8 Charter, when it comes to the use of information for non-tax purposes, the provision to other (Member) States and the exchange of information concerning legal entities.

Keywords: confidentiality, privacy, data protection, DAC, exchange of tax information.

1 Introduction

The call for more transparency in the (tax) world can hardly be overstated.¹ One of the most prominent ways to achieve tax transparency is the exchange of information between countries. Achieving a proper balance between the exchange of information, tax confidentiality and privacy is however quite a challenge.² One must be

careful, as is shown by author Dave Eggers, who, in his modern classic *The Circle*, presented a dystopian future in which one large social media company had the following three mantras: *Secrets are lies, sharing is caring, privacy is theft*.³

In this article, we will investigate some of these challenges. The relationship between privacy and confidentiality is complicated since they are intertwined, as was already pointed out by *Debelva* and *Mosquera*.⁴ For the purposes of this contribution, confidentiality means – in accordance with the OECD definition – that ‘the information exchanged is used and disclosed only in accordance with the agreement on the basis of which it is exchanged.’⁵ Privacy, in the context of the exchange of information, focuses on the right to respect private life and communications, as well as the protection of personal data.⁶

A closer look at the Dutch situation reveals how close the connection between confidentiality and privacy is. In the Netherlands, the right to confidentiality was the first of the two to be developed explicitly. At the end of the nineteenth century, a so-called tax confidentiality provision was included in Dutch tax legislation.⁷ The starting point of this provision is that everyone involved in the taxation process is obliged not to disclose the information obtained beyond what is necessary for the enforcement of the tax legislation. In this context, confidentiality meant that information provided to the tax authorities, including company data, could only be used for the taxation process and not for other purposes.⁸ The

* Esther Huiskers-Stoop is Assistant Professor of Tax Law at the Institute of Tax Law and Economics of Leiden University, the Netherlands. Almut Breuer is Assistant Professor of Tax Law at the Maastricht University and independent attorney at law in Alkmaar, the Netherlands. Mark Nieuweboer is Lecturer of Tax Law at the Institute of Tax Law and Economics of Leiden University and independent tax adviser in Rotterdam, the Netherlands. At the time of researching and writing this article, the authors were not involved in any active or pending cases concerning this subject.

1 See, for a description of the different aspects of tax transparency: F.B. Yavaşlar and J. Hey (eds.), *Tax Transparency* (2019).

2 See, for an illustration, the preliminary questions referred to the ECJ by the Belgian Constitutional Court on 15 September 2022, case no. 103/2022, ECLI:BE:GHCC:2022:ARR.103.

3 D. Eggers, *The Circle: A Novel* (2013).

4 F. Debelva and I. Mosquera Valderrama, ‘Privacy and Confidentiality in Exchange of Information Procedures: Some Uncertainties, Many Issues, but Few Solutions’, 45(5) *Intertax* 362-3 (2017).

5 OECD, *Keeping It Safe: The OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes* (2012), at 5.

6 See, for instance, Arts. 7 and 8 of the Charter of Fundamental Rights of the European Union (*Handvest van de grondrechten van de Europese Unie*).

7 The tax secrecy provision was introduced by the Wealth Tax Act 1892 (*Wet op de vermogensbelasting 1892*) and was guaranteed until the middle of the twentieth century in various material tax laws, such as the Income Tax Act 1914 (*Wet op de inkomstenbelasting 1914*). In 1959, these provisions were merged into one ‘general tax confidentiality provision’ in Art. 67 of the General Taxes Act 1959 (GTA) (*Algemene wet inzake rijksbelastingen 1959*).

8 Parliamentary documents (*Kamerstukken*) II 2005/06, 30322, nr. 3, para. 3.5 (translated): ‘In addition to the general interest in the protection of personal data, it is important that individuals should not be prevented from providing data to the tax authorities by the fear that those data will be

confidentiality provision has the purpose to meet the resistance of Dutch taxpayers to provide transparency to the tax authorities about the size of their taxable assets. Tax confidentiality was important to achieve the goal of proper taxation which would be at risk if taxpayers withheld tax information for fear of disclosure to third parties.⁹ Especially in the case of sensitive company data, confidentiality is important.¹⁰ The legal confidentiality provision was therefore not only intended to promote the willingness of taxpayers to co-operate but also to protect their privacy.¹¹

As the result of several national and international social and technological developments in the twentieth and early twenty-first centuries, privacy and confidentiality have come under increasing pressure as the retrieval and use of tax data by (tax) authorities surged. As a result of this growing use (and, in certain cases, abuse) of information by the (tax) authorities, from the second half of the twentieth century, the international recognition of the rights to privacy and the protection of personal data grew. This began with the 1948 adoption of Article 23 in the Universal Declaration of Human Rights.¹² This adoption formed the basis for Article 8 of the European Convention on Human Rights (ECHR), introduced shortly afterwards in 1950 and the subsequent introduction of Article 17 of the International Covenant on Civil and Political Rights in 1979. At the European level, the recognition of the right to privacy and the protection of personal data has been accelerated by the introduction in 2009 of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (Charter)¹³ and the further elaboration of Article 8 Charter in the General Data Protection Regulation (GDPR) in 2018.¹⁴ These international privacy provisions seem to have partially taken over the role of the privacy objective in domestic confidentiality provisions.¹⁵ Generally, in-

fringements of those provisions are only permitted based on a legal provision which is 'sufficiently clear' and 'accessible to the person concerned'.¹⁶ Laws on the exchange of information in tax matters must adhere to that standard. Furthermore, as a result of technological developments in the past decades, the international and European exchange of tax information has increased significantly, as is shown in the next section.

Just how challenging the balancing of transparency and confidentiality/privacy is, can again be shown by using the Dutch rules as an example. While the Dutch tax inspector is subject to a duty of confidentiality regarding information obtained during the taxation process, the Dutch tax authorities as an institute are obliged to disclose certain data to other European tax authorities.¹⁷ Although the domestic obligation of confidentiality applies *mutatis mutandis* to information provided to other tax authorities in the context of mutual assistance,¹⁸ it may be set aside by a legal provision. 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 the Directive 2011/16/EU (DAC) and some of the international agreements on the exchange of information also allow the information to be used for non-tax purposes or even to be disclosed to third parties.¹⁹ In doing so, the domestic (legal) interpretation of the principle of confidentiality of the data obtained is often left to the (Member) States.²⁰ However, taxpayers whose tax information is exchanged should be able to rely on the fact that non-tax use or further exchange to other (Member) 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 rule of no further disclosure than is necessary for the enforcement of taxation.²¹

used for purposes other than for the correct and efficient enforcement of the tax law.'

- 9 See B. van der Sar, 'Fiscale geheimhoudingsplicht: art. 67 AWR ontrafeld (Fiscal confidentiality in the Netherlands: Article 67 AWR unravelled)' (diss. Leiden, Leiden University 2021), at 97, 169 and 173.
- 10 See B.M.J. van der Meulen, J. Nouwt, J.E.J. Prins, W.J.M. Voermans, and A.P. de Wit, *Vertrouwelijk gegeven: juridische beschouwingen over de verstrekking van bedrijfsgegevens aan de overheid en het beheer daarvan door de overheid* 26 (1999), <https://hdl.handle.net/1887/3679> (last visited 20 January 2023).
- 11 Van der Sar, above n. 9, at 66-68, 144 and 183.
- 12 This declaration describes human rights adopted by the United Nations General Assembly on 10 December 1948. The declaration is the first international confirmation of the 'universality' of human rights.
- 13 *PbEU* 2012, C 326/391.
- 14 General Data Protection Regulation, Regulation (EU) 2016/679 of 25 May 2018 replacing the European Privacy Directive (95/46/EC). With the GDPR, differences in privacy provisions in the European countries have been largely equalised.
- 15 For the application of the privacy provisions, personal data must be protected as part of private life within the meaning of Art. 7 Charter or Art. 8 ECHR. See 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', 2018(12) *Civiel & fiscaal tijdschrift vermogen* (2018), p. 12 with reference to *Amann v. Switzerland*, 16 February 2000, ECLI:CE:ECHR:2000:0216. Privacy may also relate to business matters, see *Halford v. United Kingdom*, 25 June 1997, ECLI:CE:ECHR:1997:0625 and *Niemietz v. Germany*, 16 December 1992, ECLI:CE:ECHR:1992:1216. Whether

1.1 Research Question and Method

The privacy objective of the Dutch tax confidentiality provision has traditionally focused both on the restriction in the use of tax data and on its transfer to third parties, as have European and international privacy and confidentiality provisions (see Section 3). These provisions have come under increasing pressure in recent

er privacy is at stake must be assessed on the basis of the circumstances, see *S. and Marper v. United Kingdom*, 4 December 2008, ECLI:CE:ECHR:2008:1204.

