The Protection of Personal Data within the frame of the International Automatic Exchange of Financial Account Information

by

KRÄHENBÜHL BLAISE

I. Introduction ...................................................................................................................................... 2

II. The International Data Protection Legal Framework ......................................................... 4
  1. The UN Legal Framework ........................................................................................................ 4
  2. The OECD Privacy Guidelines ............................................................................................... 6
  3. The ECHR and Convention 108 of the Council of Europe .............................................. 7
  4. Data Protection within the EU ............................................................................................... 12

III. Data Protection under the CRS Legal Framework ............................................................. 22
  1. The Multilateral Convention on Mutual Administrative Assistance in Tax Matters .................................................. 22
  2. The Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information ..................... 25

IV. The Taxpayer's Rights ............................................................................................................. 26
  1. Applicable Rules ..................................................................................................................... 27
  2. Legal Basis ............................................................................................................................ 28
  3. Legitimacy, Necessity and Proportionality of the Processing ............................................. 30
  4. Safeguards in case of Cross-Border Transmission of Data ................................................ 35
  5. Data Security and Confidentiality ........................................................................................... 42
  6. Right to be Informed and Data Breach Notification .............................................................. 45
  7. Right of Access, Rectification and Erasure .............................................................................. 47
  8. Safeguards in case of Subsequent Use and Onward Transfers ........................................ 48
  9. Legal Remedy ....................................................................................................................... 49
  10. Right to Compensation ......................................................................................................... 50

V. Conclusion .................................................................................................................................. 51

VI. Bibliography .......................................................................................................................... 57

VII. Table of abbreviations ......................................................................................................... 60
I. Introduction

With the Introduction of the OECD / G 20 Common Reporting Standard (CRS), the Automatic Exchange of Financial Information in tax matters (AEoI) has raised a strong concern about the protection of privacy, that were already approached with the US Foreign Account Tax Compliant Act (FATCA).

Indeed, tax and bank personal information can reveal numerous valuable aspects of the life and activities of the citizens and their commercial and personal relationships and the amount of data involved, as well as the number of the potentially concerned persons, is huge.

The risks of unlawful access to it have also significantly increased in the recent years following the revelations of large scale hacking operations, including against tax administrations, or States mass surveillance, or for commercial purposes, such as consumers profiling.

Meanwhile, the national laws and international conventions for the protection of personal data are developing rapidly to take into account the latest progress of information technologies and by giving more rights to the data subjects.

Up to now, only a few scholars have examined in details the rights of the taxpayers to have their privacy protected on the international level\(^1\) and the problem is complex as various rules may interact and different cultural backgrounds be implied.

At the present stage, it is important to keep in mind that the conventional and constitutional provisions on the right to privacy are intended to have a «horizontal effect», being applicable to both the private and the public sector processing individuals’ personal data.

The right to access to the personal data being treated by the State authorities or private persons, the right to respond to any attack against one’s personal honor in the press, the criminal prosecution of such attacks or the medical secrecy are emerging, among others, from the right to privacy as provided for, notably, by the United Nations (UN) Covenant on Civil and Political Rights or the European Convention on Human Rights (ECHR).

\(^{1}\) See BAKER P. / PISTONE P., The practical protection of the taxpayers’ fundamental rights, branch reports on the 69th congress of the IFA, The Hague, 2015, p. 21 and 65
As far as the AEoI is concerned, the data protection legislation is in principle applicable, under the reservation of specific provisions provided for in the laws implementing the AEoI that would prevail.

The aim of this Master Thesis is, on the first hand, to provide a comprehensive overview of the main applicable international data protection legal instruments and on how it would apply to financial information concerning individuals\(^2\), notably through the relevant case law, being understood that the same principles may apply to other forms of exchange of financial information for tax purposes, such as FATCA or the Exchange of Information on demand, with the necessary adjustments.

At least from the European perspective, three different standards may be distinguished among the participating jurisdictions to the CRS AEoI: (1) The EU Member States submitted to the EU Data Protection Directive (28 among 100 Contracting States), with the most enhanced level of data protection; (2) The contracting States to the ECHR and/or to Convention 108 of the Council of Europe as well as the countries benefiting from an adequacy decision from the EU (51 Contracting States), that share an intermediate and similar level of data protection and (3) the contracting States to the UN Covenant on Civil and Political Rights (88 Contracting States)\(^3\).

Different requirements and standards regarding personal data protection are to be applied depending on which of these categories the involved jurisdictions belong.

The second part will summarize the personal data protection standard provided for by the Convention on Mutual Administrative Assistance in Tax Matters (The Multilateral Convention) and the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information (MCAA).

In the last part of the thesis, the conditions under which the AEoI is admissible with regard to the data protection principles and rules aforementioned will be examined and the taxpayers’ rights detailed accordingly, which will determine as well the obligations of the actors concerned (the Financial Reporting Institutions and the competent tax authorities).

---

\(^2\) The data protection laws usually only apply to individuals, but some legal persons may be protected as well under certain conditions, see, for example, ECJ Cases C-92/09 and C-93/09 of 9 November 2010, § 52-53 and 87 - 88

\(^3\) See Annex
II. The International Data Protection Legal Framework

1. The U.N. Legal Framework

Following the adoption, on 10 December 1948, by the United Nations General Assembly, through a resolution, of the Universal Declaration of Human Rights, which protected the individuals against arbitrary interferences with their privacy, family, home or correspondence and attacks upon their honour and reputation, the International Covenant on Civil and Political Rights (the UN Covenant) was adopted by the United Nations General Assembly on 16 December 1966 and entered into force in 1976. It has been ratified by 187 States up to the present day.

Article 17 of the Covenant states that no one shall be subjected to arbitrary or unlawful interference with this privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation and that everyone has the right to the protection of the law against such interference or attacks.

This article appears to be the common minimum global standard for personal data protection that is shared by almost all participating jurisdiction of the Multilateral Convention on Administrative Assistance in Tax Matters. Its scope is limited to the prohibition of “arbitrary” or “unlawful” interference in the individuals’ privacy, being understood that arbitrary interference also comprises interferences that would not be reasonable in the particular circumstances, even if it is provided for under the law.

The States parties are under the obligation, on one hand, not to engage themselves in interferences inconsistent with Article 17 of the Covenant and, on

---

4 UN General Assembly Resolutions have in principle no binding effects (see below, note n° 13), but this Universal Declaration, at least as an international custom, appears to have a “binding force” superior to that of a simple resolution of the General Assembly: JONATHAN G. C., Human Rights Covenants, in: R. Bernhardt (ed.), Encyclopedia of Public International Law, Instalment 1, Amsterdam, New-York, Oxford, 1981, p. 297
5 Art. 12 of the Universal Declaration of Human Rights, adopted by UN General Assembly Resolution n° 217 A (III)
6 See Annex. Some major participating countries have however not signed or ratified this Covenant, as it is the case for China, Malaysia, Saudi Arabia or Singapore
the other hand, to provide the legislative framework prohibiting such acts by natural or legal persons, including adequate legislation for the protection of personal honour and reputation, so that everyone is effectively able to protect himself against unlawful attacks and to have effective remedy against the responsible persons. 

The national legislations adopted should specify the precise circumstances in which such interferences may be permitted and decisions to authorize such interferences taken on a case-by-case basis.

The data collected should be protected and the holding of it be regulated by law; every individual should have the right to ascertain in intelligible form whether and what personal data is processed in automatic data files and for what purposes and every individuals should have the right to request modification or elimination when data has been collected or processed contrary to the provisions of the law or if the files contain incorrect personal data.

The UN Covenant is the first human right instrument with binding effect mentioning the individual rights to privacy. Whether the rights protected by the Covenant are directly applicable in a specific case (self-executing) should be assessed on a case-by-case basis and depends on the way the State Parties apply (or not) the provisions of the Covenant according to their own laws and procedures.

Article 17 of the Covenant was complemented by the UN Guidelines for the Regulation of Computerized Personal Data Files, adopted on 14 December 1990 by the UN General Assembly, through Resolution 45/95. These

---

8 Idem, paragraph 9 and 11
9 Idem, paragraphs 2 and 8
10 Idem, paragraph 10
11 See Art. 2 of the UN International Covenant on Political and Civil Rights; JONATHAN, op. cit., p. 298; BESSON S., Droit international public, Abrégé de cours et résumés de jurisprudence, Bern, 2011, p. 145
12 The self-executing character of the provisions of the UN Covenant will vary whether the State Parties follow a monist or dualist approach regarding the relationship between international and their national law. Furthermore, individuals may only rely on such provisions, as a principle, when it clearly confers individual’s rights which are sufficiently defined and precise, see AUER A. / MALINVERNI G. / HOTTELIER M., Droit Constitutionnel Suisse, Volume I, l’Etat, 2nd edition, Bern, 2006, n° 1291-1292, 1305-1309, and 1881; BESSON, op. cit., p. 148
13 The UN General Assembly Resolutions have no binding effect as such: Charter of the United Nations, Art. 10; ZIEGLER A. R., Introduction au droit international public, 3rd edition, Bern, 2015, No. 142
guidelines detail the main principles and safeguards, similar to other international data protection instruments, which should apply regarding the collection and processing of personal data through computerized files\textsuperscript{14}, including the requirement of independent, impartial and technically competent data protection national authorities\textsuperscript{15}. As far as trans-border flow of personal data is concerned, it is allowed and promoted at the condition that both countries’ legislation offer comparable safeguards\textsuperscript{16}.

The UN General Assembly also adopted the Resolution on the Right to Privacy in the Digital Age on December 18\textsuperscript{th}, 2013\textsuperscript{17}, after having expressed its concern about the negative impact on the exercise and enjoyment of Human Rights of the collection of personal data carried out on a mass scale, which calls the States to create the appropriate conditions to prevent violation of the right to privacy, including in the context of digital communication, and to review their procedures, practices and legislation.

2. The OECD Privacy Guidelines

On July 11th, 2013, the OECD Council issued a newly revised version of its guidelines governing the protection of privacy and transborder flows of personal data, initially adopted through a recommendation on 23 September 1980. The revision is considering the future of the Internet economy in right of changing technologies, markets and users’ behaviours and the growing importance of digital identities.

These guidelines provide for a number of minimum principles to be respected when personal data are processed, that are comparable to other international data protection instruments or national legislations, including the principle that the collection of personal data should be limited and obtained by lawful and fair means and, where appropriate, with the knowledge or

\textsuperscript{14} Notably, the principle of lawfulness and fairness, accuracy, security of the data, rights of access, rectification and erasure in the case of unlawful, unnecessary or inaccurate entries, to be informed of the addressees of the data and to benefit from a legal remedy to enforce these rights, see Principles 1, 2, 4 and 7 of the UN Guidelines

\textsuperscript{15} Principle 8 of the UN Guidelines

\textsuperscript{16} Principle 9 of the UN Guidelines

\textsuperscript{17} Resolution 68/167, The Right to Privacy in the Digital Age, which was adopted soon after the disclosure by former CIA and NSA Agent Edward Snowden, starting from June 6th, 2013, about mass surveillance by the US and some of its allies of communications
consent of the data subject\textsuperscript{18}, and should be relevant for the purposes for which they are to be used, accurate, complete and kept up-to-date\textsuperscript{19}.

The OECD guidelines are referred to within the frame of the CRS AEoI\textsuperscript{20}, but they have no binding effects, being only mere recommendations. At the present day, they are 35 Members of the OECD participating to the AEoI\textsuperscript{21}.

3. The Council of Europe Legal Framework

A. The Convention for the Protection of Human Rights and Fundamental Freedoms

The Convention for the Protection of Human Rights and Fundamental Freedoms of November 4\textsuperscript{th}, 1950 (The European Convention on Human Rights - ECHR) has been ratified by 42 of the 95 contracting States participating in the AEoI\textsuperscript{22}. It has a full binding effect\textsuperscript{23} and any person may file an application to the European Court of Human Rights (ECtHR)\textsuperscript{24}. The Contracting States are bound by the judgments rendered by that Court\textsuperscript{25}.

Article 8 ECHR grants to everyone the right to respect for his private and family life, his home and his correspondence\textsuperscript{26}.

The ECtHR has notably examined the compatibility with Article 8 ECHR of cross border exchange of financial information for a tax purposes\textsuperscript{27} or within the frame of criminal proceedings\textsuperscript{28}.

According to it, information retrieved from banking documents, including individual’s bank correspondence, material and e-mails, amounts to personal

\textsuperscript{18} Art. 7 OECD Privacy Guidelines
\textsuperscript{19} Art. 8 OECD Privacy Guidelines
\textsuperscript{20} See Revised Explanatory Report to the Multilateral Convention, Nr. 216, page 85
\textsuperscript{21} See Annex
\textsuperscript{22} See Annex
\textsuperscript{23} Art. 1 ECHR
\textsuperscript{24} Art. 34 ECHR
\textsuperscript{25} Art. 46 ECHR
\textsuperscript{26} Some other rights protected by the ECHR might also apply within the framework of the AEoI, such as Art. 13 which grants everyone the right to have an effective remedy before a national authority
\textsuperscript{27} See ECtHR Case GSB vs Switzerland, 22.03.2016, Application Nr. 28601/11
\textsuperscript{28} See ECtHR Case of M.N. and others vs San Marino, 07.07.2015, Application Nr. 28005/12
data concerning individuals and is protected under Article 8 ECHR\textsuperscript{29}. In the case of transmission of bank data to other countries, individuals suffer an interference with their rights to respect for their private life\textsuperscript{30}. The storing of data relating to the private life of an individual itself, such as bank data, falls within the application of Article 8 ECHR\textsuperscript{31}.

