ARTICLE 29 Data Protection Working Party

175/16/EN
WP 234

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

Adopted on 16 December 2015

Background

The purpose of these Guidelines is to ensure compliance with data protection requirements in the context of the automatic exchange, between competent authorities of different countries, of personal data for tax purposes.

The data protection authorities of the European Union, which are represented in the Article 29 Working Party (WP29), are examining the new trends at European and international level, including the introduction of mechanisms for the automatic cross-border exchange of personal data for tax purposes and their impact on privacy and data protection.

In the last few years, the need to fight against tax evasion led governments to engage in the creation of information exchange tools.

In the United States the "Foreign Account Tax Compliance Act" (FATCA) was enacted with the aim to combat tax evasion by US tax residents using foreign accounts.

On 15 July 2014, the OECD Council approved the "Standard for Automatic Exchange of Financial Account Information – Common Reporting Standard" ("CRS"), including common due diligence procedures to be used by financial institutions to identify reportable accounts.

At European level, Directive 2011/16/EU was adopted, and subsequently amended by Council Directive 2014/107/EU, in order to ensure a comprehensive Union-wide approach to the automatic exchange of information for anti-tax evasion purposes. It substantially incorporates the OECD´s CRS in the EU legal framework.

In the last few years, the WP29 has dealt with the impact of automatic exchange of information on the right to the protection of personal data in the following documents:

- Two letters, respectively adopted on 21st June 2012[1] and on 1st October 2012[2], concerning FATCA
- Letter on OECD´s CRS adopted on 18 September 2014[3].

More recently, on 4 February 2015[4], the WP29 adopted a "*Statement on automatic inter-state exchanges of personal data for tax purposes*", to draw the attention of national governments and EU Institutions on the need that such exchanges should meet data protection requirements set forth by EU law, with particular regard to the principles of necessity and proportionality and taking into due regards the effects of the European Court of Justice´s judgment of 8 April 2014[5] which declared Directive 2006/24/EC (the "Data Retention Directive") invalid on the ground

[1] See:http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120621_letter_to_taxud_fatca_en.pdf

[2] See:http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121001_letter_to_taxud_fatca_en.pdf

[3] The letter is available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140918_letter_on_oecd_common_reporting_standard.pdf.pdf, whereas the Annex at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140918_annex_oecd_common_reporting_standard.pdf.pdf

[4] The Statement is available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp230_en.pdf

[5] Cases C-293/12 and C-594/12, *Digital Rights Ireland, Seitlinger a.o.*, published on http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

that European Union legislators had exceeded the limits of proportionality in forging the Directive.

As announced in the said Statement, the WP29 - also further to a request by the European Commission- intends to provide additional guidance so that the bilateral/multilateral agreements and/or national laws implementing the legal framework on administrative cooperation in the field of taxation (in application of either Directive 2011/16 or OECD´s CRS or replicating FATCA) can afford additional and consistent safeguards in terms of data protection.

To that end, the WP29 considers an important preliminary step to take stock of the availability of the existing legal frameworks, detect the current data protection gaps and/or major differences in the instruments at national level. Therefore, the WP29 has prepared a questionnaire, sent by each data protection authority to national tax authorities (see the Annex), aiming at assessing the level of implementation of data protection principles, as foreseen by Directive 95/46/EC, in the context of bilateral/multilateral agreements between countries which provide for the automatic exchange of information for tax purposes. The answers received to the questionnaire reveal interesting aspects of the process leading to international cooperation against tax evasion. The replies indicate that Member States are agreeing to some sort of cooperation scheme (either through direct bilateral agreement with the USA, implementing FATCA, or by signing the *Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information* or both*)*. They also indicate that such initiatives take place under parliamentary scrutiny and with consultation of the data protection authorities. Nonetheless, some critical points emerge, concerning the actual implementation of data protection safeguards in the context of tax cooperation. Some examples relate to the fact that the data subjects are not always informed *ex ante* that their personal data will be used or transferred abroad for the purpose of countering tax evasion. In addition, we see that exchanged data may be used for different purposes, as long as secondary use is in compliance with the laws of the transmitting country (thus severely undermining the principle of adequate or equivalent protection for personal data enshrined in Directive 95/46).