- 16 See *Malone v. England*, 2 August 1984, ECLI:CE:ECHR:1984:0802: 'sufficiently clear' and *Sorvisto v. Finland*, 13 January 2009, ECLI:CE:ECHR:2009:0113: 'accessible to the person concerned'. See Van der Sar, above n. 9, at 68 with reference to *Kruslin v. France* and *Huvig v. France*, 24 April 1990, ECLI:NL:XX:1990:AD5851, *NJ* 1991/523.
- 17 Art. 67 GTA refers to 'everyone', while the obligation to exchange international information refers to the 'competent authority', which in practice is a designated person or body, like the Dutch tax authorities (Arts. 5 to 7 and 2(1)(f) WIB).
- 18 Art. 16 WIB with respect to information provided to a competent authority and Art. 28 WIB with respect to data obtained from a competent authority.
- 19 Art. 16(2) and (3) DAC.
- 20 Art. 16(1) DAC.
- 21 Van der Sar, above n. 9, at 276.

decades due to the proliferation of international exchange of tax information. However, it remains important for taxpayers to be able to exercise control over the information provided by them to national tax authorities. This control may be at stake if the exchanged information is used for non-tax purposes or is forwarded to other (Member) States. In addition, the privacy provisions traditionally aimed at protecting the ‘individual’ raise questions when it comes to the protection of taxpayers with ‘legal personality’.²² This contribution studies:

To what extent should the international and European data exchange obligations deserve particular attention in the light of the privacy provisions of Article 8 ECHR and Articles 7 and 8 Charter when it comes to the use of information for non-tax purposes, to forwarding to other (Member) States and the exchange of information concerning legal entities?

The contribution deals with the following questions: how is the international and European exchange of information for the Dutch tax authorities legally structured, more specifically under the application of the DAC (Section 2), how are the international fundamental rights of privacy and the protection of taxpayers’ personal data legally structured (Section 3), and to what extent should the obligation to exchange international information deserve particular attention when it comes to the use of information for non-tax purposes, the provision to other (Member) States, and the exchange of information concerning legal entities (Section 4).

The right to privacy has limits in the light of what may be requested by, for example, the tax inspector in the context of taxation, and what must be given by taxpayers in this context. The right to privacy also has limits in the purposes for which, once provided, data may be used. However, if – as with the exchange obligations based on the DAC – there is a systematic collection and processing of personal data, then interference with private life is assumed.²³ In view of the judgment of the Court of Justice of the European Union (ECJ) of 8 April 2014, a regulation allowing authorities to access the content of electronic communications held for a certain period of time constitutes an infringement of the essence of the fundamental right to respect for private life.²⁴ Thus, even if the collection of personal data in itself does not infringe on privacy, this can still be the case if that data is *systematically* collected and stored. In this contribution, we basically restrict ourselves to the automatic exchange of information. However, in the light of the bilateral and multilateral (Model) Agree-

ments on Exchange of Information, we also pay attention to the provision of information on request. We will not specifically discuss the exchange of information on value added tax and customs duties as laid down in Council Regulation (EU) No. 904/2010 and Regulation (EU) No 952/2013 of the European Parliament and of the Council.

The main focus of this research is on the international and European information exchange obligations of tax authorities in light of the international fundamental rights of privacy and the protection of personal data of taxpayers. In addition, the research contributes to the academic discussion about the scope of privacy provisions when it comes to legal entities. In order to answer the research question, we mainly use the ECHR, the Charter, the DAC, the OECD Model Tax Convention (OECD MC), the Model Agreement on Exchange of Information on Tax Matters (TIEA), the Convention on mutual administrative assistance in tax matters (MAC), the commentaries on it, as well as the case law of the ECJ and the European Court of Human Rights and relevant academic articles.

2 International and European Exchange of Information

As we focus on privacy issues from an international and European perspective, the first part of this section is limited to a brief introduction of the overarching international legal sources of the exchange of information and the privacy rules they contain. For a more detailed introduction to the international exchange of information, we refer to the existing literature.²⁵ In the second part of this section, we will introduce the DAC in more detail.

2.1 International Exchange of Information

The international exchange of information in tax matters has a long-standing tradition. Already in 1927 the League of Nations had issued a ‘Draft of a Bilateral Convention on Administrative Assistance in Matters of Taxation’.²⁶ Article 1 of this draft mentions the core features of the international exchange of information that are valid until today:

With a view to obtaining a better apportionment of fiscal burdens in the interest both of Governments and taxpayers, the Contracting States undertake,

22 For example, platform operators holding legal personality under DAC7.

23 See *Perry v. United Kingdom*, 17 July 2003, ECLI:CE:ECHR:2003:0717, at 40 and *P.G. and J.H. v. United Kingdom*, 25 September 2001, ECLI:CE:ECHR:2001:0925, at 57. See for Dutch case law Supreme Court 24 February 2017, ECLI:NL:HR:2017:286, 287 and 288 (ANPR), at 2.3.3 and Dutch Supreme Court 28 January 1998, BNB 1998/147 from which it can be concluded that the criterion of whether there is systematic data collection does not apply exclusively to the recording of observations in public spaces.

24 Case 293/12, *Digital Rights v. Ireland*, ECLI:EU:C:2014:238, at 34 and 39.

25 See X. Oberson, *International Exchange of Information in Tax Matter: Towards Global Transparency, Second Edition* (2018); and from a Dutch perspective: R.E.C.M. Niessen, ‘Internationale uitwisseling van fiscale gegevens en andere bijstandsvormen’, 2016(2) *Tijdschrift formeel belastingrecht* (2016) and J.A. Booij, *Internationale fiscale gegevensuitwisseling* (2018).

26 League of Nations: Committee of Technical Experts on Double Taxation and Tax Evasion. *Double Taxation and Tax Evasion: Report – Document C. 216. M. 85* (London, 12 April 1927), Part III. – Legislative History of United States Tax Conventions. 1927, <http://adc.library.usyd.edu.au/view?docId=split/law/xml-main-texts/brulegi-source-bibl-3.xml> (last visited 21 January 2023).

subject to reciprocity, to give each other administrative assistance in regard to all matters required for the purpose of tax assessment.²⁷

Article 4 provides that ‘the State to which application is made may refuse to carry out such application if it considers that it is contrary to public policy.’ In other words, almost a century ago, tax authorities had already realised the necessity to cooperate in tax matters in order to secure the correct application of the tax laws.²⁸ Also, the principles of reciprocity and the necessity to adhere to the public policy were already introduced, the latter being the angle for applying privacy and data protection laws.

What started out in 1927 has since developed into an extensive network of bi- and multilateral agreements. Both the OECD and the United Nations (UN) took over the work of the League of Nations. The OECD introduced Article 26 of OECD Model Tax Convention (OECD MC) as well as an extensive Commentary (OECD Comm.),²⁹ which since 2005 also refers to data protection.³⁰ The UN issued Article 26 of the UN Model Tax Convention (UN MC).³¹ Another bilateral instrument is the so-called Model Agreement on Exchange of Information on Tax Matters (TIEA),³² which was published by the OECD for situations in which the respective states have not concluded a comprehensive double tax convention but want to assist each other with the exchange of information. Like the OECD MC, the TIEA contains an extensive Commentary. The TIEA also provides for a confidentiality clause (Art. 8) and protects certain secrets (Art. 7).

On a multilateral level, there is the MAC which was concluded in 1988 and amended in 2010³³ and contains two articles relevant for privacy: Article 21 (protection of persons and limits to the obligation to provide assistance) and Article 22 (secrecy). Based on the MAC, a Multilateral Competent Authority Agreement (MCAA) on Automatic Exchange of Financial Account Information was introduced in 2014³⁴ and signed by 92 OECD

and non-OECD nations as of 31 January 2022.³⁵ It contains an article on confidentiality and data safeguards (see Section 5 MCAA).