The right to privacy may only be restricted in accordance with the law and if it appears to be 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 and morals, or for the protection of the rights and freedoms of others »\textsuperscript{32}.

Therefore, the impugned measure must first of all have a basis in domestic law, which must be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual, if need with appropriate advice, to regulate his conduct\textsuperscript{33}.

Secondly, the interference has to be based on one or more of the legitimate aims mentioned above, such the economic well-being of the country or the prevention of crime in the case of the AEoI\textsuperscript{34}.

Finally, the measure must further be necessary in a democratic society. This condition is closely linked with the proportionality principle. As a consequence, all the different private and public relevant interests must be com-

\textsuperscript{29} See ECtHR Case M.N. and others vs San Marino, \textit{op. cit.}, § 51 and 52
\textsuperscript{30} ECtHR Case GSB vs Switzerland, \textit{op. cit.}, § 50
\textsuperscript{31} ECtHR Case Amann vs Switzerland, \textit{op. cit.}, § 65, 69, 78 and 79
\textsuperscript{32} See Art. 8 § 2 ECHR
\textsuperscript{33} ECtHR Case M.N. and others vs San Marino, \textit{op. cit.}, § 72 ; Case GSB vs Switzerland, \textit{op. cit.}, § 68
\textsuperscript{34} For instance, the search for clues and proof in case of an investigation against a taxpayer for tax evasion was, for example, considered as a legitimate aim within the frame of the exchange of banking information, see ECtHR Case Brito Ferrinho Bexiga Villa-Nova vs Portugal, 1.3.2016, Application Nr. 69436/10; see also Case GSB vs Switzerland, \textit{op. cit.}, § 83 in which the justification put forward by the Swiss authorities for a transmission to the US tax authorities of banking data within the frame of the litigation between the States about undeclared bank accounts, which was accepted by the ECtHR, was the economic well-being of Switzerland, as the transmission of the required information formed part of an whole effort by the Swiss Government to settle the conflict between the US Tax Authorities and the bank UBS and as the very survival of that bank of national importance was jeopardized in that case; The ECtHR also accepted that the prevention of corruption may be a valid justification for the publication of banking or tax information about a municipal politician, see ECtHR Case Wypych vs Poland, 25.10.2005, Application Nr. 2428/05
pared to assess whether the interference is necessary. To this regard, the ECtHR considers that bank and financial data about a person do not deserve an enhanced protection, such as, for instance, information about individuals’ health 35.

But, when assessing whether a measure is necessary in a democratic society, the ECtHR attaches a great importance to the presence of relevant procedural safeguards, especially an effective legal remedy 36. In particular, third persons, not mentioned in a request for assistance within the frame of an exchange of information for criminal and tax purposes, must be able to access to a judicial authority before the information is transmitted 37.

B. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

a) Convention 108

The Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data of 28 January 1981 (Convention 108) includes all the principles mentioned in the UN guidelines for the Regulation of Computarized Personal Data Files and the OECD Privacy Guidelines.

It is the first binding international legal instrument in the field of data protection and a reference for national legislations. It is designed to have a universal scope, allowing non-member States to accede to it 38 and the accession to

35 ECtHR Case GSB vs Switzerland, op. cit., § 89, 93 and 97; however, when there is a decision to transfer financial data, it may have serious repercussions on the taxpayers’ reputation and honour, especially if the concerned person might appear as involved in an on-going criminal investigation that is given a wide media coverage, in which case it may be considered as an important possible impact on their personal life, see ECtHR Case M.N. and others vs San Marino, op. cit., § 34 and 39
36 See ECtHR Case M.N. and others vs San Marino, op. cit., § 80
37 Idem, § 74, 78 ff and 85, where the Court found out that there was a violation of Art. 8 ECHR due to the lack of an effective control
38 See Art. 23 of Convention 108. At the present day, all the 47 members of Council of Europe have ratified it, as well as three non-members of Council of Europe: Uruguay, Senegal and Mauritius
it is a deciding advantage to get an adequacy decision from the other members of Council of Europe.\(^{39}\)

Convention 108 covers all kinds of automatic processing of personal data in the private and the public sector, including within the field of police, justice or intelligent services.\(^{40}\) It is not directly applicable, but the contracting States have to take the necessary measures in their domestic law to give effect to it.\(^{41}\)

The main principles to be respected are, in substance, the fairness and lawfulness of the collection and processing of personal data, the legitimate purpose specification and limitation, the accuracy and necessary update of the data collected and processed, the holding period limitation and the data security.\(^{42}\) Furthermore, the data retained must be adequate, relevant and not excessive in relation to the purposes for which they are stored.\(^{43}\)

The following rights are granted to any data subject to which Convention 108 applies: to establish the existence of an automatic personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; to obtain confirmation of whether personal data are stored in the automatic data files; to obtain the rectification or erasure of data having been processed contrary to its principles and to have a remedy if the right to obtain access, rectification or erasure is not complied with.\(^{44}\)

Exceptions and restrictions to its principles and the rights granted are only admissible if they are provided for by the law and constitute a necessary measure in a democratic society in the interest of a legitimate aim.\(^{45}\)

With regard to the trans-border communication of personal data, it may not be prohibited or subject to special authorization for the sole purpose of the protection of privacy if it is sent, by whatever medium, to another contract-

---


40 Idem; Art. 3(1) of Convention 108

41 Art. 4 of Convention 108

42 Art. 5 and 7 of the Convention 108

43 Idem

44 Art. 8 of the Convention 108

45 Art. 9 of the Convention 108
ing Party to Convention 108⁴⁶, but no specific rules are provided regarding the transfer of personal data to none contracting States.

b) **The Additional Protocol to Convention 108**

The additional protocol, which entered into force in 2004 and which has been ratified by the major part of the Contracting Parties to Convention 108⁴⁷, provides that each Party shall have one or more supervisory independent authorities with powers of investigation and intervention and power to hear claims. Its decisions may be appealed through the courts⁴⁸.

The Protocol also provides rules for the transmission of personal data into a State non Party to Convention 108 or not ensuring an adequate level of protection, which may not be allowed unless it is justified by specific interests of the data subject or legitimate prevailing interests, especially important public interests or unless adequate safeguards are provided⁴⁹.

c) **The Modernization Process of Convention 108**

Since October 2011, discussions about the modernization of Convention 108 have taken place within the frame of the Council of Europe⁵⁰. The main objectives of the revision are to adapt to the increasing use of new information and communication technologies, globalization and the increase of personal data flows, as well as the reinforcement of the monitoring mechanism and of the control of the data subjects over the use of their personal data⁵¹.

Its territorial scope would be extended, within the meaning that it would apply to any public body in the jurisdiction of a contracting State and to any

---

⁴⁶ Art. 12 of the Convention 108
⁴⁷ Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, ETS No. 181, of 8 November 2001 (39 ratifications)
⁴⁸ Art. 1 of Additional Protocol to Convention 108
⁴⁹ Art. 2 of Additional Protocol to Convention 108
⁵⁰ See Draft of the modernized version of Convention 108 of September 2016 and Draft of explanatory report about the proposal for modernization of Convention 108 prepared on the basis of retained consultation and informal conference of August 24th, 2016, both available at www.coe.int
⁵¹ See Draft of explanatory report, op. cit., page 3
private body as far as the processing has sufficient links with the territory of one of the contracting Parties\textsuperscript{52}.

The proportionality principle, as set out in Convention 108 would be reinforced, within the meaning that a principle of « minimization of data » is provided for, according to which the collection and the processing must be limited to the strict minimum necessary\textsuperscript{53}.

Regarding the security of the data, a data breach notification obligation is introduced, according to which the controller of the data file must inform the competent control authority of violations of data which may seriously affect the right and fundamental freedom of the concerned data subjects\textsuperscript{54}.

Furthermore, the principle of the transparency obliges the controller of the file to provide information about its identity, the purposes of the treatment, the recipients of the data, the duration of the holding, the legal means, etc., and further information in case of transfer of personal data to third Parties\textsuperscript{55}.

4. **Data Protection within the EU**

A. **The EU Data Protection Legal Framework**

Within the EU, Article 7 of the European Charter of Fundamental Rights of 26 October 2012\textsuperscript{56} provides for the right to privacy and a specific fundamental right to protection of personal data was introduced in its Article 8.

The EU data protection framework goes beyond the Council of Europe Convention 108, by giving more substance and amplifying the principles of Convention 108\textsuperscript{57}.

\textsuperscript{52} See Art. 3 of the Draft of the modernized version of Convention 108, Draft of explanatory report, \textit{op. cit.}, p. 4-5 and Report of the President of the Consultative Committee of Convention 108, \textit{op. cit.}, p. 2

\textsuperscript{53} See Report of the President of the Consultative Committee of Convention 108, \textit{op. cit.}, p. 6 and Art. 5 of the draft modernized version of Convention 108

\textsuperscript{54} See Art. 7, § 2 of the Draft of the modernized version of Convention 108

\textsuperscript{55} See Art. 7bis of the Draft of the modernized version of Convention 108 and Report of the consultative Committee, \textit{op. cit.}, p. 8-9)

\textsuperscript{56} European Charter of Fundamental Rights of 26 October 2012 (2012/C 326/02)

\textsuperscript{57} See Recital 11 of Directive 95/46/EC: “\textit{The principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing}
a) Data Protection Directive 95/46/CE

The 1995 Data Protection Directive (Directive 95/46/EC) is the main legal instrument for the realization of the right to privacy and to data protection.

The national provisions implementing it are applicable in the field of the administrative cooperation and exchange of financial information for tax purposes within the EU, as set forth by Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation, but with limitations.

Data Protection Directive establishes the principles and rules that must be contained in the national legislation concerning the processing of personal data of individuals by natural or legal person, public authority, agency or any other body, wholly or partly by automatic means or otherwise, if the data form part of a filing system or is intended to form part of a filing system.

The main principles provided by the Data Protection Directive are substantially the same as in the Council of Europe Convention 108. Data subjects have notably the right to be informed about data processing concerning them, its purposes, the recipients or the categories of recipients and of their access and rectification rights.

They are granted the right to access to the data concerning them and the right of rectification, erasure or blocking of data in the case of unlawful processing, in particular because of incomplete or inaccurate data.

Restrictions to the data subjects’ rights are in principle only admissible when such restrictions constitute a necessary measures to safeguard, among others, an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters.

---

58 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data
59 See below, let. c)
60 Art. 2, let. a) and d) and Art. 3(1) Directive 95/46/EC
61 See above, let. B(a) and b), p. 9 - 11
62 Art. 10 and 11 Directive 95/46/EC
63 See Art. 12 and 14 Directive 95/46/EC
64 Art. 13 Directive 95/46/EC
which is the justification that apply for any restriction within the frame of administrative cooperation in the field of taxation\textsuperscript{65}.

A right to obtain compensation from the controller for the damage suffered is granted to the data subjects in the case of unlawful processing operation, except if the controller proves that he is not responsible for the event giving rise to the damage\textsuperscript{66}.

The transfer of personal data to third countries may take place only if the third country in question ensures an « adequate level of protection » in the light of all the circumstances\textsuperscript{67}. The EU Commission may issue an adequacy decision concerning one country, in which case the Member States take the necessary measures to comply with the Commission's decision\textsuperscript{68}. Transfer of personal data to a country not ensuring such an adequate level of protection may only take place under strict conditions and with adequate safeguards\textsuperscript{69}.

The EU data protection legislation went through a reform that started in 2012, soon after the modernization process initiated by the Council of Europe of its Convention 108, and ended with the adoption of the General Data Protection Regulation on 27 April 2016.

**b) General Data Protection Regulation (EU) 2016/679 (GDPR)**

The General Data Protection Regulation (GDPR), which will be directly applicable\textsuperscript{70} from 25 May 2018\textsuperscript{71} and replacing Data Protection Directive 95/46/CE, offers extensive and precise rights and obligations.

Its territorial scope of application is extended to any processing of personal data of EU data subjects if related to the offering of goods or services to such data subjects or the monitoring of their behaviour\textsuperscript{72}.

The notice requirements are expanded as well\textsuperscript{73} and a data breach notification mechanism has been introduced\textsuperscript{74}.

\textsuperscript{65} See Art. 25 of Directive 2011/16/UE
\textsuperscript{66} Art. 23 Directive 95/46/EC
\textsuperscript{67} Art. 25(1 – 2) Directive 95/46/EC
\textsuperscript{68} Art. 25(6) Directive 95/46/EC
\textsuperscript{69} See Art. 26 Directive 95/46/EC
\textsuperscript{70} See Art. 288 of the Treaty on European Union and the Treaty on the Functioning of the European Union (2012/C 326/01)
\textsuperscript{71} See Art. 99(2) of GDPR (EU) 2016/679
\textsuperscript{72} Art. 3 and Recital 22 – 25 GDPR (EU) 2016/679
Administrative fines may be imposed\textsuperscript{75} and the competent courts for claims of compensation are designated\textsuperscript{76}.

Finally, the conditions for a transfer of personal data to third countries not covered by an adequacy decision are more detailed and are, as a principle, only authorized in the presence of specified appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available\textsuperscript{77}.

c) The Data Protection Provisions in Directive 2011/16/EU on Administrative Cooperation in the Field of Taxation

Data protection provisions are also mentioned in Directive 2011/16/EU on Administrative Cooperation in the Field of Taxation\textsuperscript{78}, applicable in the case of exchange of information between EU Member States for tax purposes.

In particular, it provides that the national provisions about the protection of personal data implementing the Directive 95/46/EC are applicable, with specific limitations to the right to be informed about the collection and treatment of personal data, the right of access, rectification, blockage and erasure and of publicizing of the processing operations\textsuperscript{79}.