Having also in mind the said answers to the questionnaire, these guidelines aim at providing indications as to the data protection safeguards[6] to apply in three different settings: (i) exchange

[6] These safeguards are related to the respect for the rights of individuals to privacy and data protection, as enshrined in the Charter of fundamental Rights of the European Union (Articles 7 and 8) and to the EU data protection legal framework rules. The legal framework governing the processing of personal data in the EU currently consists of four major instruments:
Directive 95/46/EC or the Data Protection Directive, is the central piece of legislation on the protection of personal data in Europe. It sets down general rules on the lawfulness of personal data processing and on the rights of the individuals whose data are processed (data subjects), and requires each Member State to ensure that there is an independent supervisory authority responsible for monitoring implementation of the directive.
Regulation (EC) No 45/2001 covers processing of personal data by EU institutions and bodies and establishes the EDPS as an independent supervisory authority.
Directive 2002/58/EC concerns personal data processing in the electronic communications sector and sets rules of specific relevance including confidentiality, billing and traffic data, and rules on unsolicited commercial communications.
Council Framework Decision 2008/977/JHA addresses police and judicial cooperation in criminal matters and includes rules applicable to exchanges of personal data, including national and EU databases and transmissions to competent authorities and to private parties for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

At international level, the legal framework governing the processing of personal data consists of two major instruments:

of personal data between EU Member States; (ii) exchange of personal data between an EU Member State and a third country which has been the subject of an adequacy decision by the EU Commission, and (iii) exchange of personal data between a EU Member State and a third country which has not been the subject of an adequacy decision by the EU Commission. Following a number of safeguards that should be always included in the context of the automatic exchange, between competent authorities of different countries, of personal data for tax purposes.

1. Exchange of data between EU Member States

In this case, personal data (*e.g.* financial information identifying a natural person) are systematically transferred on a regular basis from the financial institution of an EU Member State to the financial institution of another Member State. Both Member States will have in place national rules implementing Directive 95/46/EC (the "Directive").

In order to make the personal data exchange lawful it is necessary that the exchange complies with such national rules. In addition the data controller in charge of processing the data applies all data protection safeguards provided by the Directive and its national implementing legislation.

The safeguards that will most commonly apply are, among others, the necessity and proportionality of the data exchange, the correct information of the data subject as to the information which is being transferred and the purposes of the exchange, the right of access and rectification, the supervision of the competent national DPA, the availability of legal redress to the data subject and so on, as better explained in paragraph 3, below.

It is also possible, that personal financial data are exchanged between competent authorities within the same Member State for the purpose of ensuring compliance with the tax legislation. Such a possibility has been the subject of a recent judgment of the ECJ in the *Bara*[7] case. In its ruling, the Court has clarified that "*the requirement of fair processing of personal data laid down in Article 6 of Directive 95/46 requires a public administrative body to inform the data subjects of the transfer of those data to another public administrative body for the purpose of their processing by the latter in its capacity as recipient of those data*". In addition, the Court has clarified that the rights of the data subject may be restricted for certain purposes, including tax reasons, but the restriction shall be provided by law, not being sufficient a mere administrative cooperation agreement between the authorities concerned.[8] The principles of law elaborated by the Court also apply, *mutatis mutandis*, to international exchange of personal financial information.

2. Exchange of data between an EU Member State and a third country covered by an adequacy decision

In this case, personal data are systematically transferred on a regular basis to a non- EU country which is covered by a Commission decision finding that the country in question provides adequate protection to personal data pursuant to Article 25 of the Directive ("Adequacy

The Convention 108 refers to the Convention for the Protection of Individuals with regard to automatic processing of personal data which was adopted by the Council of Europe in 1981. This Convention is the first legally binding international instrument adopted in the field of data protection.
The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (as updated in 2013) apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties.

[7] See ECJ judgment of 1 October 2015, in Case C-201/14, *Smaranda Bara and Others*.

[8] See Bara, para. 40.

Decision"). In this case, personal data may be transferred to the receiving country, provided that the safeguards cited in the Adequacy Decision are applied under the responsibility of the proceeding tax authority. In this respect, as recently established by EU jurisprudence,[9] it is for the national data protection authority to supervise and, where necessary, intervene by opening an investigation, if they have elements to determine that the data protection safeguards implemented by the third country are not or no longer adequate.