The OECD prominently addressed the exchange of information on several occasions, which we will list below. Firstly, the OECD launched the Global Forum on Transparency and Exchange of Information for Tax Purposes in 2009, which resulted in an extensive number of peer reviews in which the practices of the participating countries were addressed.³⁶ A few years later, the OECD stressed the importance of the matter in the BEPS project.³⁷ Action 5 of the BEPS Action Plan tackles transparency issues and recommends the exchange of information on tax rulings as a minimum standard and an element of its transparency framework.³⁸ The OECD kept monitoring the introduction of those rules by way of a peer review system. While one of the topics to be peer-reviewed is confidentiality,³⁹ the peer review reports thus far have not addressed the issue.⁴⁰ Furthermore, in Action 12, the OECD advised on the Mandatory Disclosure Rules regarding the exchange of information on aggressive tax planning strategies.⁴¹ Action 13, lastly, contains the Country-by-Country Reporting (CbCR), which provides for the exchange of information on the global allocation of the income, taxes and other indicators of the location of economic activity of large multinational enterprise groups (MNE Groups).⁴² As with Action 5, the OECD published a peer review report in 2021, which, *inter alia*, deals with confidentiality issues.⁴³

The Member States of the European Union have decided to jointly introduce the earlier mentioned OECD-BEPS initiatives as well as the exchange of information on Financial Account Information by way of amending the DAC, which is explained in more detail in the following section.

2.2 EU Directive on Administrative Cooperation

On 10 February 1975, the European Council adopted a resolution on the measures to be taken by the Commu-

27 See <https://ad.library.usyd.edu.au/view?docId=split/law/xml-main-texts/brulegi-source-bibl-3.xml;chunk.id=d2401e1834;toc.depth=1;toc.id=d2401e1834;database=;collection=;brand=default> (last visited 21 January 2023).

28 For a historic overview, see M.B. Knittel, ‘Articles 25, 26 and 27. Administrative Cooperation’, in T. Ecker and G. Ressler (eds.), *History of Tax Treaties*, Series in International Tax Law, Volume 69 (2011).

29 Most recent version: OECD, *Model Tax Convention on Income and on Capital* (2017).

30 See OECD Commentary 2017, at Art. 26, para. 10.

31 Most recent version: *United Nations Model Double Tax Convention between Developed and Developing Countries* (2017).

32 OECD, *Agreement on Exchange of Information in Tax Matters* (2002) and Model Protocol for the Purpose of Allowing the Automatic and Spontaneous Exchange of Information under a TIEA (2015).

33 OECD and Council of Europe, *The Multilateral Convention on Mutual Administrative Assistance in Tax Matters: Amended by the 2010 Protocol* (2011).

34 OECD, *Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information*, www.oecd.org/ctp/exchange-of-tax-information/multilateral-competent-authority-agreement.pdf (last visited 20 January 2023).

35 See www.oecd.org/tax/beps/CbC-MCAA-Signatories.pdf (last visited 20 January 2023).

36 See www.oecd.org/tax/transparency (last visited 20 January 2023). For an in-depth analysis, see Leo E.C. Neve, ‘The Peer Review Process of the Global Forum on Transparency and Exchange of Information for Tax Purposes. A Critical Assessment on Authority and Legitimacy’, 2017(2) *Erasmus Law Review* (2017).

37 OECD, *Action Plan on Base Erosion and Profit Shifting* (2013).

38 For a deeper analysis of the exchange of tax rulings under BEPS Action 5 see A. Breuer, K. Boer and S. Douma, ‘Uitwisseling van tax rulings’, 2016(50) *Weekblad Fiscaal Recht* (2016).

39 OECD, *BEPS Action 5 on Harmful Tax Practices – Transparency Framework: Peer Review Documents* (2021), at 11.

40 For the last report see OECD, *Harmful Tax Practices – 2020 Peer Review Reports on the Exchange of Information on Tax Rulings* (2021). The same is true for earlier reports, which can be found at www.oecd.org/tax/beps/beps-actions/action5/ (last visited 20 January 2023).

41 OECD, *OECD/G20 Base Erosion and Profit Shifting Project – Mandatory Disclosure Rules, Action 12 – 2015 Final Report* (2015).

42 OECD, *OECD/G20 Base Erosion and Profit Shifting Project – Transfer Pricing Documentation and Country-by-Country Reporting – Action 13 – 2015 Final Report* (2015).

43 OECD, *Country-by-Country Reporting – Compilation of 2021 Peer Review Reports* (2021).

nity in order to combat international tax evasion and tax avoidance. Measures should include the exchange between Member States 'of all information that appears to be of use' for making correct assessments for taxes on income and profits. Three years later, the Council adopted Directive 77/799/EEC concerning mutual assistance by competent authorities of the Member States in the field of direct taxation. The objective was to strengthen the collaboration between tax administrations of Member States through the exchange of information on request and without request. From the outset, the Directive stressed the care that must be taken to ensure 'that information provided in the course of such collaboration is not disclosed to unauthorised persons so that the basic rights of citizens and enterprises are safeguarded.'⁴⁴ When compared to the current DAC, the scope of the 1977 Directive is limited; it only governs (i) the exchange on request, (ii) automatic exchange in very specific situations and (iii) spontaneous exchange of information in a delineated list of circumstances.

In respect of confidentiality, the 1977 Directive clearly states that the information shared under the Directive shall be kept secret and shall in no circumstances be used for other than taxation purposes. Moreover, forwarding information to third Member States is only allowed with the consent of the originating Member State. The 1977 Directive contains no provision for forwarding to non-Member States.

In the first decade of this century, the Commission realised that Directive 77/799/EEC was no longer able to meet the current requirements of administrative cooperation. The new Directive 2011/16/EU of 15 February 2011 repealed and replaced the 1977 Directive. As mentioned in Section 1, over the years, the DAC has been amended and expanded half a dozen times, and each time, the scope of the mandatory automatic exchange of information has expanded:

- DAC2 (2014) implements the global Standard for Automatic Exchange of Financial Account Information in Tax Matters (also known as the Common Reporting Standard, CRS);
- DAC3 (2015) adds information concerning advance tax rulings (ATR) and advance pricing agreements (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 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 automati-

cally share this information with *all* Member States;⁴⁵

- DAC7 (2023) aims to provide tax administrations with comprehensive information about activities on online platforms.

DAC8 is in the making and will impose reporting obligations on crypto asset service providers and automatically share the information with other Member States.

3 The Right to Privacy and Data Protection

The rights to privacy and data protection are fundamental rights which seek to guarantee everyone's right to respect them. However, fundamental rights are not absolute rights and must therefore be weighed against the fundamental rights of others, for example, the right of a state to tax its subjects.⁴⁶ Because states have broad powers of taxation, conflict with these rights does not easily occur in the context of taxation.⁴⁷ The following section discusses the international fundamental rights of privacy and the protection of personal data.

3.1 Fundamental Rights in International Human Rights Treaties

In the context of taxation, the fundamental rights of privacy and the protection of personal data require that data provided by taxpayers be protected and that they are aware of how, why and by whom their data is used.⁴⁸ If the importance of providing data in the context of taxation does not outweigh the interests of respect for privacy and the protection of personal data, a taxpayer may refuse to hand over data unless a legal provision requires this. Such a provision concerns, for example, the national implementation of the provisions from the DAC.

The rights to privacy and the protection of personal data have been expressed in various international human rights treaties, as discussed in Section 1. On the basis of Article 8 ECHR, everyone has the right of 'respect for his private and family life' and, under Articles 7 and 8 Charter, everyone has the right to 'respect for his private and family life, home and communications' and to 'protection of personal data concerning him'.⁴⁹ Article 7 Charter is the equivalent of Article 8 ECHR, while Article 8 Charter does not have a separate equivalent in the

44 Recitals, Directive 77/799/EEC.

45 See E.A.M. Huiskers-Stoop, M. Nieuweboer and A.C. Breuer, 'De Mandatory Disclosure Richtlijn: beschrijving en kritische analyse', 167(1) *Tijdschrift Fiscaal Ondernemingsrecht* 29-60 (2020).