\textsuperscript{73} They must notably include the retention time and, if applicable, the fact that the controller intends to transfer personal data to a third country and the existence or absence of an adequacy decision by the EU Commission or appropriate or suitable safeguards. The data subjects have the right to obtain from the controller a free copy of the personal data undergoing processing and the information about to whom the personal data have been or will be disclosed, in particular recipients in third countries, see Articles 13 – 15 GDPR.

\textsuperscript{74} The data controller will be under a legal obligation to notify the Supervisory Authority in the case of personal data breach and, if it is likely to result in a high risk to the rights and freedoms of natural persons, to the concerned data subjects, except if the personal data is rendered unintelligible to any person who is not authorized to access it or if sufficient subsequent measures have been taken to reduce the risk for the data subjects or if it would involve disproportionate effort, see Articles 33-34 GDPR (EU) 2016/679.

\textsuperscript{75} Art. 83 GDPR (EU) 2016/679

\textsuperscript{76} See Art. 82(6) cum 79(2) GDPR (EU) 2016/679

\textsuperscript{77} See Articles 46 and 47 GDPR (EU) 2016/679

\textsuperscript{78} Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC.

\textsuperscript{79} See Art. 25 of the Council Directive 2011/16/EU: « All exchange of information pursuant to this Directive shall be subject to the provisions implementing Directive 95/46/EC. However, Member States shall, for the purpose of the correct application of this Directive, restrict the scope of obligations and rights provided for in Art. 10, Art. 11(1), Art. 12 and 21 of Directive 95/46/EC to the extent required in order to safeguard the [financial
With the introduction of the mandatory automatic exchange of information through Directive 2014/107/UE\(^{80}\), it was clarified that both the Reporting Financial Institutions and the competent authorities of each Member States are to be considered as data controllers for the purposes of application of the EU personal data protection legislation\(^{81}\) and therefore liable for compensation in the case of unlawful processing operation or other acts incompatible with the data protection legislation\(^{82}\).

Furthermore, a right was granted to each individual reportable person to be informed that data relating to him or her will be collected and transferred through mandatory automatic exchange of information, and about his / her rights under the legislation implementing Directive 95/46/EC, sufficiently in advance to allow him / her to exercise the said rights, in any case before the information is reported to the competent authority of its Member State of residence\(^{83}\). And each individual Reportable Person has to be notified in case of a breach of security with regard to his data when that breach is likely to adversely affect the protection of his personal data or privacy (data breach notification)\(^{84}\).

Finally, the information processed in accordance with Directive 2011/16/UE shall not be retained longer than necessary to achieve the involved tax purposes, and, under all circumstances, in accordance with each data controller's domestic rules on statute of limitations\(^{85}\).

With the entry into force of the GDPR on 25 May 2018, the applicable implementing provisions of the Data Protection Directive 95/46/EC will be replaced by the corresponding or complementary provisions of the GDPR\(^{86}\).

Directive 2011/16/EU also mentions some principles about the use of the data concerned for other, non-specified, purposes, regarding onward transfers of the data obtained to third countries, the use of that information by the


\(^{81}\) Art. 25(2) of Directive 2011/16/EU, introduced by Art. 1(5) of Directive 2014/107/EU

\(^{82}\) See Art. 23 of Data Protection Directive 95/46/EC and Art. 82 of GDPR (EU) 2016/679

\(^{83}\) Art. 25(3) of Directive 2011/16/EU, introduced by Art. 1(5) of Directive 2014/107/EU

\(^{84}\) Art. 21(2) of Directive 2011/16/EU, introduced by Art. 1(4) of Directive 2014/107/EU

\(^{85}\) Art. 25(3) of Directive 2011/16/EU, introduced by Art. 1(5) of Directive 2014/107/EU

\(^{86}\) Art. 94(2) GDPR
third country for other purposes\textsuperscript{87} and about the conditions under which the information received by a Member State from third countries may be forwarded to other Member States’ competent authorities\textsuperscript{88}.

**B. The ECJ Case Law**

Different cases brought before the Court of Justice of the European Union (ECJ) provide guidelines about the application of the EU data protection legislation that may have a certain impact of the conditions according to which the AEoI would be in line with the data protection requirements.

In the first place, the ECJ has examined the accordance with the data protection legislation of general personal data processing for the purposes of the investigation, detection and prosecution of serious crimes, in particular organized crime in the Digital Rights Case\textsuperscript{89}.

In this case, the ECJ was required to issue a preliminary ruling concerning the validity of Directive 2006/24/EC (Data Retention Directive\textsuperscript{90}), which introduced, for the said purposes, a general obligation for the provider of a publicly available electronic communications to retain all traffic data (but not the content of the communications), for a period of at least six months up to two years.

This case is relevant as far as the application of the proportionality principle in such circumstances is concerned. The ECJ noted that, however fundamental the objective pursued may be, it does not, in itself, justify such a retention...
being considered to be necessary for the purpose of that fight and that, considering the extent and seriousness of the interference with the right to privacy, the derogations and limitations to that right had to apply only in so far as is strictly necessary and with clear and precise rules imposing minimum safeguards, especially where personal data are subjected to automatic processing with a significant risk of unlawful access to those data. As a consequence, the Data Retention Directive was invalidated as being contrary to Articles 7 and 8 of the EU Charter of Human Rights for different reasons linked with the proportionality principle.

In a subsequent judgment, the ECJ added that such kind of legislation must contain clear and precise rules, in particular with regard to the circumstances and conditions under which data retention measures may be undertaken, and impose minimum safeguards for the persons concerned in order to mitigate the risk of misuse.

The PNR Case is also relevant as far as the scope of application of the Data Protection Directive is concerned, in order to distinguish processing concerning public security and the activities of the States in areas of criminal law, which fall outside the scope of the Data Protection Directive, even when the personal data is initially collected by private operators for commercial purposes, who arranged the transfer to the third country.

In the Smaranda Bara Case, the ECJ examined the rights of the data subjects to be informed and to state its position about a transfer of his personal

---

91 ECJ Case Digital Rights C-293/12 and C-594/12, § 48, 51-52 and 54-55
92 Idem, § 57-68. The reasons were in substance the following: the impugned measures were targeting all persons, even persons not indirectly in a situation which could give rise to criminal prosecutions and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception, for example to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime; no objective criterion was provided for to determine the limits of the access of the competent national authorities to the data and their subsequent use or the requirement of a prior review by a court or by an independent administrative authority; the data retention period rule did not provide for a distinction between the categories of data and the rules relating to the security and protection of data by the electronic communications services providers did not offer sufficient safeguards
93 ECJ Cases C-203/15 and C-698/15 of 21 December 2016, § 109
94 ECJ Case C-317/04 and 318/04 of 30 May 2006
95 According to Art. 3(2) of Data Protection Directive, see ECJ Case PNR C-317/04 and 318/04, § 54-59
96 See ECJ Case PNR C-317 and 318/04, § 54-59
97 ECJ Case C-201/14 of 16 October 2015
data, and the legality of a transmission from the tax authority to a social security administration of information concerning his declared income, although the national law only authorized the transmission of identification data, such as the name and address.

The ECJ ruled that, in the absence of a clear legal basis, or at least a publication of the agreement between the two authorities, on which the data transfer was based, the public authority sending this information had the obligation to inform the taxpayer about it. The authority receiving the data was also obliged to inform the data subject about the purposes of the processing of their data and the categories of data concerned.

As far as a transfer of personal data to a third country covered by an adequacy decision is concerned, the Schrems Case is relevant. In this case, the adequacy of the level of protection in the US within the so-called Safe Harbor program was challenged by a Facebook user residing in the EU, who was complaining regarding the fact that Facebook Ireland Ltd transferred his personal data to the US and kept it on servers located in that country, with the risk of surveillance activities engaged in there by the public authorities.

In the first place, the ECJ ruled that persons whose personal data have been or could be transferred to a third country covered by an adequacy decision are not prevented to lodge a claim with their national supervisory authorities. Then, the ECJ explains the conditions to be met by the third country to be considered as ensuring an « adequate » level of protection. Such country should ensure, by reason of its domestic law or its international commitments and through its practice, a level of protection of fundamental rights and freedoms essentially equivalent to that guaranteed within the EU.

In that respect, the content of the applicable rules resulting from domestic law or international commitments must be assessed, as well as the domestic

---

98 Idem, § 34 and 40-41
99 Idem, § 43-45
100 ECJ Case c-362/14 of 6 October 2015
103 ECJ Case C-362/14 of 6 October 2015, § 53-60
104 Idem, § 73-74
practice. Periodical controls should follow to check if the adequacy finding remains factually and legally justified, especially where new circumstances have arisen after the adoption of the decision.\textsuperscript{105}

The ECJ found out that the adequacy decision covering the US was based on a system of self-certification, which in itself was not contrary to the requirement of the Data Protection Directive, but which was not addressed to US public authorities, that were not required to comply with the safe harbour principles.\textsuperscript{106} Moreover, the data subjects had in fact no redress regarding their rights of access, rectification and erasure, which did not respect the essence of the fundamental right to effective judicial protection.\textsuperscript{107} As a result, the adequacy decision was declared invalid.

The question of the communication to a public Court of Audit and a large number of bodies subject to its control of the salaries and pensions exceeding a certain level paid to the employees of public institutions and pensioners together with the names of the recipients was examined by the ECJ in the \textit{Österreichischer Rundfunk Case}.\textsuperscript{108}

In a later case, the ECJ assessed the conditions under which the names and amounts received by EU agricultural funds beneficiaries may be published on a website with regard to the principle of proportionality and indicated that the legal persons could claim the protection of Articles 7 and 8 of the EU Charter of Fundamental Rights in so far the official title of the legal person identified one or more natural persons, although such legal persons are not granted a comparable level of protection.\textsuperscript{112}

Finally, in the \textit{Tietosuojavaltuutettu Case}, the ECJ examined, notably with regard to the derogations in favour of journalistic activities, the right to publish tax information concerning individuals on Internet for commercial purposes in Finland, where tax information about the taxpayers is accessible to the public, including the amount of income and wealth.\textsuperscript{114}

\textsuperscript{105} Idem, § 75-78
\textsuperscript{106} Idem, § 80-82
\textsuperscript{107} Idem, § 91-95
\textsuperscript{108} ECJ Cases C-465/00 and C-138/01 of 20 May 2003
\textsuperscript{109} ECJ Cases C-92/09 and C-93/09 of 9 November 2010
\textsuperscript{110} See, notably, § 86
\textsuperscript{111} Idem, § 52-53
\textsuperscript{112} See § 87-88
\textsuperscript{113} ECJ Case C-73/07 of 16 December 2008
\textsuperscript{114} See, notably, § 22-23 and 58-62
C. The Guidelines of the Article 29 Data Protection Working Party

The EU Article 29 Data Protection Working Party (WP29) is composed of representatives of data protection authorities of the EU to provide independent advice on data protection matters, with the authority to issue recommendations115. It has taken position on a certain number of issues regarding AEOI at the time of the introduction of the USA Foreign Account Tax Compliance Act (FATCA) and later, during the discussions about the implementation of the CRS AEOI and expressed concerns about the potential impacts on the individuals’ fundamental right to data protection116.

In particular, further to a Statement on automatic inter-state exchanges of personal data for tax purposes, issued on 4 February 2015117, the WP29 adopted the Guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes on 16 December 2015118.

According to the WP29, the following safeguards were notably required in the context of AEOI119: specific, clear, accessible and foreseeable legal basis; clear purpose limitations; clear, extensive and appropriate information of the data subject before the actual exchange takes place; explicit data retention period; strict security measures and explicit security standards120; clear limi-

---

115 Articles 29 and 30 of Directive 95/46/CE
118 WP29 Guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes of 16 December 2015, available at: http://www.dataprotection.ro/servlet/ViewDocument?id=1278
119 For a complete view of the safeguards recommended, see WP29 Guidelines, p. 3 ff
120 According to WP29, in appreciation of the high security standards regulated by the Directive 95/46/EC and with reference to the ECJ Case Law Digital Rights Ireland, it should be targeted to host the data in the territory of the EU, see WP29 Guidelines, p. 8
tations and safeguards relating to onward transfers; availability of legal redresses and supervision and enforcement mechanism\textsuperscript{121}.

The lawfulness of the Automatic Exchange of Financial Information according to the different legal instruments with regard to the principle of necessity and proportionality and with reference to the ECJ Case Digital Rights, was also questioned by the WP29\textsuperscript{122}.

III. Data Protection under the CRS Legal Framework

1. The Multilateral Convention on Mutual Administrative Assistance in Tax Matters

The Convention on Mutual Administrative Assistance in Tax Matters (The Multilateral Convention) was originally jointly developed by the OECD and the Council of Europe in 1988. It was amended by a protocol in 2010 following a call of the G20 countries during the 2009 London Summit, with the introduction, among others, of the AEoi\textsuperscript{123}. At the present time, 95 States signed the Multilateral Convention, including jurisdictions covered by territorial extensions\textsuperscript{124}.

Its main aim, as described in the preamble, is to fight tax avoidance and evasion, while taking into account the necessity of protecting the confidentiality of the information exchanged in accordance with the international legal instruments for the protection of privacy and flows of personal data.