According to the said judgment, any adequacy decision must fully respect the criteria provided in article 25. The Court underlined that even a sectorial decision, such as the Safe Harbor decision, requires an in-depth, continuous analysis of the third country domestic laws and international commitments.

The principles of law elaborated by the Court in this case also apply, *mutatis mutandis*, to international exchange of personal financial information.

3. Exchange of data between an EU Member State and a third country NOT covered by an adequacy decision

In this case, personal data are systematically transferred on a regular basis to a non-EU country which is NOT covered by a Commission´s Adequacy Decision. It is crucial, therefore, to ensure that the receiving country provides adequate protection to personal data, through the adoption of an *ad hoc* agreement with binding safeguards. In consideration of the comprehensive and systematic nature of the data transfer concerned, the exceptions provided for in Article 26 (1,d) of the Directive 95/46/CE cannot be applied.

Therefore, the Article 7 (e) of the said Directive can be the only legal basis. In this case, the criteria for making the data transfer legitimate is that *"the processing is necessary for the performance of a task carried out in the public interest (...)",* such as the tax evasion.

Below, we discuss a number of safeguards that should be always included where there is a legislative legal basis assisting the exchange of personal data.

These recommendations, however, do not represent an exhaustive list of the safeguards, whose implementation would be, in itself, sufficient to comply with the Directive. As the Directive itself clarifies in Article 25(2), the assessment of which safeguards should be included shall be made on a *case-by-case* basis, after assessing the context of the data exchange, the data protection rules already in place in the receiving country and the risks potentially involved in the exchange.

4. Safeguards that should be always included in the context of the automatic exchange of personal data for tax purposes

Legal basis

The exchange of personal data shall be regulated by a clear legal basis, whether a legislative act or an international agreement. It is essential that any law or agreement is accessible by citizens and foreseeable in its application, in accordance with the requirements of Article 8 ECHR. Such instruments shall contain substantive provisions that implement (and not just merely refer to) the Directive and/or the national data protection law that implement it. It is also important that national procedures, providing for the involvement of respective Parliaments -and eventually

[9] See ECJ judgment of 6 October 2015, in Case C-362/14, *Schrems v Data Protection Commissioner.*

DPAs -are fully respected in order to create a democratic, clear and foreseeable legal basis.

Purpose limitation

In accordance with Article 6 of the Directive, any international agreement should clearly identify the purposes for which data are collected and validly used. The wording on the purpose ("tax evasion"/"improvement of tax compliance") for example may appear vague and insufficiently clear, allowing too much flexibility to the competent authority. It is not clear whether such purposes include, for example, legal acts of tax evasion, illegal acts of tax evasion or (serious) financial crimes.

Citizens shall be always aware of the exact purpose behind the processing of their data and such purpose shall be used as a parameter for assessing the necessity and proportionality (and thus the legality) of the data exchange.

Necessity and proportionality

Necessity and proportionality of data processing have been a main focus of the European Court of Justice´s judgment in the *Digital Rights Ireland* case (see above).

While that case focused on the necessity and proportionality of certain anti-terrorism measures, the WP29 is of the opinion that the balancing exercise mandated by the ECJ ruling applies to any public policies developed (including policies on tax cooperation) which have an impact on personal data protection rights. Therefore, in the tax cooperation agreements, it is necessary to demonstrably prove the necessity of the foreseen data exchange and that the required data are the minimum necessary for attaining the stated purpose.[10]

As a consequence, tax cooperation agreements should include provisions and criteria that explicitly link information exchange and, in particular, the reporting of personal data concerning financial accounts to possible tax evasion and that exempt low-risk accounts from reporting. In this respect, such criteria should be applicable *ex ante* to determine which accounts (and which information) would need to be reported.

In this context, also the use of electronic due diligence mechanisms, if not limited in its application, might lead to disproportional processing of personal data. Considering that electronic search may have a significant impact on personal data, we suggest to clearly identify -in the provisions of a cooperation agreement- the circumstances that might require an electronic search to be performed and the purposes such search aims at (*e.g.* determining the residence of an account holder).