46 Art. 104 Dutch Constitution, Art. 52(1) Charter and Consideration 153 GDPR.

47 Huiskers-Stoop and Nieuweboer, above n. 15, at 8.

48 See the contribution of F. Cannas on *Tax Cooperation and Exchange of Information: The Issue of 'circulation of evidences'* to this Erasmus Law Review Special.

49 Case 131/12, *Google Spain*, ECLI:EU:C:2014:317, at 69.

ECHR.⁵⁰ Because the scope of the Charter is limited to cases where EU law is expressed, in tax matters with a purely domestic component, an appeal can be made to Article 8 ECHR.⁵¹ For the mutual relationship between Article 7 Charter and Article 8 ECHR, Article 52(3) Charter stipulates that:

In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

The rights of the Charter therefore offer the same protection as the ECHR, but on the basis of Article 52(3) Charter this protection may also be more.⁵² The explanation of Article 7 Charter is therefore also based on the case law on Article 8 ECHR, while Article 8 Charter has an independent meaning.

In principle, the drafters of the ECHR intended to provide protection only to ‘individuals’; after all, it is about the protection of ‘human’ rights. However, this classic idea of privacy was nuanced around the turn of the century, because some fundamental rights, such as Article 8 ECHR, by their nature may also be relied on by legal entities.⁵³ Also the drafters of the GDPR – which gives a further elaboration of the right to data protection of Article 8 Charter – appear to have intended only to protect the rights of natural persons.⁵⁴ Nevertheless, we believe that the rights to privacy and the protection of personal data, under certain circumstances, should also be invoked by legal entities. On the privacy protection of legal entities, we come back in Section 4.3.

The GDPR regulates the Community legal framework for the protection of personal data – such as the right of access, rectification, erasure and objection – as well as the obligations for data controllers and data processors.⁵⁵ However, for the purposes of the GDPR, the processing of personal data must fall within the scope of EU

law. Article 8 Charter stipulates that everyone has the right to the protection of their personal data and imposes requirements on the way in which such data are processed. According to the GDPR, the controller is obliged to take reasonable measures to ensure that the personal data is processed correctly.⁵⁶ As soon as data has been received by the tax authorities, the tax authorities must fulfil their responsibility to process it correctly. The tax authorities must also take appropriate technical and organisational measures to guarantee the security of the personal data.⁵⁷

The main rule is that personal data may only be collected and processed in accordance with the law in a proper and careful manner.⁵⁸ They may only be processed insofar as they are adequate, relevant and not excessive.⁵⁹ Furthermore, data should not be kept longer than necessary to achieve the purposes for which they are processed, they should be secured and confidentiality should be guaranteed.⁶⁰ Finally, persons should have the right to rectify, erase or block (inaccurate or incomplete) data.

Yet, also under the GDPR, rights of taxpayers may be limited in the economic or financial interest of the Union or a Member State.⁶¹ These limitations relate in particular to: the right of access, the right to rectification and erasure, the right to restriction of processing and the right to notification of a breach (data leaks).⁶² Such restrictions are allowed, under the condition that they are provided for by law, respect the essence of fundamental rights and freedoms, be proportionate and contribute effectively to the objectives of general interest (necessary).⁶³

Legal breaches of the fundamental rights of privacy and the protection of personal data must therefore be justified and be understandable to the taxpayer. In addition to a legal basis, a breach 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.⁶⁴

The question of whether an infringement is necessary plays an important role in this. In order to assess this, it is also important to determine whether an infringement is proportionate and whether the data can also be obtained in another, less onerous way.

50 Art. 7(3) Charter and Commentaries on Art. 7 Charter. Art. 8 Charter is based on Art. 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 Art. 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. See Commentaries on Art. 8 Charter, OJEU, 14 December 2007, C 303/17.

51 Art. 51 Charter, Art. 2(2) 2 GDPR, Case 617/10, *Aklagaren v. Hans Akerberg Fransson* ECLI:EU:C:2013:105 and Case 620/19, *Land Nordrhein-Westfalen v. J&S Service*, ECLI:EU:C:2020:1011.

52 Art. 52(3) Charter aims to ensure the necessary consistency between the Charter and the ECHR, ‘without affecting the autonomy of Union law or of the Court of Justice of the European Union’, Case 601/15, *J.N. v. State Secretary for Security and Justice*, ECLI:EU:C:2016:84, at 47.

53 See *Sté Colas EST v. France*, 16 April 2002, ECLI:NL:XX:2002:AE4682, *NJ* 2003/452.

54 Art. 1 GDPR.

55 ‘Processing’ can be understood as any automated operation with regard to personal data and includes, among others, the ‘collection, consultation, use, transmission and exchange of data’, Art. 4(2) GDPR.

56 Art. 4(7) and Art. 5(1)d GDPR.

57 Art. 5(1)(f) GDPR. In the Netherlands, the Dutch Data Protection Authority (AP) is the supervisory authority for the protection of personal data (Art. 8(3) Charter).

58 Art. 6 GDPR.

59 Case 131/12, *Google Spain*, ECLI:EU:C:2014:317, at 72.

60 Art. 5(1)(e) GDPR.

61 Art. 23(1) GDPR.

62 Arts. 15-19 GDPR.

63 Art. 23(1) GDPR and Art. 52 Charter.

64 Art. 8(2) ECHR.

3.2 Privacy Rules in (Model) Agreements on Exchange of Information

As mentioned in Section 2.1, the international (model) agreements on the exchange of information contain rules on which the protection of privacy and confidentiality can be based. In this section, we discuss confidentiality requirements, privacy and data protection and the notion of foreseeable relevance.

3.2.1 Confidentiality Requirements

First, exchange of information requires trust between the governments exchanging information. Governments also need the trust of the citizens. As such, governments are in a delicate situation, compelled to carefully balance the needs of other governments and those of their citizens. One of the elements to achieve this goal are confidentiality requirements: the government can exchange information, but the exchanged information needs to be treated as confidential by the receiving government. In Article 26 OECD MC, this rule has been laid down in the first part of the second paragraph:

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 referred to in the first sentence. 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.

The OECD Commentary adds that the state from which the information is requested can suspend assistance under Article 26, if the receiving state does not comply with the confidentiality requirements.⁶⁵ Article 22, para. 2 MAC uses almost the same wording as Article 26 OECD MC, as does Article 8 Model TIEA. The TIEA also provides for extensive guidance on confidentiality in its Commentary.

3.2.2 Privacy and Data Protection

Under Article 26(3)(c) OECD MC, states may refrain from providing information which would disclose any trade, business, industrial, commercial or professional secret of trade process, or information, the disclosure of which would be contrary to public policy (*ordre public*). However, a state may not refrain from the exchange of information because it is held by a bank, other financial institution, nominee or person acting in an agency or fiduciary capacity or because it relates to an ownership interest in a person (Art. 26(5) OECD MC). In other words, national laws on bank secrets and the like may not stop a state from providing information. Furthermore, para. 10 of the Commentary 2017 on Article 26 OECD MC recognises that states may have data

65 See OECD Commentary 2017, at. Art. 26, para. 11.

protection laws and the right to privacy and recommends those countries to include provisions that safeguard those rights. Thus, the OECD MC does not, in itself, provide for data protection and privacy requirements, which raises the question what happens if a state (especially a Member State of the European Union) does not have a data protection and privacy safeguard clause in its bilateral tax treaty. In our opinion, adhering to the GDPR by an EU Member State should not be regarded as an unlawful treaty override, but should be covered by Article 26(3)(c) OECD MC as a matter of *ordre public*. Under the MAC, the same protections as under Article 26 OECD MC apply. Article 21(2)(d) MAC is comparable to Article 26(3)(c) OECD MC, and Article 21(4) is comparable to Article 26(5) OECD MC. As regards data protection however, Article 22(1) MAC contains a specific provision that reads:

Any information obtained by a Party under this Convention shall be treated as secret and protected ... to the extent needed to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the supplying Party as required under its domestic law.

Thus, the MAC contains a safeguard regarding data protection and privacy.

Articles 7(2) and 7(4) TIEA are comparable to Articles 26(3)(c) and (5) OECD MC. The TIEA does not contain any safeguard for data protection and privacy but it does provide for a separate clause on client-attorney privilege in Article 7(3) TIEA. According to that clause, if information falls under client-attorney privilege of one state, that state does not have to exchange the respective information.