Some of its provisions, and of the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information (MCAA), complementing it, aim at the protection personal data, mostly through the

\textsuperscript{121} Accordingly, the data protection safeguards to apply were to be considered in three different settings, whether the exchange of information takes place between EU Member States, with a jurisdiction covered by an adequacy decision or with other States. In this last case, it was crucial, according to WP29, to ensure that the receiving jurisdiction provides adequate protection to personal data through \textit{ad hoc} agreements with binding effects to be determined on a case-by-case basis, see WP29 Guidelines, p. 4 ff

\textsuperscript{122} See WP29 Guidelines, p. 6

\textsuperscript{123} See Art. 6 of the Multilateral Convention

\textsuperscript{124} See Annex
confidentiality principle, which is applicable to all types of information received under the Convention.\footnote{Revised Explanatory Report to the Multilateral Convention, Nr. 218, page 86}

Article 22 of the Multilateral Convention states that: « Any information obtained by a Party shall be treated as secret and protected in the same manner as information obtained under the domestic law of that Party and, to the extent needed, to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the supplying Party as required under its domestic law. ».

As a result, beside the confidentiality rules as per the Multilateral Convention and MCAA, the main mechanism to ensure the individuals’ rights to protection of their privacy is the possibility for the participating jurisdiction supplying the information to specify safeguards to the jurisdiction receiving the information in order to ensure that the latter will comply with data protection rules applicable according to its own domestic law or international commitments.\footnote{The Multilateral Convention explicitly refers to the protection of personal data, which is not the case of the OECD Double Tax Convention Models or of other exchange of information instruments}

To determine the content of the right to privacy within the different participating jurisdictions, it may be referred to the OECD Privacy Guidelines or to Convention 108.\footnote{Revised Explanatory Report to the Multilateral Convention, Nr. 216, p. 85} The safeguards that may be required by the jurisdiction supplying the information may be, for example, an individual right to access to personal data processed for the concerned taxpayer or independent data protection oversight or redress.\footnote{Revised Explanatory Report to the Multilateral Convention, Nr. 216, p. 86}

According to the confidentiality principle, the information received shall only be disclosed to persons and authorities concerned with the assessment, collection or recovery in relation to taxes in that jurisdiction, and shall only be used for tax purposes as a principle.\footnote{See art. 22(2) of the Multilateral Convention} In case of a violation of the confidentiality principle in the receiving jurisdiction, the requested State may suspend the assistance under the Convention.\footnote{See Section 7, § 3 MCAA}

Regarding the purpose limitation principle, the information received by a participating jurisdiction may be used for other purposes than tax purposes.
only if it is permitted by the laws of the supplying Party and if the competent authority of that Party authorizes such use, being recalled that, normally, legal instrument specially designed for other purposes should be used, such as the European Convention on Mutual Assistance in Criminal Matters.

Regarding onward transfers, only the authorization of the jurisdiction providing the information is required.

Article 21 of the Convention provides for other rules for the protection of persons very similar to the rules of Article 26 of the OECD Model Tax Convention.

Furthermore, limitations to the cooperation based on the principle of reciprocity are provided, notably when trade and business secret would be involved or when the disclosure of the information would be contrary to public policy.

2. The Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information (MCAA)

The MCAA is applicable as far as the AEoI according to Article 6 of the Multilateral Convention is concerned, but the jurisdictions that signed the Convention have also the possibility to conclude a specific agreement.

It specifies the information to be exchanged and a notification mechanism is provided for, according to which a competent authority shall notify the

---

131 Art. 22(4), first sentence of the Multilateral Convention
132 Revised Explanatory Report to the Multilateral Convention, Nr. 225, p.88
133 Art. 22(4), second sentence of the Multilateral Convention
134 See Art. 21(1) of the Multilateral Convention. The rights and safeguards secured to persons by the laws and administrative practise of the requested State shall notably not be affected by other provisions of the Convention
135 Revised Explanatory Report to the Multilateral Convention, Nr. 191, p. 78 - 79
136 When, for example, a request of information is motivated by political, racial or religious persecution or if the information constitutes a State secret, see Art. 21, § 2, let. b of the Multilateral Convention and p. 80 of its Revised Explanatory Report
137 See, for example, the Agreement between the Swiss Confederation and the European Union on automatic exchange of financial account information in order to improve the compliance with the tax obligations at the international level
138 See Section 2, § 2 of MCAA. The data to be exchanged is notably the name, address, tax identification number (TIN), date and place of birth, the account number, the account balance or value as of the end of the relevant time period and the total gross amount of inter-
other competent authority if it has reason to believe that an error may have led to incorrect or incomplete information reporting\textsuperscript{139}.

The confidentiality and data protection principles are provided for by Section 5 of the MCAA\textsuperscript{140}. According to it, all the information exchanged are subject to the confidentiality rules and safeguards provided for in the Multilateral Convention, but the supplying competent authority may require its extensive safeguards in order to ensure the necessary level of personal data protection that would be required under its domestic law. The required safeguards are to be listed in an annex to the agreement.

Beside the commentaries on the Multilateral Convention and MCAA, the OECD also issued a CRS implementation handbook and a guide about the confidentiality within the frame of exchange of information for tax purposes\textsuperscript{141}.

\textsuperscript{139} See Section 4 MCAA

\textsuperscript{140} See Section 5, § 1 MCAA. See also Section 7, § 1 MCAA. According to the OECD, the confidentiality of the taxpayer’s information has always been fundamental cornerstone of the tax systems needed to guarantee the trust in the international exchange of information procedures taking into account the often sensitive character of the financial information concerned. The respect of this principle is to be ensured by the applicable international legal instrument, that must be legally binding, the domestic legislation and practices. Systems and procedures are to be put in place are detailed and include information security management procedures, employees background checks, specific provisions on employment contracts, training for the tax administration employees involved, security measures to restrict the entry to the premises of the tax authority, etc, see Commentary on Section 5 MCAA and CRS, notably Nr. 1, p. 79 and Nr 11-37, p. 82-88

\textsuperscript{141} OECD guide “Keeping it safe”, which provides for a set of practical means and recommendations to help the tax administration to ensure the compliance with the confidentiality principle and the checking that should be made before the activation of the AEoI with another country, see, p. 10 ff and 29 ff
IV. The Taxpayers’ Rights

Different levels of international data protection standard apply throughout the jurisdictions committed to take part to the OECD / G20 AEoI\textsuperscript{142} and different schools of thought may conflict pertaining to the application of procedural rights within the framework of international administrative assistance, some States considering that such assistance is a mere preparatory fact-gathering process where no specific procedural rights should be granted, whereas other States consider it to be an independent administrative procedure with all the relevant procedural rights\textsuperscript{143}.

In the first place, we will determine to what extent the general data protection laws may apply within the framework of AEoI (hereafter, Chap. 1). Afterward, the taxpayers’ rights will be determined in order to identify a common and uniform minimum standard (hereafter, Chap. 2-10).

As we will see, when examining the rights of the taxpayers regarding the protection of their personal data, the question of the constitutionality of the AEoI arises, which was questioned by different scholars\textsuperscript{144} and it is not excluded, at the present stage, that the AEoI may be blocked or declared illegal by the competent jurisdictions.

In that respect, the main issues concern the legal basis, which is required to restrict the right to privacy, especially in the case of onward transfers and subsequent use of the data for other purposes (Chap. 2 and 8); the legitimacy, necessity and proportionality of the measure (Chap. 3) and the activation of AEoI without providing the required safeguards for the protection of the taxpayers’ financial data when the transfer is intended to take place with jurisdictions with a lower or inadequate level of personal data protection (Chap. 4).

\textsuperscript{142} See Annex
\textsuperscript{143} OBERSON X., Towards Automatic Exchange of Information, in SZW/RSDA 2/2015, p. 105
\textsuperscript{144} See, for example, in Switzerland, MATTEOTTI R., Verfassungskonformität des automatischen Infomationsaustauschs – Kurzgutachtung im Auftrag des Staatsekretariats für Internationale Finanzfragen, 13 August 2015, in http://biblio.parlement.ch and NAEF F. and E., N., Sur l’inconstitutionnalité de l’échange automatique de renseignements, in : Jusletter 7 December 2015. See also the Decision from the Belgian Constitutional Court of 8 March 2017 in the X. v. Tax Administration Case Nr. 32/2017 on the constitutionality of AEoI under the Belgium – US FATCA Model 1A Agreement and MICHEL B., Belgium and United States: Exchange of bank data held constitutional, News IBFD, 22 March 2017
The uniform standard and related taxpayers’ rights within the framework of the AEoI should, in our opinion, be in line with the standard of data protection as set out by the Council of Europe Convention 108, which principles seem to be shared by the majority of the participating jurisdictions and therefore appear to be legitimate\(^ {145}\), being recalled that, according to the Explanatory Report of the Multilateral Convention, the content of the right to privacy within the different participating jurisdictions may be determined by reference to the OECD Privacy Guidelines or to Convention 108 and its Additional Protocol of 8 November 2001\(^ {146}\).

1. **Applicable Rules**

The Multilateral Convention and the MCAA provide for specific provisions for the protection of the taxpayers’ privacy to be applicable to all automatic exchange of financial accounts information: the confidentiality of the information received by a jurisdiction\(^ {147}\) (including guidelines on the different procedures and practices to put in place\(^ {148}\) ); the limitation of the use of the information provided to tax purposes (purpose limitation), unless the legislation of the supplying State allows it and the supplying State gives its authorization\(^ {149}\); the requirement of the authorization of the supplying State in case of an onward transfer of the data to a third State\(^ {150}\) and limitations to the obligations to exchange information due to trade and business secrets being involved or public policy (ordre public)\(^ {151}\).

These rules, or the corresponding domestic provisions implementing or completing it, may be applied by the Courts as *lex specialis* prevailing on the general data protection legislation rules, according to the principle « *lex specialis derogat generali* ».

In our opinion, only the core rules of these international legal instruments about the confidentiality of the information exchanged may be interpreted as *lex specialis* that would prevail over the general data protection provisions to

---

\(^{145}\)See Annex

\(^{146}\)See Revised Explanatory Report to the Multilateral Convention, Nr. 216, p. 85

\(^{147}\)Art. 22 of the Multilateral Convention and Section 5 of the MCAA

\(^{148}\)See above, Title III, chap. 2.

\(^{149}\)Art. 22(4), first sentence of the Multilateral Convention

\(^{150}\)Ibidem, second sentence

\(^{151}\)Art. 21 of the Multilateral Convention
be applicable for the following reasons. In the first place, the reservation of Article 22 of the Multilateral Convention in favour of « specific safeguards [for the protection of personal data] which may be specified by the supplying Party as required under its domestic law» and Section 5 of the MCAA with its commentary, clearly indicate that the data protection legislation is to be, as a principle, fully applicable to the information processed within the frame of the AEoI. Furthermore, the AEoI is not to be considered as a legal field where the general laws and principles for the protection of personal data may not apply, such as the public security, defence or activities of the States in areas of criminal law.

Regarding the safeguards in the case of use of the information exchanged for purposes other than tax purposes and in the case of onward transfers to third countries, the mere authorization of the supplying State (or the accordance with its domestic legislation) appears not to be sufficiently precise and substantive to override, as lex specialis, the data protection applicable legislation, but should be considered as additional requirements to be complied with, unless the domestic law provides for specific data protection provisions to be applied within the AEoI.

2. Legal Basis

Article 17 of the UN Covenant on Civil and Political Rights prohibits unlawful interference in the individuals’ privacy and requires the States parties to

---

152 Even the rules of the Multilateral Convention and MCAA on the confidentiality are to be complemented by domestic legislation, which must include sufficient provisions, notably to provide for specific and limited circumstances under which the financial information concerned can be disclosed and used and impose sanctions in case of breach of the confidentiality requirement. See Commentary on MCAA and CRS, Commentary on Section 5, No. 10, p. 82. If these rules are not put in place, the general data protection provisions might apply to complement the confidentiality requirements as set out by the Multilateral Convention and the MCAA

153 The Multilateral Convention explicitly refers to the protection of personal data, which is not the case of the OECD Double Tax Convention Model or of other exchange of information instruments, see OECD guide “Keeping it safe”, Nr 1.3, p. 11

154 See Art. 8 § 2 ECHR; some of the reservations to Art. 3(2)(a) Convention 108; Art. 3(2) the EU Directive 95/46/EC and Art. 2(2) EU GDPR. See also above, Title I, chap. 4, let. B and ECJ Cases Digital Rights C-293/12 and C-594/12 and PNR C-317/04

155 The restrictions to the right to privacy must rely on clear, precise and sufficiently foreseeable legal basis according to Art. 8 § 2 ECHR, see, notably, ECtHR Cases Amann vs Switzerland, op. cit., § 56 ; M.N. and others vs San Marino, op. cit., § 72 and GSB vs Switzerland, op. cit., § 68
provide the legislative framework prohibiting such acts by natural or legal persons, including effective remedy against the responsible persons.\textsuperscript{156} The principle of lawfulness and fairness of the collection and treatment is reaffirmed in the UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files.\textsuperscript{157}

According to it, the precise circumstances under which such interferences may be permitted should be determined and exceptions to this principle expressly specified in the law or equivalent regulation, with limits and appropriate safeguards, and allowed only if necessary, among others, to protect national security or public order.\textsuperscript{158}

The requirement of lawfulness of the processing is also mentioned in the OECD Privacy Guidelines\textsuperscript{159} and Article 8 paragraph 2 of the ECHR requires an adequately accessible and with sufficient precision formulated legal basis for interferences to individuals rights to privacy, that should enable the individuals, if need with appropriate advice, to regulate their conduct.\textsuperscript{160} In particular, the law must indicate the scope of any powers conferred on the competent authorities and the manner of their exercise with sufficient clarity to give the individuals adequate protection against arbitrary interference.\textsuperscript{161} The storing of the data itself must be provided for by the law, with sufficient clarity about the scope and conditions, whatever the subsequent use of the stored information might be.\textsuperscript{162}

Accordingly, Convention 108 mentions the necessity of a legal basis for restrictions to the rights to personal data protection.\textsuperscript{163} The EU data protection legislation provides for the same principles.\textsuperscript{164}


\textsuperscript{157} Principle 1 UN Guidelines for the Regulation of Computerized Personal Data Files, adopted on 14 December 1990 through Resolution 45/95

\textsuperscript{158} See General Comment No. 16 of the Human Rights Comity of the UN, op. cit., paragraphs 2 and 8, and Principle 6 of the UN Guidelines, op. cit.