Interestingly, all provisions that have been mentioned in this section (apart from Art. 22(1) MAC on data provision) are phrased not in a prohibitive way ('shall not'), but in a voluntary way ('may refrain from'). States are therefore not prohibited from exchanging information that falls under a privacy rule, but they rather have a choice. Thus, it is for the national states to lay down legislation that safeguards the earlier mentioned rights to privacy. In the Netherlands, for example, the law reflects this voluntary character of privacy protection in Article 14(2) of the Dutch Law on International Assistance in the levying of Taxes, which uses the words 'does not need to provide information if...'⁶⁶

3.2.3 The Notion of 'Foreseeable Relevance'

The notion of foreseeable relevance is defined in para. 5 of the OECD Commentary on Article 26. According to that provision, states are – at least regarding the exchange of information on request⁶⁷ – not at liberty 'to engage in fishing expeditions', nor to request informa-

66 In Dutch: 'behoeft geen inlichtingen te verstrekken indien...'

67 There are three forms of exchange of information: on request, spontaneously and automatically. See for further reference para. 9 of the OECD Commentary on Art. 26 and the article of Niessen mentioned in above. 25.

tion that is unlikely to be relevant to the tax affairs of a given taxpayer:

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 standard requires from the requesting state sufficient information to identify the relevant taxpayer or a specific group of taxpayers.⁶⁸ The meaning of foreseeable relevance is virtually the same under the OECD MC, the TIEA (Art. 1) and the MAC (Art. 4).

When it comes to privacy and data protection, the prevention of fishing expeditions is vital. A ‘fishing expedition’ is a random or speculative request that has no apparent nexus to an open inquiry or investigation.⁶⁹ From an EU standpoint, one could even argue that only the exchange of information that is foreseeably relevant would, under the European data protection rules, be regarded as based on a legal provision and would therefore only then be allowed. The interesting question remains however whether the standard of foreseeable relevance as laid down in the OECD Commentary is too broad. According to the OECD Commentary, it is not necessary to provide names and addresses of the relevant taxpayers, but contextual information sufficient to identify that taxpayer is enough.⁷⁰ But what of the situations where the information provided by the requesting state points at a group of taxpayers, only one of which is of relevance to the requesting state? In our view, in such cases there should be no exchange of personal data by the requested state, because it cannot be ruled out that the privacy of uninvolved third parties is violated.

3.3 Privacy Rules in DAC

3.3.1 Privacy and Data Protection

The automatic exchange of information between Member States is provided by electronic means through a secure platform based on the Common Communication Network (CCN) and specifically developed for all transmissions by electronic means between competent authorities in the area of customs and taxation.⁷¹ The CCN has been operational since 1999 and interfaces between dozens of IT systems of and between EU and EEA 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. With respect to information that is exchanged with *all* Member States (i.e., DAC3 and DAC6; see the following text), the Commission develops and operates a central directory which records the infor-

mation collected and shared.⁷² The competent authorities of all Member States have access to the information in that directory.

In respect of data protection, Article 25 DAC confirms that all exchange of information pursuant to the DAC shall be subject to the provisions of the GDPR, with important exceptions. In order to safeguard the interests of monitoring, inspection or regulatory function connected with the exercise of official authority in cases of important economic or financial interest of a Member State, including taxation matters, Member States shall restrict many rights of a natural person. Most importantly, the right to be automatically or on request to be informed about what information is to be obtained or disclosed, the purpose of such processing and disclosure and his or her right to rectify, erase or block processing or disclosure of the information.⁷³

3.3.2 Relations with Third Countries

Article 24 DAC allows, under circumstances, the exchange of information from and to third countries:

- Information obtained by a Member State *from* a third country, that is foreseeably relevant for the Member State, may, on request from another Member State, be forwarded to that other Member State, provided that the agreement with the third country allows this. Moreover, such information may be transmitted spontaneously to another Member State if the information might be useful for that Member State;
- Information obtained by a Member State from another Member State may be shared with a third country, under the condition that the originating Member State has consented to that communication and the third country has committed to combatting tax evasion.

3.3.3 Foreseeable Relevance

The DAC applies to information that is *foreseeably relevant* to the administration and enforcement of the domestic tax laws of the Member States (Art. 1(1) DAC). Recital 9 defines the standard of ‘foreseeable relevance’ as the intention

to provide for exchange of information in tax matters to the widest possible extent and, at the same time, to clarify that Member States are not at liberty to engage in ‘fishing expeditions’ or to request information that is unlikely to be relevant to the tax affairs of a given taxpayer.

The new Article 5a DAC, introduced in DAC7 (2023), more precisely defines foreseeable relevant information requests:

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 request-

68 OECD Commentary, above n. 30, paras. 5.1 and 5.2.

69 Commentary 5 and 5.2 on Art. 26 OECD MC. According to case law, this concept also applies to the concept of ‘foreseeably relevant’ in the DAC; Case 682/15, *Berlioz*, ECLI:EU:C:2017:373.

70 OECD Commentary, above n. 30, para. 5.2.

71 Art. 3(13) DAC.

72 Art. 21(5) DAC.

73 Art. 25(1) DAC and Art. 23 GDPR.

ed 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 second paragraph continues with a detailed list of information the requesting authority must provide to the requested authority to demonstrate that the requested information is relevant. This includes, amongst others, the tax purpose for which the information is sought and the identity of the taxpayers. If this is a group, then the effort of the requesting authority greatly increases. Not only should the group be described in detail, but the authority should also explain the applicable law and based on what facts it believes that the taxpayers in the group have not complied with the applicable law. Finally, the authority must explain how the requested information would assist in determining compliance by the taxpayers in the group. This new article has the purpose of allowing requests for information about groups of taxpayers that cannot be identified individually, though under strict conditions.

The concept of foreseeable relevance is also used in Article 26 OECD MC and in Article 1 TIEA (see Section 3.2.3). In the *Berlioz* case, the ECJ confirmed that the concept of ‘foreseeably relevant’ in the DAC is similar to the concept used in Article 26 OECD MC and adopts the threshold that there must be a reasonable possibility that the requested information will be relevant.⁷⁴ This precludes tax administrations from making unspecified bulk request to other Member States and requesting information that is of no relevance to the investigation concerned.⁷⁵ The insertion of the new Article 5a DAC, described earlier, largely codifies this decision.⁷⁶

The expression ‘foreseeable relevance’ 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.⁷⁷

Moreover, according to the ECJ, a request for exchange of information seeking to engage in a ‘fishing expedition’ would be tantamount to an arbitrary or disproportionate intervention by the public authorities.⁷⁸ In essence, the ECJ confirms that such a request is impermissible.

The question is whether the ‘foreseeably relevance’ threshold only applies to information on request (Chapter II, Section I DAC), or whether it also applies to the mandatory automatic exchange of information under Chapter II, Section II DAC. The latter exchanges are, due to their nature, unrelated to ongoing investigations

concerning a specific taxpayer or concerning a specifically described group of taxpayers. On the one hand, the term ‘foreseeably relevant’ is used in Article 1(1) DAC which lays down the general subject matter of the DAC, strongly suggesting that this is an overarching standard. Article 5 DAC, on the exchange of information on request, specifically refers to Article 1(1) DAC, leaving no doubt as to the application of the ‘foreseeable relevance’ threshold. On the other hand, Chapter II, Section II DAC makes no specific reference to Article 1(1) DAC. Moreover, the scope and conditions of the mandatory automatic exchange of information in Chapter II, Section II DAC is very specific (in respect of the information collected and shared; it is not specific in respect of the group of taxpayers) and is not conditional on relevance. The structure of the DAC therefore suggests that the ‘foreseeably relevant’ threshold does not apply to the mandatory automatic exchange of information of Chapter II, Section II DAC.

If we use the Commentary on Article 26 OECD MC as a guiding interpretation instrument for the DAC, which the ECJ suggests we should do, then the conclusion may be different. The foreseeable relevance standard has the purpose to protect individuals and companies from unspecified, speculative and irrelevant request and storage of information. From para. 5.2 of the Commentary on Article 26 OECD MC, we conclude that only information that assists tax administrations in determining compliance by (a group of) taxpayers should be shared (and stored). The Commentary on Article 26 OECD MC even illustrates, as an example, that a (group) request that merely describes the provision of financial services to non-residents and only mentions the *possibility* of non-compliance by the non-resident customers, does not meet the standard of foreseeable relevance. The standard not only applies to information to be exchanged on request, but also to information exchanged automatically (para. 9 of the Commentary on Art. 26 OECD MC).