\textsuperscript{159} See, notably, Art. 7 and 10 OECD Privacy Guidelines,

\textsuperscript{160} See European Courts of Human Rights Cases M.N. and others vs San Marino, op. cit., § 72 and GSB vs Switzerland, op. cit., § 68

\textsuperscript{161} Case Amann vs Switzerland, 16.12.2000, Application Nr 27798/95, § 56; case GSB vs Switzerland, op. cit., § 68

\textsuperscript{162} Case Amann vs Switzerland, op. cit., § 65, 69, and 78-80

\textsuperscript{163} See Art. 9(2) of Convention 108, see also Art. 5(3) and 9(1) of Draft modernized Convention 108
In the case of the AEoI for tax purposes, the exchange and processing of the data is based on the Multilateral Convention. But, neither the latter, nor the MCAA, provide for specific restrictions to the data protection rights, such as the right to be informed or the access or ask for a rectification of the concerned data. Therefore, such restrictions have to be provided for by a formal domestic law, sufficiently precise and accessible to the data subjects and there must be rules about the conditions and holding period of the concerned data.

Within the EU, Directive 2011/16/EU on Administrative Cooperation in the Field of Taxation specifies that limitations to certain rights are to be determined by the Member States (right to be informed about the collection and treatment of personal data, of access, rectification, blockage and erasure and of publicizing of the processing operations), without further details\(^\text{165}\).

As a consequence, the legal basis principle requires a clear and precise legal provision within the AEoI for any restriction to the rights provided for by the data protection regulations. In addition, according to this principle, the conditions for a subsequent use of the data received or collected by a competent authority need to be clearly provided for by the law, as well as the conditions which would allow forwarding the data to another administrative body or another jurisdiction.

### 3. Legitimacy, Necessity and Proportionality of the Data Processing

Article 17 of the UN Covenant on Civil and Political Rights forbids arbitrary interference to the right to privacy, which also comprises unreasonable interferences in the particular circumstances, even if it is provided for under the

---

\(^{164}\) See Art. 5 and 7 Directive 95/46/EC, Art. 5(1)(a), 6 and 23(1) EU GDPR and, notably, ECJ case Smaranda Bara C-201/14 of 1 October 2015, § 34 and 40-45, according to which the transmission of financial data from the tax authority to a social security administration within the same jurisdiction, without a clear legal basis (or at least a publication of the agreement between the two authorities on which the data transfer was based), the supplying authority as well as the receiving one had the obligation to inform the taxpayer about it, including about the purposes of the transfer and processing and the categories of data concerned.

\(^{165}\) See Art. 25(1) of Directive 2011/16/EU
law. It is completed by Principle 1 of the UN Guidelines of 14 December 1990 for the regulation of Computerized Personal data Files, which provides for the fairness of the collection and treatment of personal data.

The OECD, through its privacy guidelines, states that the collection of personal data should be limited and obtained, where appropriate, with the knowledge of the data subject.

According to Article 8 ECHR, any interference by public authorities to the right to respect for private life, such as in the case of cross-border communication of personal bank data, should be necessary in a democratic society for other important interests, notably the economic well-being of the States. It follows that such interferences must not only be in accordance with the law, but also necessary (or proportionate) in order to reach legitimate aims.

Likewise, Council of Europe Convention 108 states that the personal data retained must be adequate, relevant and not excessive in relation to the purposes for which they are stored and the Draft of the modernized version of Convention 108 under discussion goes further by introducing the principle of « minimization of data », according to which the collection and the processing must be limited to the strict minimum necessary.

The ECJ case law provides for limitations of data transfer and processing by States or private persons when individuals financial and tax information are involved, as for example in the Smaranda Bara, Österreichischer

---


167 Art. 7 of OECD Privacy Guidelines

168 See case GSB vs Switzerland, op. cit., § 89 - 91


170 Art. 5 of the Convention 108


172 ECJ Case C-201/14 of 1 October 2015, see above, Title II, chap. 4, let. B
Rundfunk\textsuperscript{173} or Tietosuojaavaltuutettu\textsuperscript{174} Cases. According to this case law, the collection and process of the data must be fair and relevant for the legitimate aim pursued and, especially, reasonably balanced between the interference to the concerned individual’s right to privacy and other rights, on one hand, and the legitimate aim on the other hand.

ECJ Case Digital Rights\textsuperscript{175} is comparable when assessing the proportionality and constitutionality of general personal data processing for prevention and prosecution purposes, such as in the case of the AEoI, at least when a EU Member State is concerned. In this case, the ECJ invalidated the EU Data Retention Directive\textsuperscript{176} that introduced a general obligation for the providers of publicly available electronic communications means, including telephony, Internet access and e-mails, to retain all traffic data except the content of the communications, for a period of at least six months up to two years, in order to ensure that this data would be available for the investigation, detection and prosecution of serious crimes, as defined by the Member States, in particular organized crime and terrorism\textsuperscript{177}.

According to the ECJ, although the aim of the impugned measures was legitimate and necessary as the concerned data represented a valuable tool in the prevention of offences and the fight against crime, in particular organized crime\textsuperscript{178}, the retention of the data constituted a wide-ranging interference with the rights guaranteed by Articles 7 and 8 of the EU Charter of Fundamental Rights\textsuperscript{179}. Concerning the proportionality, the objective pursued did not, in itself, justify such a retention of data, recalling that the derogations and limitations to that right had to apply only in so far as is strictly necessary and with clear and precise rules imposing minimum safeguards, especially

\textsuperscript{173} ECJ Cases C-465/00 and C-138/01 of 20 May 2003, see above, Title II, chap. 4, let. B
\textsuperscript{174} ECJ Case C-73/07 of 16 December 2008, see above, Title II, chap. 4, let. B
\textsuperscript{175} ECJ Cases C-293/12 and C-594/12 of 28 April 2014. Concerning the relationship that this case law may have with the AEoI, see the Guidelines of Art. 29 Data Protection Working Party on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes of 16 December 2015, available at : ec.europa.eu/justice/data-protection/Article-29, p. 2-3 and note n°5
\textsuperscript{177} See ECJ Cases C-293/12 and C-594/12, § 41 and 51
\textsuperscript{178} Idem, § 42-44, 49
\textsuperscript{179} Idem, § 34, 35 and 37
where personal data are subjected to automatic processing with a significant risk of unlawful access to those data\textsuperscript{180}.

Within the framework of the AEoI, although the impugned measures concern financial data to which a lower level of protection may be granted, these measures are targeting without distinctions all persons as well, even persons not indirectly in a situation which could give rise to criminal prosecutions, and an important part of the concerned data, without limitations to a circle of particular persons likely to be involved, in one way or another, in serious crimes\textsuperscript{181}. Furthermore, nor objective criterion to determine the subsequent use of the data, neither requirements of a prior review by a court or by an independent administrative body in order to limit their subsequent use to what is strictly necessary are provided in both cases\textsuperscript{182}.

According to ECJ, objective criteria are to be chosen for such measures to establish a connection between the data to be retained and the objective pursued, with the view to circumscribe in practice the extent of the data retention measure and the public affected, general and indiscriminate retention of all data not being admissible\textsuperscript{183}. Moreover, the data concerned should be retained within the European Union\textsuperscript{184}.

A particular concern about the AEoI is that many personal details about the taxpayers are to be communicated, such as the name, address, date and place of birth, wealth and income\textsuperscript{185} and, when trusts or similar legal entities are involved, the names of the trustees, potential beneficiaries, settlers, and protectors, as well the name of other persons considering to be controlling persons may be transferred to multiple jurisdictions\textsuperscript{186}. In addition, it involves an important economical contribution from the private sectors, especially banks, due to the due diligence and reporting requirements.

On the other hand, the ability of the AEoI to contribute to reduce serious tax crimes is limited, especially when taking into account the amount of data that will have to be analysed and due to the loopholes that remain, although it clearly contributes to reduce tax avoidance risks.

\textsuperscript{180} \textit{Idem}, § 48, 51-52 and 54-55
\textsuperscript{181} \textit{Idem}, § 57-59. Compare with the
\textsuperscript{182} \textit{Idem}, § 60 and 62.
\textsuperscript{183} \textit{Idem}, § 110 and 112
\textsuperscript{184} \textit{Idem}, § 133
\textsuperscript{185} See Section 2, § 2 MCAA
\textsuperscript{186} See Section 2, § 2 MCAA and Section VIII, let. D, § 6 of the CRS
The purpose of the AEoI, combating tax fraud and improving tax compliance, which is linked with the financial interests of the States (or their economic well-being), although important, still remains vague and cannot as such be compared to fundamental security purposes, such as the fight against terrorism or organized crimes, as it was the case in the ECJ Digital Rights case. Therefore, it is to be expected that the Courts which will be examining the proportionality and constitutionality of the AEoI in a specific case will impose similar conditions as in that case law.

Nevertheless, the standard applicable to the Exchange of Information on Request (EoIR), which takes place in a very different context of specific investigation, cannot be applied as such. This being said, the level of data protection in specific cases may vary, especially when third persons not directly implied are concerned, and States are recognized to have a certain margin of appreciation.

In our view, one or more of the following amendments to the legal instruments on which the CRS model of AEoI is based would be required to make it compatible with the latest European constitutional and legal personal data protection provisions, with regard to the principle of proportionality:

- The limitation of the data exchanged to what is strictly necessary as the transmission of the data required without mentioning the name and personal data of the account holder, when a Tax Identification Number (TIN) is available;
- The introduction in all circumstances of a taxpayer’s right to be expressly informed and of a legal remedy to challenge the exchange of information before it effectively takes place, especially where the information is likely not to be relevant, for example when sending data about persons such as trustees or protectors or other controlling persons;

---

187 See BAKER / PISTONE, op. cit., p. 59 and 64, who notes that the introduction of the AEoI may mean that EoIR will in the future be used only in cases where the information is critical to an investigation, in which circumstances it might imply a higher level of protection of taxpayers’ rights.

188 See, notably, ECHR Cases GSB vs Switzerland, op. cit., § 93 and M.N. and others vs San Marino, op. cit.; see also OFFERMANS R., Switzerland, United States, Switzerland Federal Supreme Court: Swiss financial institutions may not disclose names of financial advisors who assisted US residents in setting up undisclosed Swiss bank accounts, IBFD Report, 7 October 2016.

• A de minimis rule, according to which the Reporting Financial Institutions are only obliged to conduct their due diligence and reporting duties for accounts exceeding a certain amount, such as it is the case with FATCA model of AEoI, with thresholds of USD 50’000 or USD 250’000\(^\text{190}\), as the lower amounts accounts imply less risks of intermediate or serious tax offences or

• The limitation of the reporting obligation of the Reporting Financial Institutions to cases where the client has not proved that the amounts concerned were duly declared to the competent tax authorities.

4. **Safeguards in case of Cross-Border Transfer of Personal Data**

At the time of signature of the MCAA or as soon as possible after the necessary laws are in place to implement the CRS, the competent authorities should have in place adequate measures to insure the required confidentiality and have specified the safeguards it may require, if any, for the protection of personal data sent to another participating jurisdiction\(^\text{191}\). On the other hand, as previously mentioned, specific data protection conditions apply to transfers of personal data to third countries (i.e. jurisdictions not sharing the same data protection standard or providing a comparable and sufficient level of data protection), which vary depending on the jurisdictions involved.

As a consequence, if the recipient State does not provide for a sufficient level of data protection, mostly through other binding and enforceable international commitments or its domestic law, as well as its practice\(^\text{192}\), specific safeguards for the protection of personal data have to be specified in the dedicated annex of the MCAA or another international binding agreement with the recipient jurisdiction on the basis of Article 22(1) of the Multilateral Convention including, as the case may be in the future, data protection re-

\(^{190}\) See Annex 1, Art. II(A) and III(A) of FATCA Model Intergovernmental Agreement

\(^{191}\) See Section 7, § 1 MCAA

\(^{192}\) See ECJ Case Schrems, *op. cit.*, § 73-74 and above, Title II, chap. 4, let. B. See also Art. 45(2) EU GDPR, which adds, as a condition, the existence and effective functioning of one or more independent supervisory authorities in the third country; Art. 2 of Additional Protocol to Convention 108; Art. 12(2-3) Draft of modernized Convention 108, which requires that the third State level of data protection is secured by the law of that State or international organization or *ad hoc* or standardized safeguards provided by legally binding and enforceable instruments and Art. 17 OECD Privacy Guidelines.
requirements to be respected by the Reporting Financial Institutions in the third country providing the information, such as a right to be informed of the intended transfer of banking personal data.\(^{193}\)

In our opinion, mere specifications imposed when sending the information to the competent authority of the receiving jurisdiction as « conditions » to be respected may appear not to be sufficient and legally binding for all the recipient State authorities.

Similarly, the specification of safeguards provided for in the dedicated Annex of the MCAA, according to Section 5, paragraph 1 of it, or in another similar applicable competent authorities agreement, would only apply to the other concerned competent authority and not to other parts of the recipient State administration, to which the data could be transferred according to Article 22(4) of the Multilateral Convention. A bilateral binding agreement between the States concerned would appear to be necessary.\(^{194}\)

The precise safeguards to be required from third jurisdictions are more extensive for EU Member States, especially with the introduction of the EU GDPR, which will enter into force in May 2018.\(^{195}\) Specific safeguards are also required to be put in place for countries of the Council of Europe in order to comply with the strict conditions of Article 8 ECHR for restrictions

\(^{193}\) The situation where the receiving State would impose data protection requirements to the competent authority of the supplying State for the information that it will receive (and which, per definition, concerns its own residents) is not considered in the Multilateral Convention, the MCAA or the CRS Documentation, but the wording of the Multilateral Convention and of the MCAA does not prevent a contracting State receiving data to specify data protection requirements to be respected within the supplying jurisdiction. Although it is not clear, up to the present day what the precise scope of application of the latest data protection instruments, such as GDPR or modernized version of Convention 108, will be, they are tending to be applicable to any processing of personal data concerning resident data subjects or consumers, wherever the processing takes place; it is therefore likely that it will apply to the Reporting Financial Institutions situated abroad processing personal data for the purpose of the AEoI, see, notably, Art. 3 and Recital 22 – 25 GDPR (EU) 2016/679 and Art. 3 of the Draft of modernized version of Convention 108 and n° 24 of its Draft Explanatory Report, p. 4, according to which « processing carried out by controllers in the private sector fall within the jurisdiction of a Party when they have sufficient connection within the territory of that Party ». In such situations, it might appear necessary for the receiving State to impose such requirements to the supplying State, through the international binding agreement if the level of data protection in the supplying State appears not to be sufficient.

\(^{194}\) See, in this respect, ECJ Case Schrems, op. cit., § 80 ff

\(^{195}\) See Articles 45 ff EU GDPR and see above, Title II, chap. 4, let. A/b
to the right to privacy\textsuperscript{196} and for jurisdictions which ratified Convention 108 and its additional protocol, as well as for the OECD Members providing information to countries not following the same principles or not providing other sufficient safeguards. Furthermore, contracting States to the UN Covenant on Civil and Political Rights should also, in our opinion, impose specific safeguards if activating the AEoI with a jurisdiction that did not ratify this covenant or otherwise ensures an acceptable level of data protection\textsuperscript{197}.

The core principles that any participating jurisdictions should share include the protection from disclosure of financial information (which is partly covered by the Multilateral Convention and MCAA confidentiality rules), the right to a fair trial, including a fair investigation and appeal rights, freedom from discriminatory or arbitrary tax laws or procedures and the respect of the rule of law in tax legislation and tax procedures\textsuperscript{198}.

Furthermore, as minimum data protection standard, at least the following safeguards are to imposed to jurisdictions not providing a comparable level of personal data protection: the right of the data subject to access and require a correction of the data received by the competent authority; a limitation of the data received holding period, that should not be longer than the statute of limitation for the assessment of the taxes concerned; an effective legal remedy in the case of an onward transfer of the data and independent data protection oversight or redress.

In our view, the requirement of the taxpayer to be informed by the Reporting Financial Institution of the data about them being collected and the intended transfer is also to be imposed to the other third jurisdictions, as well as the requirement that the taxpayer concerned is granted a right to access and to ask the Reporting Financial Institution (or the competent authority of the supplying State) for a rectification of the data which is intended to be transferred, before it is effectively sent, including a legal remedy to that effect\textsuperscript{199}.

\textsuperscript{196} See, notably, the conditions for the transfer of banking data in European Court of Human Rights Case GSB vs Switzerland, 22.03.2016, Application Nr. 28601/11. Regarding the applicability of the ECHR in extraterritorial contexts, see also BLUM N., The European Convention on Human Rights beyond the nation-state - The applicability of the ECHR in extraterritorial and inter-governmental contexts, Basel, 2015.

\textsuperscript{197} See Principle 8 of the UN Guidelines for the Regulation of Computerized data Files of 14 December 1990.

\textsuperscript{198} See BAKER P. / PISTONE P., op. cit., p. 22.

\textsuperscript{199} See, in that respect, regarding EoIR, OBERSON Xavier, Towards Automatic Exchange of Information, op. cit., p. 104, Nr 2.2 in fine.
The possibility for the taxpayer to check and ask for rectification of the data before it is sent to the other participating jurisdiction appears not only to be a data protection standard requirement, but also improves the accurateness of the data transferred with lower risks of errors.

This being said, the level of data protection requirements and applicable rules vary significantly depending on the jurisdictions involved and the contracting States concerned will have to determine the safeguards that should be imposed to the other participating jurisdictions on a case-by-case basis. Hereafter, a summary is provided as guidelines about the applicable rules within five situations that should be distinguished.

A. **AEoI between EU Member States**

The AEoI within the EU is ruled by Directive 2011/16/EU on Administrative Cooperation in the Field of Taxation as amended by Directive 2014/107/EU, which specifies that the national provisions about the protection of personal data implementing Directive 95/46/EC are applicable, but with limitations to certain rights to be determined by the Member States.

But specific rules on data protection are provided for: the right of the individual Reportable Persons to be informed about the collection and exchange of information and about their rights before the information is reported, a data breach notification mechanism and a maximum holding period.

The limitations about the use of the data for other purposes than tax purposes and about transfers to third parties are equivalent to the limitations imposed by the Multilateral Convention, but the Member States have to comply with their domestic legislation on personal data protection if the information is sent to third countries.

As a consequence, under the reservation of these rules, the EU data protection legislation is fully applicable to the AEoI between the Member States.

---

200 The Summary of minimum standard and best practices for taxpayers’ rights of the IFA 2015 General Report might be a useful tool to assess the level of data protection granted to the taxpayers, see BAKER P. / PISTONE P., op. cit., p. 74 ff; see also the example questionnaire to assess the level of confidentiality, Commentary on MCAA and CRS, Annex 4, p. 291-297, and the OECD check list before the activation of the AEoI, OECD guide “Keeping it safe”, p. 29 ff

201 See above, Title I, chap. 4, let. Alc, note Nr. 79 and Art. 25(1) of Directive 2011/16/EU

202 See above, Title I, chap. 4, let. Alc and Art. 25 (3-4) and 21(2) of Directive 2011/16/EU

203 See Art. 16 and 24 of Directive 2011/16/EU
and it is up to the Member States to determine precisely the restrictions to the data protection rights within the limits of Articles 7 and 8 of the EU Charter of Fundamental Rights. It should notably be clarified which will be the restrictions to the aforementioned rights that will apply.\textsuperscript{204}

**B. AEOI between EU Member States and ECHR or Convention 108 State Parties**

State Parties to the ECHR and Convention 108 share a common and adequate level of data protection due to these international commitments.

As a principle, according to Convention 108, the flow of personal data between the contracting Parties may not be restricted unless it would result in an illegal transfer to a non-contracting State through the intermediary of another State Party.\textsuperscript{205}

The transfer of personal data from EU Member States to ECHR or Convention 108 State Parties should be in principle admissible as well, as it is considered that the State Parties to Convention 108 offer an adequate level of data protection from the EU point of view (and vice versa), and generally therefore may benefit from an adequacy decision.

Hence, with the reservation of contracting States only to Convention 108 and not to its Additional Protocol or ECHR or States not benefitting from an adequacy decision from the EU, which gives rise to certain concerns regarding onward transfers to third countries,\textsuperscript{206} the EU and Council of Europe legal frameworks do not provide for specific restrictions to such transmission of personal data.

\textsuperscript{204} According to the legal basis principle, see above, chap. 2. If the restrictions to the data protection rights are not provided for by the EU legislation, a conflict between the restrictions under the domestic law and GDPR might occur in the future, in which case the latter should prevail, as per the principle of supremacy of EU law, see ECJ Case Costa v. Enel 6/64

\textsuperscript{205} Art. 12 of Convention 108

\textsuperscript{206} A distinction should be made between recipients State Parties to Convention 108 and ECHR (which implies an international enforcement mechanism) and State Parties only to Convention 108, and between State Parties to Convention 108 which ratified its additional protocol (which implies the requirement of data protection supervisory authorities and provide for limitations of transfer of personal data to third countries not ensuring an adequate level of data protection) and State Parties that did not, when assessing whether particular safeguards are to be provided for due to the level of data protection according to the international commitments of the other participating jurisdiction
C. **AEoI between EU Member States and Other States**

The AEoI with third countries is based on the specific agreements binding the concerned jurisdictions, mostly the Multilateral Convention and the MCAA. EU Directive 2011/16/EU is not meant to apply and does not provide for specific provisions in that case, being only applicable for AEoI between Member States\(^{207}\), under the reservation that the Member States must comply with their domestic legislation on personal data protection if the information is received from another Member State and then sent to third countries\(^{208}\).

As a result, the general data protection legislation is applicable regarding transfer on personal data to third countries\(^{209}\). According to it, personal data can in principle be sent to third countries benefitting from an adequacy decision (or ensuring an adequate level of personal data protection), being however recalled that, in such a case, the persons concerned are not prevented to lodge a claim with their national supervisory authorities against the communication of personal data concerning them and that the level of data protection in a jurisdiction covered by an adequacy decision is to be reassessed regularly\(^{210}\).

The transmission of information to jurisdictions not covered by an adequacy decision would be possible (except if the data subject gives its unambiguous consent) only in the presence of sufficient safeguards through binding agreements\(^{211}\).

---

\(^{207}\) See Art. 1(1) and, notably, Articles 25 (3-4) and 21(2) of Directive 2011/16/EU

\(^{208}\) See Art. 16 and 24 of Directive 2011/16/EU

\(^{209}\) *i. e.* Art. 25 and 26 of Data Protection Directive and Chapter 5 of GDPR

\(^{210}\) See above, ECJ Case Schrems, *op. cit.*, and above, Title I, chap. 4, let. B

\(^{211}\) See Art. 26(1)(a and d) and (2) of Directive 95/46/EC. We share the opinion expressed by the EU Data Protection WP29 according to which the exception for important public interest grounds is not applicable in the case of the AEoI, taking into account the derogatory character of this exception and, notably, the systematic and wide extent of the interference on the right to privacy in comparison with the public interest involved. Therefore, the transmission of personal data to jurisdictions not covered by an adequacy decision may only take place with the consent of the concerned data subject or with sufficient safeguards imposed to the receiving Party through binding agreements, see WP29 Guidelines, *op. cit.*, p. 5. See also, for more details, the conditions imposed by Art. 46 of EU GDPR for transfers subject to appropriate safeguards
D. AEoI between ECHR or Convention 108 State Parties and Other States

Only the Additional protocol to Convention 108 provide for specific safeguards in the case of communication of personal data to third countries. According to it, such transfer is not allowed if the third country in question does not ensure an adequate level of data protection for the intended transfer, but the domestic law may provide that such transfers take place for legitimate prevailing interests, such as important public interests, or if the competent authority of the other participating jurisdictions accepts the specific safeguards provided by the controller.212 The limitations to interferences to the right to privacy according to Article 8 ECHR might apply as well in the case of exchange of information with third countries213.

Under these reservations, the respective domestic data protection regulations are applicable in both States, as well as Article 17 of the UN Covenant on Civil and Political Rights, provided that one or both of the involved jurisdictions have ratified it.

The draft modernized Convention 108 only allows transfer of personal data to third countries if it offers an appropriate level of data protection through its laws, including international commitments, or if ad hoc or approved standardized safeguards are provided by legally binding and enforceable instruments214.

E. AEoI between Other Jurisdictions

If one or both of the involved jurisdictions have ratified it, Article 17 of the UN Covenant on Civil and Political Rights is in principle applicable to the AEoI. If not, and under the reservation of other international applicable data protection provisions215, the own domestic data protection regulations are applicable in each States.

212 Art. 2 of Additional Protocol to Convention 108
213 See, for example, ECtHR Case GSB vs Switzerland, op. cit.
214 Art. 12 of Draft modernized Convention 108
215 See, for example, Art. 14 of the UN International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families adopted by the UN General Assembly resolution 45/158 of 18 December 1990, which grants to migrant workers and members of their families similar rights as Art. 17 of the UN Covenant on Civil and Political Rights
Specific safeguards should be put in place for transfer of personal data from a jurisdiction that ratified the UN Covenant on Civil and Political Rights, due to these commitments, to jurisdictions which did not ratify it, except if the level of data protection in the recipient State appears to be comparable and acceptable due to the domestic legislation and practice\textsuperscript{216}.

5. **Data Security and Confidentiality**

Data security is definitely a significant challenge within the framework of the AEoI due to the amount of data exchanged, their sensitive character, the potential value it may have (as the concerned data may be used for identity theft, ransoming, political pressures, consumers profiling, etc.) and the risks of hacking associated with the conservation of data on servers and transfers of it through the Internet\textsuperscript{217}.

The standard of security to be complied with within the AEoI is firstly determined by the confidentiality requirements as provided for by the Multilateral Convention and MCAA or other similar agreements, in light of their commentaries. According to it, the information received by a Party shall be protected in the same manner as information obtained under the domestic law of that Party (and, to the extent needed to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the supplying Party) and only be disclosed to persons and authorities concerned with the assessment, collection or recovery in relation to taxes in that jurisdiction\textsuperscript{218}.