It is interesting to see a certain ‘function creep’ in the automatic exchange of information. Under the initial DAC (2011), a Member State would only communicate the specifically listed income and capital information of *residents* of another Member State to that other Member State. This makes sense, because it is not difficult to see that information about income and capital is foreseeably relevant for the residence state. The same applies for information shared under DAC2 (on the mandatory automatic exchange of financial information), DAC4 (on the exchange of information on CbCR) and DAC7 (on information on activities on online platforms). They each limit the circle of recipients of information to the *relevant* Member States where the subject is either resident or (potentially) has a taxable presence. Again, this makes sense because such information is not manifestly devoid of any foreseeable relevance for that Member State. On the other hand, DAC3 (on the exchange of APA and ATR) and DAC6 (on mandatory disclosure of potentially tax aggressive arrangements), makes the information indiscriminately accessible to *all* Member States.

74 Case 682/15, *Berlioz*, ECLI:EU:C:2017:373, at 67.

75 *Ibid.*, at 71.

76 Including the decision in the joined cases 245/19 and 246/19, *État luxembourgeois v. B and Others*, ECLI:EU:C:2020:795.

77 Case 245/19, *État luxembourgeois v. B*, ECLI:EU:C:2020:795, at 111.

78 *Ibid.*, at 113.

Even Member States which have no connection with the APA, ATR or the arrangement and with the persons involved therein, will have access to (personal) information and all details thereof.

We notice a huge difference in the protection of taxpayers fundamental rights between the exchange of information on request (which is subject to the foreseeable relevance standard) and the mandatory automatic exchange of information. When it comes to an automatic exchange of information that is of no relevance for the receiving Member State, we consider such exchange in violation 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.

4 Exchange of Information in the Light of Privacy and Data Protection

In our opinion, the mandatory international and European exchange of information has some vulnerabilities when it comes to the privacy protection of taxpayers. In this section, we will discuss a number of topics that fall under the notion of privacy and/or confidentiality and how those are dealt with in the different international agreements. We identify three areas where the (automatic) exchange of information may affect privacy: information which is used for other purposes, shared with other (Member) States and is provided by legal entities.

4.1 The Use of Information for Other than Tax Purposes

In principle, a taxpayer who provides tax information to the tax authorities must be able to trust that this information will not end up ‘in the wrong hands’. To achieve this, a number of safeguards against the abuse of information by tax authorities exist in bilateral and multilateral agreements as well as in the DAC: for instance, any further disclosure of information should not be incompatible with the purposes for which data were obtained. Thus, a domestic tax inspector may use obtained data for other purposes if in the issuing state the information can also be used for that purpose and – in principle – permission has been granted for that use. For example, in an international context, exchanged tax information may also disclose personal beliefs, lifestyles or other individual circumstances, which in some countries may be relevant in other areas than tax. In the following sections, we will discuss some of the safeguards and the challenges which have not yet been sufficiently addressed.

4.1.1 Bilateral and Multilateral (Model) Agreements on Exchange of Information

With respect to the use of information for other than tax purposes, the principle of reciprocity is particularly rel-

evant. Under the principle of reciprocity, which as explained in Section 2.1 was introduced way back in 1927, states do not have to exchange information which they would not receive from the other state. The principle can be found in Article 26(2) and (3)(a) and (b) OECD MC as well as in Article 7(1) TIEA and Article 21(2)(a) and (c) and (4) MAC.

Under the OECD MC and the MAC, the information generally may be used for other than tax purposes if (i) the principle of reciprocity is observed that is, the information may be used for other purposes under the laws of both states, and (ii) to the extent both states agree.⁷⁹ It is generally acknowledged that information may also be used for certain high priority matters (combat money laundering and the like), but for other non-tax purposes the two states would need to specifically agree on using the information.⁸⁰ Under a TIEA, the information may be used for tax purposes only.⁸¹ Thus, as a general rule, the use of information for other than tax purposes based on bilateral and multilateral agreements cannot be based on the general assumption that this would be acceptable, neither is it possible to use whitelists that contain certain purposes, unless this possibility is specifically included in the bilateral or multilateral agreement.

It seems on first sight that states can agree to use the information for any purpose. However, they are bound by their respective national laws, as is explicitly laid down in Article 26(2) OECD MC and 21(4) MAC. Therefore, the exchange of information for other purposes must have a legal basis in the laws of both states. If at least one of the two states is a Member State, that means that the rules of the EU on privacy and data protection must be observed. Whether the use of information for other purposes is in line with the principle of proportionality will have to be assessed on a case-by-case basis. On a more general level, the use of information to combat certain financial crimes, like money laundering, seems to be proportionate from a viewpoint of the European fundamental privacy rights, given that these crimes can only be combatted successfully if states work together on an international level. In this regard, it is however important to closely observe whether the right not to incriminate oneself (*nemo tenetur se ipsum accusare*) is properly observed. It goes beyond the scope of this article to discuss this any further.

One specific case, not so much of the use of information for other purposes, but of a disclosure of information to the general public (where it can be used for all kinds of purposes), is the use in court proceedings. From Article 26 OECD MC it becomes clear that the information may be disclosed in public court proceedings. To us this does not seem to be a problem as long as the requested state also has a system of public court hearings in tax matters, because the risk of the exchanged information becoming public already existed irrespective of the ex-

79 Art. 26(2), last sentence OECD MC, Art. 12(3), OECD Commentary 2017 and Art. 22(4) MAC.

80 OECD Commentary, above n. 30, para. 12.3.

81 Arts. 1 and 5, para. 1 Model TIEA.

change. However, in countries that have a system of private court hearings in tax matters,⁸² this constitutes a problem. Information that otherwise would not become public, might end up in the public domain by being introduced at a court hearing in another state. Under Article 26 OECD MC, states are not at liberty to refuse the exchange of information in that case, and doing so based on national law or even EU regulations would create an unlawful treaty override.

4.1.2 DAC

The principal objective of the DAC is to lay down rules and procedures under which Member States shall cooperate with each other in the assessment, administration and enforcement of domestic tax laws (including VAT and other indirect taxes). Article 16 DAC, however, expands the potential use of information to:

- Judicial and administrative proceedings that involve fiscal penalties; and
- Other purposes, with the permission of the originating Member State and only insofar as allowed under the laws of the receiving Member State and only on a reciprocal basis.

The possibility under the DAC to expand the authorised use of the received information to other than tax purposes is in line with the developments at the level of the OECD. In 2012, Article 26(2) OECD MC was amended by the sentence:

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 authorises such use.

While the OECD Commentary already provided for this possibility before 2012, the possibility of using the information for other purposes became the default situation in 2012.

The last two sentences of para. 2 of Article 16 DAC have been amended by DAC 7. They read:

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.

Since DAC7, Member States can publish a ‘whitelist’ of other purposes for which, in accordance with its national law, information and documents may be used without

82 Like, for example, the Netherlands (unless the hearing concerns a penalty), see Art. 27c GTA.

prior permission. The purpose of this amendment is to make it easier for Member States to use the information provided for other purposes to the extent that this is allowed under the national laws of both Member States.⁸³

4.2 Forward Information to Other (Member) States

Another aspect of the use of the information is sharing it with other states that are either not a part of the respective agreement, or that are so-called ‘outsider states’ who are not directly concerned with the information that is exchanged. The question in this respect is whether providing information to those states is in line with the principles of privacy and confidentiality.

4.2.1 Bilateral and Multilateral (Model) Agreements on Exchange of Information

The OECD Commentary 2017 is very clear on the disclosure of information to third countries: this is prohibited unless there is an express provision which allows for the disclosure.⁸⁴ The same goes for the Model TIEA (see Art. 8, third sentence). Under the MAC, the disclosure of information to third parties is permitted only if this is authorised by the state that has provided the information (see Art. 22(4) MAC).

If the state from which the information originated is an EU Member State, the authorisation under Article 22(4) MAC to disclose the information to a third state can in our view only be given by that Member State if the disclosure is permitted under the European privacy and data protection rules. Member States will therefore have to carefully analyse whether the third state can and will observe those EU standards, otherwise they violate the rights to privacy and data protection of the individuals the information is concerned with. To us, it seems rather unlikely that third states will observe these principles, as they are seen as the highest standard in the world.⁸⁵ Consequently, disclosure will only be possible if the information is anonymised,⁸⁶ which will render the disclosed information useless in most cases.

4.2.2 DAC

Third Countries

As we mentioned in Section 1, regarding the application of the DAC we focus on the mandatory automatic exchange of information: the systematic communication of predefined information to another Member State, without prior request, at pre-established regular intervals (see Art. 3(9) DAC). The automatic nature of sharing and storing information, in bulk and without prior request about individuals will conflict with the fundamental right to protect and respect the private and family life of individuals (Art. 7(1) Charter).

83 Para. 31 of the preamble of Council Directive (EU) 2021/514 of 22 March 2021 amending Directive 2011/16/EU on administrative cooperation in the field of taxation.

84 See OECD Commentary, above n. 30, para. 122.

85 See <https://gdpr.eu/what-is-gdpr> (last visited 20 January 2023).

86 See in that regard (on DAC7), *Parliamentary documents II* 2021/22, 36063, nr. 6, p. 13.

Article 24(2) DAC allows Member States to share information obtained under the Directive with a third country, under the condition that the originating Member State has consented to that communication and the third country has committed to combatting tax evasion.⁸⁷ Contrary to the approach introduced in DAC7 for the exchange of information between Member States, this paragraph contains no whitelist of pre-approved communications.

Pre-approval can, in our view, only be granted by a Member State if the information can be shared under the domestic laws and tax conventions of the originating Member State. This means that the information can only be shared to a third country with which the originating state has concluded a double tax convention or tax information agreement, covering this information. We find it difficult to agree with a situation where information collected and stored by the tax administration under the (protective) laws of the originating Member State can, via another Member State, end up in a third country if this information cannot be shared with that third country directly.

Outsider States

In respect of DAC3 and DAC6 we note that information is collected from taxpayers and intermediaries and that this information is made indiscriminately accessible, including personal data, to *all* Member States. Even with outsider states: Member States that have no relevant connection with the APA, ATR or the arrangement and with the persons involved therein. In our view, the large circle of recipients violates the standard of foreseeable relevance, because there is no reasonable possibility that the information will be relevant for outsider states and consider such exchange an arbitrary and disproportionate intervention by the public authorities. Bear in mind that DAC6 (and to a lesser explicit extent DAC3) has the purpose to ‘discover, dismantle and discourage’ aggressive tax planning structures. Discovering and discouragement requires information about the mechanics of the tax schemes in general and the extent of their use, but does, for example, not require personal data of taxpayers. In the exchange of information in DAC3 and DAC6, however, no distinction is made between the three objectives. Consequently, personal data is also shared where this is not necessary to achieve these objectives.

The disproportionate nature is even worse under DAC6, which requires that arrangements are reported and shared which have been made available to the taxpayer but have not been implemented (for example, because the taxpayer considers the arrangement as too aggressive, expensive or complex). Sharing personal data about taxpayers in these circumstances, especially to outsider states, is manifestly devoid of any foreseeable relevance for the outsider states. Even if the DAC provides a legal basis for the exchange, we are of the opinion that such

87 It is not clear towards whom the third country has to give such an undertaking.

exchange is disproportionate and unnecessarily burdensome on the taxpayers (EHRM/Charter), and that it does not meet the conditions of Article 23(1) GDPR.⁸⁸ For outsider states, there can be no economic or financial interest to have access to personal data concerning reportable arrangements which are not likely to concern them. Meanwhile, shortly before this article was submitted, the Belgian Constitutional Court recognised that the DAC6 may be unnecessarily broad and referred this question to the ECJ: does the DAC6 infringe on Article 7 Charter and Article 8 ECHR, because it is a disproportional privacy infringement which would not be pertinent for safeguarding of the internal market?⁸⁹

4.3 Exchange of Information Concerning Legal Persons

The drafters of the ECHR assumed that Article 8 applies only to natural persons and that legal entities cannot derive any rights from them. The treaty serves to protect ‘people’, as does the universal declaration of 1948. These treaties themselves give no indication that the provisions would also apply to legal persons. The rights to, for example, life (Art. 2) and personal freedom and security (Art. 5) also seem to be bound to the ‘spiritual life’ of the human being.⁹⁰ With regard to the rights to a fair trial (Art. 6), respect for private life (Art. 8), freedom of expression (Art. 10) and the right of assembly and association (Art. 11), this may be considered differently. By their very nature, these rights may also be granted to legal persons. A bond to the spiritual life is not necessary for this. Moreover, the rights and freedoms of the ECHR should be guaranteed without distinction according to ‘all human characteristics’, such as sex, race and religion (Art. 14) or, for example, the structuring of economic and financial interests.

The Dutch Supreme Court therefore ruled at the end of the last century that guarantees laid down in the ECHR generally apply not only to natural persons, but also to legal persons.⁹¹ In the opinion of the Supreme Court, there is in principle nothing to prevent legal persons from being able to derive rights from fundamental rights enshrined in the ECHR; behind the legal entity there is always a natural person.⁹² Legal persons would also have a ‘private sphere’ and should in principle be able to claim protection against an unlawful interference. As

88 Art. 23(1) GDPR allows Member States to restrict rights under the GDPR, on the condition that such restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the general public interest of the Union or of a Member State, in particular, an economic or financial interest of the Union or a Member State, including monetary, budgetary and taxation matters.

89 Belgian Constitutional Court, 15 September 2022, case no. 103/2022, ECLI:BE:GHCC:2022:ARR.103, preliminary question no. 5.

90 Dutch Supreme Court of 17 January 1990, ECLI:NL:HR:1990:ZC4207, BNB 1990/193, note by J.P. Scheltens, section 1.

91 Supreme Court 17 January 1990, ECLI:NL:HR:1990:ZC4207, BNB 1990/193, note by J.P. Scheltens. This decision relates more specifically to the application of Art. 6 ECHR on legal persons.

92 For a similar decision, see *Autronic AG*, 22 May 1990, ECLI:NL:XX:1990:AD1123, NJ 1991/47, at 47, in relation to the right to freedom of expression based on Art. 10 ECHR.

the taxpayer's successful lawyer argued in this case, it would lead to an unacceptably discriminatory situation if natural persons were treated differently according to whether they have structured their economic and financial interests differently.⁹³ For a taxpayer who has contributed his or her company to, for example, a Dutch Private Company (BV), it is not difficult to visualise the natural person behind the legal entity. For example, in the case of a listed multinational with multiple shareholders, it can be difficult to visualise the natural person behind the legal entity, but ultimately there is always a natural person behind the construction. For the applicability of the right to privacy and data protection concerning a legal entity, it must involve the processing of information ultimately relating to an identified or identifiable natural person.⁹⁴

Shortly after the turn of the century, the European Court of Human Rights ruled that legal persons can, under certain circumstances, claim protection of the safeguards of Article 8 ECHR; this Article must, in certain circumstances, be interpreted in such a way that legal persons can also derive protection from it.⁹⁵ An infringement is only justified if it is based on a legal provision, there is a legitimate aim and the infringement is necessary.

The question that arises is whether the mandatory provision and exchange of tax relevant information under the DAC is subject to sufficient constitutional safeguards with regard to personal data provided by legal persons, for example, with regard to 'legal entity sellers' on digital platforms, such as certain hotel chains on the platforms of well-known booking websites (DAC7). Why should natural persons selling on these platforms be able to invoke the right to privacy and data protection, while legal persons cannot?

Given the nature of the information provided by platform sellers having legal personality, the collection by tax authorities and the mandatory disclosure to other European tax authorities infringes the protection of their company data. However, a distinction must be made between data that does and does not fall within the scope of Article 8 ECHR; after all, a legal person can-

not rely on Article 8 ECHR actions in respect of data not falling within the scope of this article. Company data falling within the scope of Article 8 ECHR concern, for example, personal data about employees, a tax structure intended by the company or other data about the financial position of the company. For example, DAC7 requires a tax authority to report and automatically exchange with relevant Member States what has been paid by the reporting platform, for what activities and how many fees have been withheld.⁹⁶ Data that are known to everyone cannot be regarded as under Article 8 ECHR covered company data; for example, the data entered in the trade register, published annual accounts or information that has been made public via a press release.⁹⁷ Violation of the confidentiality of data covered by Article 8 ECHR can, under certain circumstances, lead to damage to the company.