The method(s) for data transmission including encryption and the safeguards the participating jurisdictions may require, as well as the adequate measures to insure the required confidentiality are to be determined and put in place at least « as soon as possible after the necessary laws are in place to implement the CRS »\textsuperscript{219}. More precisely, the domestic legislation has to include sufficient provisions for ensuring the confidentiality of the information received, notably to provide for the specific circumstances under which the financial information concerned can be disclosed and used and significant penalties or

\textsuperscript{216} See Principle 9 of the UN Guidelines for the Regulation of Computerized Personal Data Files
\textsuperscript{217} See BAKER / PISTONE, op. cit., p. 59 – 60 and p. 30 - 31 for examples of tax data breaches of confidentiality
\textsuperscript{218} Art. 22 of the Multilateral Convention
\textsuperscript{219} See Section 7, § 1 MCAA
sanctions for improper disclosure or use of the taxpayers’ information are to be imposed\(^{220}\), which includes information security management procedures with a set of policies practices and procedures, including IT relating risks, that should not be just a technical issue, but also a management, cultural and organisational issue to cover all aspects relevant to protecting confidentiality (employees background checks and training, specific provisions on employment contracts, security guards and security checks to restrict the entry to the premises, secure storage units with limited access and combinations and keys, monitoring of the security means for information system, storage of the users’ identities and access, regular updates of the security assessments and of third parties providers of information systems, monitoring and sanctioning in the case of any breach of confidentiality)\(^{221}\).

The international data protection laws and recommendations\(^{222}\) also provides for measures to be taken for the protection of personal data being processed, notably Convention 108\(^{223}\).

The EU data protection legislation and case law require a high level of data security\(^{224}\), notably appropriate technical and organizational measures against unlawful forms of processing, including destruction, loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and the measures to be implemented should be in accordance to the state of the art and the cost of their implementation in order to ensure a level of security appropriate to the risks represented and the nature of the data\(^{225}\). Furthermore, if a sub-contractor is

\(^{220}\) Commentary on MCAA and CRS, Commentary on Section 5, Nr. 10, p. 82

\(^{221}\) Idem, Nr. 11 ff, p. 82-88

\(^{222}\) See, notably, Principle 6 and 7 of the UN Guidelines for the Regulation of Computerized Personal Data Files and Art. 11 OECD Privacy Guidelines

\(^{223}\) Convention 108 and the draft of its modernized version require appropriate security measures to be taken against accidental or unauthorized destruction or accidental loss, as well as against an unauthorized access, alteration or dissemination of personal data being processed, see Art. 7 of the Convention 108 and of the draft of its modernized version.

\(^{224}\) See, notably, ECJ case Digital Rights, op. cit., § 66-68

\(^{225}\) Art. 17(1) Directive 95/46/EC. This directive also provides that any person who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law, see Art. 16 Directive 95/46/EC. Also note that the adequacy of the data protection level of a third State, when assessing if a transfer of personal data to that State may take place, also depends on the security measures which are complied with in that country, see Art.25(1 – 2) Directive 95/46/EC. See also Art. 32 GDPR (EU) 2016/679, according to which the controllers and the processors of personal data ought to take the appropriate measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs, nature, scope, context and purposes
designated to process the data, it should provide sufficient guarantee, a contract or any other legal act must stipulate that the sub-contractor act only on instructions from the controller and the relevant data protection obligations shall also apply to it.\textsuperscript{226}

In the case of AEoI within the EU, Directive 2011/16/EU determines how the responsibility about the security of the data processed is to be shared between the Member States and the EU authorities.\textsuperscript{227}

It is understood that, within the AEoI, the receiving jurisdictions must ensure the confidentiality of the data received at least according to the level of standard provided for by the Multilateral Convention and MCAA and by following the OECD published recommendations and that, in the case of violation of the confidentiality principle, the supplying State may suspend the administrative assistance.\textsuperscript{228} Accordingly, the supplying jurisdiction is responsible for the confidentiality of the data it receives and processes before sending it abroad, as well as the Reporting Financial Institutions, that should also put in place the necessary measures according to the applicable legislation.

The main security issue concerns the transmission of the data between the two concerned competent authorities. The level of security required is high due to the amount and sensitive character of the data involved, the risks of data breach and consequent interference on the rights of the data subjects.

Among the methods of transmission proposed by the OECD (encrypted CD, through a secured platform or in encrypted attachments by e-mail), the most secured method would be a personal remittance of an encrypted CD or other data storage device between the heads of each competent authorities, which could be done during a yearly international conference between the directors of the competent authorities of the participating jurisdictions, or through highly secured registered or governmental mail services.

\textsuperscript{226} Art. 17(2-4) Directive 95/46/EC
\textsuperscript{227} See Art. 21(2) of Directive 2011/16/EU, introduced by Art. 1(4) of Directive 2014/107/EU : the EU Commission is responsible for the security of the common communication network (CCN network) used for the transmissions between competent authorities and the Member States for ensuring the security of their own system
\textsuperscript{228} See Section 7, § 3 MCAA
\textsuperscript{229} See OECD Guide on Confidentiality, p. 23
The transmission of the information through a secured platform raises the question of the place where this platform would be situated\textsuperscript{230}. And it does not seem to avoid the risk linked with any transmissions over a network and presents a potential risks to this regard\textsuperscript{231}. The transmission of the information through e-mails, even in encrypted attachments, might be problematic as it also gives raise to risks of unauthorized access depending on the emailing services security level and encryption methods.

6. **Right to be Informed and Data Breach Notification**

According to the reservation of Article 21 of the Multilateral Convention in favour of the rights and safeguards secured by the laws and administrative practice of the requested State, the participating jurisdictions are not prevented to provide that the taxpayer must be notified when he is subject to the administrative assistance\textsuperscript{232}, unless it would unduly prevent or delay effective administrative assistance and provided that some exceptions may apply\textsuperscript{233}.

On the other hand, the right of the data subjects to be informed about its data being processed or communicated (if applicable, through “a certain amount of publicity”\textsuperscript{234}), is foreseen by all the international legal data protection instruments according to the principle of legitimacy, although some exceptions (which must be provided for by an adequate legal basis and be justified

\textsuperscript{230} The ECJ recent case law requires that sensitive personal data about EU residents is retained within the European Union for security reasons, see ECJ Case Digital Rights C-203/15 and C-698/15, § 68

\textsuperscript{231} Some concerns about the choice of a private service provider subsidiary of a US company (submitted to the US Patriot Act obliging such providers to transmit information to some US authorities or agencies) have been raised in the press, see, notably, Neue Zürcher Zeitung, Forderung an Banken: “Vergütung muss an Leistung gekoppelt sein”, 20 May 2017, available at: https://nzzas.nzz.ch

\textsuperscript{232} See Revised Explanatory Report to the Multilateral Convention, Nr. 180, p. 75

\textsuperscript{233} This condition is mostly relevant in the case of EoIR, for example in case of information request of a very urgent nature or when the notification is likely to undermine the chance of success of an investigation, see Revised Explanatory Report to the Multilateral Convention, p. 76

\textsuperscript{234} See Principle 6 of the UN Guidelines
by a legitimate interest) may apply due to the circumstances and although the extent of the information to be received by the data subject may vary.

According to the EU Data Protection Directive, the data subjects have notably the right to be informed about data processing concerning them, its purposes, the recipients or the categories of recipients and of their access and rectification rights. In addition, they have the right to be informed about the duration of the holding and receive further information in case of transfer of personal data to third countries according to the EU GDPR and the Draft of the modernized version of Convention 108.

Furthermore, the EU GDPR grants the data subjects a specific right to be informed in the case of personal data breach likely to result in a high risk to their rights and freedoms of natural persons except if sufficient subsequent measures have been taken to reduce the risk for the data subjects or if it would involve disproportionate effort.

The ECJ attaches a significant importance to the right to be informed about the data processing and its subsequent use, in particular in the absence of a sufficient legal basis or accessible information.

Indeed, the right to be informed is closely linked with the right to be heard and is a prerequisite to allow the exercise of other rights, such as the right to ask for rectification of erroneous data or challenge the measure before a judicial authority.

As far as the AEoI within the EU is concerned, a right was expressly granted to each individual reportable person to be informed that data relating to them will be collected and transferred through AEoI, and about their rights under the legislation implementing Directive 95/46/EC in any case before the information is reported to the competent authority of its Member State of resi-


236 See Art. 7bis of the Draft of the modernized version of Convention 108 and Report of the consultative Committee, op. cit., p. 8-9; Art. 13(1)(f) and 14(1)(f) GDPR (EU) 2016/679.

237 See Art. 7bis of the Draft of the modernized version of Convention 108 and Report of the consultative Committee, op. cit., p. 8-9; Art. 13(1)(f) and 14(1)(f) GDPR (EU) 2016/679.

238 See Art. 33-34 GDPR (EU) 2016/679; see also Art. 7(2) of the Draft of the modernized version of Convention 108, which provides for a data breach notification, but only to the competent control authority.

239 See, notably, ECJ Case Digital Rights, C-293/12 and C-594/12, § 34, 35 and 37.

240 See ECJ Smaranda Bara, C-201/14, to be compared with ECJ Case Sabou, C-276/12 of 22 October 2013; see also ECJ Case Digital Rights, op. cit., § 42-44, 49.
Data Protection and AEoI

47

dence\textsuperscript{241}, as well as a notification to individual Reportable Persons in case of a breach of security with regard to their data when that breach is likely to adversely affect their privacy\textsuperscript{242}.

Although it would appear disproportionate to require each participating jurisdiction to notify the taxpayers in case of data breach at the present time, the right to be informed about the AEoI \textit{ex ante}, with sufficient time before the data is actually sent to the other jurisdiction, whether by the Reporting Financial Institutions or the supplying Competent Authority, appears to be a minimum standard to be followed by all of them, which should allow the data subjects to exercise their other data protection rights, such as the right to ask for rectification of erroneous data\textsuperscript{243}.

7. \textbf{Right of Access, Rectification, Erasure and Blockage}

The commentary on Section 5 MCAA makes it clear that further data protection rights may apply within the frame of the AEoI, such as the right to access, correction, redress and existence of an oversight mechanism.

The international data protection standards provide for the right of the data subjects to have the holding of their personal data be regulated by law, to ascertain in intelligent form whether and what personal data is processed in automatic data files and for what purposes and to request modification or elimination when data have been collected or processed contrary to the provisions of the law or if the files contain incorrect personal data\textsuperscript{244}.

Within the EU, Article 8 of the European Charter of Fundamental Rights grants to everyone the right of access to data which has been collected concerning them, and the right to have it rectified. Furthermore, the data subjects have the right to obtain a notification to third parties to whom the data have been disclosed of any of such rectification (or of erasure or blocking),

\begin{flushright}
\footnotesize\textsuperscript{241} Art. 25(3) of Directive 2011/16/EU \\
\footnotesize\textsuperscript{242} Art. 21(2) of Directive 2011/16/EU \\
\footnotesize\textsuperscript{243} See, in that respect, BAKER / PISTONE, \textit{op. cit.}, p. 64, ECtHR Case Klass and others vs Federal Republic of Germany, \textit{op. cit.}, § 57 \\
\footnotesize\textsuperscript{244} With the right to have a legal remedy in case of refusal according to Convention 108 and EU legislation, see, notably, General Comment No. 16 of the Human Rights Comity of the U.N., \textit{op. cit.}, § 10 ; Principle 4 of the UN Guidelines ; Art. 13 OECD Privacy Guidelines ; Art. 8 Convention 108, Art. 12 Directive 95/46/EC and Art. 15 and 16 GDPR 2016/679
\end{flushright}
unless this proves impossible or involves a disproportionate effort. In addition, a right to object at any time to the processing of the data, on compelling legitimate grounds relating to their particular situation, is granted to the data subjects by the EU data protection legislation.

As far as the AEoI within the EU is concerned, these rights have been granted to the data subjects, with some limitations to be defined by the Member States. We do not see any justified ground to limit these rights in the context of the AEoI, but the legislation should determine at which stage they may be exercised with appropriate delays so that the effective assistance is not delayed.

8. Safeguards regarding Subsequent Use and Onward Transfers

Regarding the purpose limitation principle, the information received by a participating jurisdiction may be used for other purposes than tax purposes only if it is permitted by the laws of the supplying Party and if the competent authority of that Party authorizes such use. Regarding onward transfers of the data received, only the authorization of the jurisdiction providing the information is required.

This vagueness about the conditions for subsequent use of the data exchanged raises a lot of concerns relating to the protection of individuals personal data, which have to be tackled by the participating jurisdictions. In particular, the data subjects have the right to know where and to whom personal data concerning them will be stored and disclosed and for which purpose it will be used, according to the purpose limitation principle. There is a risk that the data will be held for many years in the jurisdictions with a low

245 See Art. 12 Directive 95/46/EC and Art. 19 GDPR
246 See Art. 14 Directive 95/46/EC and Art. 21 GDPR; see also Art. 8(1)(d) of the Draft of modernized Convention 108 and Art. 18 GDPR (right to restriction of processing)
247 See Art. 25 of Directive 2011/16/EU
248 Art. 22(4), first sentence of the Multilateral Convention; the other purposes for which the information received may be used are notably the combat against money laundering, corruption or terrorism financing, i.e. certain high priority matters, see Revised Explanatory Report to the Multilateral Convention, Nr. 225, p. 88
249 Art. 22(4), second sentence of Art. 22 of the Multilateral Convention
250 See notably WP29 Guidelines, p. 3 and 8; OBERSON, Towards Automatic Exchange of Information, op. cit., p. 107
data protection standard, in opposition to the principle of minimization of data processing, and used for unintended purposes.

In our view, an adequate additional safeguard to this regard would the requirement of the deletion of the data when the purpose for which it was held is reached \(i.e\.\) the tax assessment with a maximum data retention period to be imposed to the receiving State \(\text{with appropriate exceptions}\). Furthermore, the authorization from the supplying competent authority should be subject to a judicial review.