Although a legal basis can be identified for the provision of information on sellers on digital platforms (DAC7) and a legitimate aim can be identified with the objective of achieving proper taxation, also with regard to legal persons the question can be raised whether the provision and use of data is necessary in the light of Article 8 ECHR. In addition, adequate safeguards must be in place against any disproportionate use of the data. These do not seem to exist in the provision of data based on the DAC. For example, domestic Dutch legislation does not provide for a system of legal protection to have the (further) provision or use of personal data subject to judicial review.

The absence of safeguards also makes the infringement vis-à-vis legal persons disproportionate. In the absence of independent constitutional safeguards to protect company data, we believe that the scope of the right to privacy and the protection of data should also be extended to legal persons. In the light of the rights to privacy and data protection, it should not matter whether a mandatory exchange of information by the tax authorities is regarding a natural or a legal person even if this leads to a wider scope of the ECHR, the Charter or the GDPR than was intended by its drafters.⁹⁸

93 Supreme Court 17 January 1990, ECLI:NL:HR:1990:ZC4207, *BNB* 1990/193, consideration 3.2 (second appeal).

94 Case 73/16, *Pušár*, ECLI:EU:C:2017:725, at 103: 'As is apparent from paragraphs 33 and 34 of the present judgment, the drawing up of a list, such as the contested list, which contains the names of certain natural persons and associates them with one or more legal persons within which those natural persons purport to act as company directors, constitutes "processing of personal data" within the meaning of Article 2(b) of Directive 95/46.' Art. 2(b) of Directive 95/46 provides that: 'processing of personal data (processing) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.'

95 *Sté Colas EST v. France*, 16 April 2002, ECLI:NL:XX:2002:AE4682, *NJ* 2003/452 with note by E.J. Dommering: both an office of a natural or legal person falls under the concept of residence of Art. 8 ECHR. See Case 419/14, *Web-MindLicenses*, ECLI:EU:C:2015:832, *BNB* 2016/55, at 72, for the application of Art. 7 Charter to legal persons.

96 Art. 8 bis quarter Directive (EU) 2021/514.

97 Dutch Supreme Court 15 December 1992, ECLI:NL:HR:1992:AD1798, *NJ* 1993/550 with note by A.H.J. Swart. This judgment was issued in the light of the mandatory publication of the annual accounts by legal entities pursuant to Art. 2:394 Dutch Civil Code, which concerns data relating to the company run by a legal person, which is not covered by Art. 8 ECHR.

98 For the purposes of Art. 8 Charter or GDPR, Union law must apply. See Case 620/19, *Land Nordrhein-Westfalen v. J&S Service*, ECLI:EU:C:2020:1011, at 33-35 (translated): '(33) In that regard, it should be recalled that the Court has repeatedly held that it has jurisdiction to rule on requests for a preliminary ruling concerning provisions of EU law in situations where the facts in the main proceedings fell outside the scope of EU law and therefore fell within the exclusive competence of the Member States, but in which those provisions of EU law had been made applicable by national law by referring to the content of those provisions (judgment of 12 July 2012, *SC Volksbank România*, C-602/10, EU:C:2012:443, paragraph 86 and the case-law cited). (34) Such a power is justified by the obvious interest for the EU legal order that, in order to avoid divergent interpretations in the future, provisions taken from EU law should be interpreted uniformly (see, to that effect, judgments of 18 October 1990, *Dzodzi*, C-297/88 and C-197/89, EU:C:1990:360, paragraph 37, and of 12 December 2019, *G.S. and V.G.*

5 Conclusion

This contribution summarises to what extent the international and European exchange obligations should deserve particular attention in light of the privacy provisions of Article 8 ECHR and Articles 7 and 8 Charter, when it comes to the use of information for non-tax purposes, the provision to other (Member) States and the exchange of information concerning legal entities. From this perspective, we have limited the overarching international legal sources of the exchange of information and the privacy rules they contain to a brief introduction in Section 2. A review of the rights to privacy and data protection of (automatically) exchanged information means, in particular, a test against the necessity of such an exchange in general and its proportionality in particular (Section 3). The fact that in some situations data traceable to taxpayers must also be exchanged with Member States that have no involvement (DAC3 and DAC6) and can also be used for non-tax purposes (Art. 16(2) DAC) seems to be contrary to the proportionality and – taking into account the foreseeable relevance standard – even the legality requirement as a test component for the justification of an infringement of the rights of privacy and data protection (Section 4).

In this respect, we have observed that on the one hand, with respect to confidentiality, the international agreements on the exchange of information tend to be stricter than the EU directives. Both the use of information for other than tax purposes (safe for combatting certain economic crimes) and the disclosure of information to third parties are either prohibited or strictly limited under those agreements. To a certain extent, this seems logical, as the EU internal market is integrated to a much higher degree than what can be achieved by international agreements. On the other hand, when it comes to privacy and data protection, the agreements contain either no specific rules or the rules are by no means as far-reaching as the GDPR. Furthermore, privacy and data protection rules under international agreements tend to be not prohibitive, but rather grant states a possibility to refrain from the exchange of information.

The domestic implementation of the DAC seems to further weaken the protection of personal data. However, we believe that when rights protected by the GDPR are violated, there should be the possibility to challenge this in court. Returning to the Dutch situation, we point to the possibility that taxpayers who believe that their privacy rights under the GDPR are being violated can

(Threat to public policy), C-381/18 and C-382/18, EU:C:2019:1072, paragraph 42 and the case-law cited). (35) However, the Court has jurisdiction only to examine provisions of EU law. In its reply to the national court, it cannot take account of the general scheme of the national provisions referring to EU law, but at the same time determine the scope of that reference. What limits, if any, the national legislature has imposed on the application of EU law to purely internal situations to which it applies only through national law is a question of national law which can therefore be assessed only by the courts of the Member State concerned (see, to that effect, judgment of 18 October 1990, *Dzodzi*, C-297/88 and C-197/89, EU:C:1990:360, paragraph 42)'.⁹⁹

apply to the Dutch administrative court for a full assessment of the guarantees of the domestic (tax) confidentiality provision.⁹⁹ Although this is the Dutch case, we can imagine that the ECJ and the European Court of Human Rights also believe that – in line with the *Berlioz* and *État luxembourgeois* cases – such an appeal option should be present in the domestic legislation of all (Member) States.¹⁰⁰ In addition to natural persons, in our opinion, legal entities should also be able to rely on the protection of the rights to privacy and data protection.

Finally, in light of the international exchange obligations of the Dutch tax authorities, the domestic confidentiality provision appears to be the only provision that protects the interests of taxpayers providing information. However, as soon as the tax data have been passed on to other tax authorities, this confidentiality can no longer be guaranteed. The fact that other tax authorities should keep the data secret in the same way as the national tax authorities do with the data received, poses a risk to the taxpayer whose data is provided for non-tax purposes, to other (Member) States or in the event that the taxpayer is a legal entity. A breach of confidentiality by the receiving tax authorities does not appear to be open to taxpayers' legal remedies. Nor does a preliminary assessment of the information against the rights to privacy and data protection seem possible. The purposes for which the data may be used should in our view therefore be exhaustive, with the establishment of proper taxation always being the main objective.

⁹⁹ This possibility relates in particular to the written decisions on requests based on the Arts. 15-22 GDPR. Art. 34 of the Dutch GDPR Implementation Act (*Uitvoeringswet Algemene verordening gegevensbescherming*) stipulates that such decisions, insofar as taken by an administrative body, are to be regarded as a decision that is open to objection within the meaning of Art. 1:3 of the Dutch General Administrative Law Act (*Algemene wet bestuursrecht*). See for instance Court Midden-Nederland, 23 June 2020, ECLI:NL:RBMNE:2020:2424 (preliminary judgment) with regard to a privacy violation by providing non-anonymised data to a journalist by the Financial Supervision Office (*Bureau Financieel Toezicht*).

¹⁰⁰ For legal protection-issues in the context of international exchange of information, see the contribution of W. Boei and J.J. van Dam to this Erasmus Law Review Special.