Clear limitations and safeguards relating to onward transfers to third countries taking place after the initial exchange also need to be provided for. It should, first of all, only take place, according to the conditions of EoIR, Spontaneous Exchange of Information \(\text{(SEoI)}\) or Mutual Assistance in Criminal Matters\(^251\), as per the applicable rules of both the supplying and receiving States, with appropriate legal remedies.

9. **Legal Remedy**

The individuals claiming that their right to privacy has been violated by the State authorities must have an effective remedy, notably to exercise their rights of access, rectification and erasure, and impartial, independent and technically competent supervising authorities for the protection of this right are required by all the international relevant legal instruments, which may sometimes issue appealable decisions\(^252\).

Article 13 of the ECHR provides for the right to have « an effective legal remedy before a national authority » in the case of interference to the right to privacy\(^253\).

Within the EU, Article 47 of the Charter of Fundamental Rights is more extensive since it guarantees the right to an effective remedy before a

---

\(^{251}\) See PISTONE / BAKER, op. cit., p. 55 and 59

\(^{252}\) See, among others, Art. 2(3)(a) UN Covenant, Principle 8 UN Guidelines; Art. 13 and § 2 and 61 of its comment; Art. 10 Convention 108; Art. 8(f and g), 10, 12bis Draft of modernized version of Convention 108

\(^{253}\) But not necessarily to a judicial authority, see KUIJER M., Effective remedies as a fundamental right, in: Seminar on Human Rights and Access to Justice in the EU, Barcelona, 2014, p. 5; BREUER M., EMRK Kommentar, Art. 13, BECK C.H., München, 2012 (also concerning the relationship between Art. 6 and 13 ECHR). Art. 6 ECHR is in principle not applicable in the field of taxation, see OBERSON, Towards Automatic Exchange of Information, op. cit., p. 103
Likewise, the data protection legislation grants the right to a judicial remedy for any breach of the data protection rights guaranteed. According to the case law, such safeguard is notably to be provided for to fulfill the data subjects’ rights of access, rectification and erasure in the third country where the data is being sent.

Within the frame of the AEoI, the right to have a legal redress before at least an administrative superior authority, which goes together with the right to be informed, of access and of rectification of the data being gathered and transmitted, appears to be a minimum standard.

10. Right to Compensation

For the time being, a legal right to claim for compensation for the damage suffered in case of violation of the right to privacy is only provided for by the European legislation, although the other international data protection instruments state that appropriate sanctions are to be imposed, respectively that the data controllers (and possibly their subcontractors) should be accountable for complying with the right to privacy.

Within the EU, an express right to get a compensation from the controller is granted for the damage suffered in the case of unlawful processing operations, except if the controller proves that he is not responsible for the event giving rise to the damage, in which case it may be exempted from its liability, in whole or in part. EU GDPR provides for the right to receive compensation from the controller or the processor. Claims for compensation can be raised before the courts of the Member State where the controller or processor has an establishment or, unless the controller or processor is a public

---

254 See also ECJ Cases Johnston 222/84 and Heylens C-97/91
255 See Art. 22 EU Directive 95/46/EC, see also Art. 77 – 80 GDPR (EU) 2016/679. See however ECJ Case Sabou, op. cit., § 38 - 44
256 See, in that respect, ECJ Case Schrems, op. cit., § 88 - 90
257 See also EU WP29 Guidelines, p. 3, about the need of legal redresses within the frame of the AEoI
258 See, notably, Principle 8 UN Guidelines; Art. 14 OECD Guidelines and § 62 of its comment and Art. 10 Convention 108. See also Art. 10 of the Draft of modernized version of Convention 108 and § 97 in fine of its draft explanatory report, according to which financial compensation for material and non-material damages caused by the processing could be considered too. Usually administrative fines apply as sanctions
259 Art. 23 Directive 95/46/EC
authority of a Member State, before the courts of the Member State where the data subject has his or her habitual residence\textsuperscript{260}.

Within the framework of the AEoI in the EU, it is to be considered that both the Reporting Financial Institutions and the competent authorities of each Member States are to be considered as data controllers\textsuperscript{261} and therefore liable for compensation in the case of unlawful processing operation or other acts incompatible with the data protection legislation. But the EU Commission is also responsible for ensuring the security of the common communication network (CCN network)\textsuperscript{262}.

V. Conclusion

The need to protect the individuals’ personal data has increased during the last years with the turn into the Digital Era and the emergence of the « Big Data ». The right to data protection has notably been raised to the constitutional level with its introduction in the Charter of European Fundamental Rights.

Meanwhile, with the economic globalisation and recent financial crises (as well as revelations of large scale tax frauds), the political need of reinforced international administrative cooperation has increased as well, especially in the tax matters.

The AEoI appears to be a legal field where the tension between this call to share more information between State authorities and the requirements of limitation of the processing of personal data is exacerbated, as it was the case with other general prevention or « surveillance » measures, notably against terrorism, as it transpires from the ECJ Cases PNR or Digital Rights.

In the field of taxation, there is another tension, which varies significantly from one country to another, between the demand for financial transparency and the right to keep the information about the individuals’ income and wealth confidential.

\textsuperscript{260} See Art. 82(6) cum 79(2) GDPR (EU) 2016/679
\textsuperscript{261} Art. 25(2) of Directive 2011/16/EU, introduced by Art. 1(5) of Directive 2014/107/EU
\textsuperscript{262} See Art. 21(2) of Directive 2011/16/EU, introduced by Art. 1(4) of Directive 2014/107/EU
On the international level, the standard of data protection within the participating jurisdictions to the AEoI is very different according to their international commitments. Almost all of these jurisdictions have ratified the UN Covenant on Civil and Political Rights, which appears to be a minimum standard. Around half of them have ratified Convention 108 of the Council of Europe, which is intended to have a universal scope and which represents an adequate level of data protection at the present day. But some contracting States to the Multilateral Convention did not ratify any of these international instruments.

The mechanism to ensure data protection requirements within the AEoI appears simple: the confidentiality of the data sent is as a principle protected and the supplying State should specify the additional data protection requisites it would have to the recipient authority. If the latter does not comply with it, the supplying State may suspend the AEoI.

However, a lot of questions remain unanswered from the data protection legislation perspective and it might be a matter for the courts to decide, if the appropriate legislation and safeguards are not provided for, with a risk of negative court decisions.

A little attention has been brought so far to the taxpayers’ rights within the frame of the AEoI. Data protection and an enhanced cooperation between authorities must go hand in hand.

The main data protection issues to be considered within the frame of the AEoI that were approached in this thesis are the following:

- The presence of an adequate legal basis for the restrictions to the rights to personal data protection;

- The proportionality and necessity of the AEoI, due to the wide extent content of the data to be exchanged and the absence of a de minimis rule or other rules to exclude from data processing the low amounts accounts with low risks of tax avoidance or the fact that the identification information exchanged is not limited to the tax identification number (TIN) if such a number is available;

- The safeguards to be imposed for the data sent to third countries without a comparable level of data protection and the examination of the level of data protection in that third country before the AEoI
is activated, which is to be carefully assessed on a case-by-case basis;

- The rights of the taxpayers to be pre-informed of the data collection and exchange and to exercise their rights to access and ask for a rectification of the data before it is sent to the third country, with appropriate legal remedies;

- The conditions to allow onward transfers of these data by the recipient State, that should comply with the conditions of spontaneous or on request exchange of information in the supplying and in the receiving jurisdictions, and the use of it for subsequent non intended purposes. Both should be subject to a prior legal review in the supplying State in the absence of sufficient safeguards or data protection level in the recipient State;

- The level of security to be provided for the exchange of data and the consequences in case of data breaches, such as administrative sanctions, as well as the rights of the taxpayers to be informed about it and to claim for a compensation from the responsible data processor.
Annex: Level of Personal Data Protection among contracting States to the Multilateral Convention on Mutual Administrative Assistance in Tax Matters

<table>
<thead>
<tr>
<th>Signatories of the Multilateral Convention as of 8 January 2018 (and territorial extensions)</th>
<th>Ratification of UN Convention on Civil and Political Rights</th>
<th>OECD Members (Privacy Guidelines)</th>
<th>Ratification of ECHR</th>
<th>Ratification of Council of Europe Convention 108</th>
<th>Ratification of Additional Protocol to Convention 108</th>
<th>Benefiting from an EU Adequacy Decision</th>
<th>EU Member States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albania</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Andorra</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Argentina</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Austria</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>n. a.</td>
<td></td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bahamas</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bahrain</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Barbados</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Belgium</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>n. a.</td>
<td></td>
</tr>
<tr>
<td>Belize</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brunei Darussalam</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulgaria</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>n. a.</td>
<td></td>
</tr>
<tr>
<td>Burkina Faso</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cameroon</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chile</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>China</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Colombia</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cook Islands</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Costa Rica</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Croatia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>n. a.</td>
<td></td>
</tr>
<tr>
<td>Cyprus</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>n. a.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Czech Republic</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>n. a.</td>
<td></td>
</tr>
<tr>
<td>Denmark (incl. Faroe Islands and Greenland)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>(Faroe Islands)</td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>------</td>
<td>---</td>
</tr>
<tr>
<td>El Salvador</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Estonia</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Finland</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>France</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Gabon</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Georgia</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Germany</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Ghana</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greece</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Guatemala</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hungary</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Iceland</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>India</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indonesia</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ireland</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Israel</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Italy</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Jamaica</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kenya</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Korea</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kuwait</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Latvia</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Lebanon</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liechtenstein</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Lithuania</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Luxembourgh</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Malaysia</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malta</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Marshall Islands</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mauritius</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mexico</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moldova</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monaco</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Morroco</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nauru</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netherlands (incl.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>n. a.</td>
<td>✔</td>
</tr>
<tr>
<td>Aruba, Curacao and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sint Maarten)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Zealand</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nigeria</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Niue</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Norway</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pakistan</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Panama</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peru</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Philippines</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poland</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portugal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qatar</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Romania</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Russia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saint Kitts And Nevis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saint Lucia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saint Vincent and the Grenadines</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Samoa</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>San Marino</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Senegal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seychelles</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Singapore</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slovak Republic</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slovenia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>South Africa</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sweden</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switzerland</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunisia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Turkey</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uganda</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ukraine</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>United Kingdom (incl. Anguilla, BVI, Cayman Islands, Gibraltar, Guernsey, Isle of Main, Jersey, Montserrat and Turks &amp; Caicos Islands) ✓ ✓ ✓ ✓ (Jersey, Guernsey and Isle of Main) ✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United States</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uruguay</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VI. Bibliography

ALTENBURGER P. R., Der internationale Informationsaustausch in Steuersachen (direkte Steuern), Zürich Dike, 2015


BELSER E. M. / EPINEY A. / WALDMANN B, Datenschutzrecht - Grundlagen und öffentliches Recht, Bern, 2011

BESSON S., Droit international public, Abrégé de cours et résumés de jurisprudence, Bern, 2011


COUDRAY L., La protection des données personnelles dans l’Union européenne - Naissance et consécration d’un droit fondamental, Sarrebruck, 2010


EPINEY A. / NUESCH D (ed), Big Data und Datenschutzrecht / Big Data et droit de la protection des données, Zürich, 2016

EPINEY A. / NUESCH D (ed), Die Revision des Datenschutzes in Europa und die Schweiz / La révision de la protection des données en Europe et la Suisse, Zürich, 2013


MEIER F., Protection des données - Fondements, principes généraux et droit privé, Bern, 2010


NAEF F. and E. N., Sur l’inconstitutionnalité de l’échange automatique de renseignements, in: Jusletter 7 December 2015
OFFERMANS R., Switzerland, United States, Switzerland Federal Supreme Court: Swiss financial institutions may not disclose names of financial advisors who assisted US residents in setting up undisclosed Swiss bank accounts, IBFD Report, 7 October 2016


RAPPO A. / TILLE A., Les conditions d’assistance administrative internationale en matière fiscale selon la LAAF, in: RDAF 2013 II 1

RENUCCI J.F., Droit européen des droits de l’homme - Droits et libertés fondamentaux garantis par la CEDH, 7th ed., Issy-les-Moulineaux, 2017


SCHELLER S., Manuale sullo scambio di informazioni in materia fiscale, Manno, 2015


THIELE C., Das Recht auf einen wirksamen Rechtsbehelf in vergleichender europäischer Perspektive (Art. 47 GRC, Art. 6 und 13 EMRK), Berlin / Heidelberg, 2015


WINIGER M., Der automatische Informationsaustausch in Steuersachen : Grundlagen, Funktionsweise, Würdigung, Basel, 2017

### VII. Table of abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEoI</td>
<td>Automatic international exchange of financial information for tax purposes</td>
</tr>
<tr>
<td>CRS</td>
<td>Common Reporting Standard</td>
</tr>
<tr>
<td>ECJ</td>
<td>Court of Justice of the European Union (European Court of Justice)</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights of 4 November 1950</td>
</tr>
<tr>
<td>EctHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>EoIR</td>
<td>International Exchange of information on request for tax purposes</td>
</tr>
<tr>
<td>FATCA</td>
<td>Foreign Account Tax Compliance Act</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>GDPR</td>
<td>Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (The General Data Protection Regulation – GDPR)</td>
</tr>
<tr>
<td>IFA</td>
<td>International Fiscal Association</td>
</tr>
<tr>
<td>MCAA</td>
<td>Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>SEoI</td>
<td>Spontaneous international Exchange of Financial Information for tax purposes</td>
</tr>
<tr>
<td>TIN</td>
<td>Tax identification number</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>WP29</td>
<td>Article 29 Data Protection Working Party</td>
</tr>
</tbody>
</table>