Data retention

Proportionality should also guide data retention. The WP29 reiterates that as a consequence of the ECJ jurisprudence, national data retention laws and practices should ensure that any decision to retain personal data is subject to appropriate differentiation, limitations or exceptions, and clearly indicate where the data are stored. The Court also highlighted that data retained outside EU, would prevent the full exercise of the control, explicitly required by Article 8(3) of the Charter, by an independent authority, an essential component of the protection of individuals

[10] See WP's Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf

with regard to the processing of personal data.[11]

The indication of an explicit retention period for the personal data collected and exchanged ensures that data are retained for the time strictly necessary to pursue legitimate policy goals and, once this is achieved, they are deleted, restoring in full individual rights. Should this not be the case, the massive and continuous exchange of tax information concerning citizens would result in a large archive difficult to control and potentially harmful to the citizens.

Tax cooperation agreements, therefore, should clearly indicate for how much time tax information should be retained, in order to counter tax evasion. They shall also explicitly provide for the deletion of such information once the retention period has expired.

Transparency, fair processing and data subject´s rights

Clear and appropriate information should place data subjects in a position to understand what is happening to their personal data and how to exercise their rights, as foreseen by Articles 10 and 11 of the Directive. Any restriction or exemption to those provisions (or to any data subject´s right) shall be limited and duly justified and respect the strict criteria set forth in Article 13 of the Directive. Also, it has to be prescribed by law, as indicated by the mentioned *Bara* jurisprudence.

Controllership

Data controllers (and possible data processors) should be clearly identified in the data exchange agreement. A correct allocation of controllership is indeed a crucial step in order to ensure accountability of the entities processing personal data. As a consequence, it will be easier to ensure compliance with the data protection principles and the data subjects will be facilitated in the exercise of their rights.[12]

Onward transfers

Data controllers involved in the data exchange should be informed and adopt safeguards in relation to possible onward transfers of data taking place after the initial exchange of data. In particular, they shall ensure that the data are not used for general crime prosecution, without appropriate safeguards. Information concerning onward transfers shall be available also to the competent supervisory authority and to the data subjects, so that rights of redress and access may be enforced more easily.

Security measures

The cross-border exchange of personal data may result in an exponential increase of the risks inherent in the processing of personal data in relation to the amount of information collected. Strict security measures shall be adopted, in particular, to avoid accidental or unlawful destruction or any unauthorized disclosure or access and against any other unlawful form of processing as set forth by Article 17 of the Directive.

[11] See ECJ judgment of 8 April 2014, In Joined Cases C‑293/12 and C‑594/12, *Digital Rights Ireland*, para 68.

[12] (See WP's Opinion 1/2010 -WP1692 -which outlines the concept of "data controller", its interaction with the notion of "data processor", and the implications in respect of allocation of responsibilities; the Opinion is available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf)

In the light of the new framework emerging within the Proposed General Data Protection Regulation,[13] the WP29 emphasises the importance of the introduction of data breach notifications to the data subjects concerned and to the data protection authorities of the transferring country.

In consideration of the delicate nature of tax information (they can reveal valuable aspects of the life and activities of citizens), tax cooperation agreements shall explicitly set forth the security standards to be complied with by the authorities engaging in systemic data exchange.

As the Court stated (see above in data retention paragraph), in appreciation of the high security standards regulated by the Directive 95/46/EC, it should be targeted to host the server processing these data in the territory of the EU (or use the System of the Commission processing data under Directive 2014/107/EU amending Directive 2011/16/EU).

Merging technology and data protection and designing a privacy-compliant system from the outset -rather than applying data protection rules *ex post*- is an example of *privacy-by-design* approach suitable to improving the level of data protection.

Privacy Impact Assessment

Each Member State should consider implementing an agreed Privacy Impact Assessment aiming to ensure that the data protection safeguards are adequately addressed and a consistent standard is applied for the tax cooperation agreements by all EU countries.[14]

Processing of tax information for additional purposes

Personal data may be processed only for an explicit, specific and legitimate purpose. Further processing for additional purposes may only take place if such purposes are compatible with the original purpose (Article 6 of the Directive). It is therefore necessary to specify the purpose of the processing and adopt rules that limit the circulation of the data and prevent use for secondary purposes.

The information exchanged, including personal data, shall be disclosed on a "need-to-know" basis only to persons and authorities concerned with the assessment, collection or recovery of, the enforcement or prosecution in respect of, or the determination of appeals in relation to taxes of that jurisdiction, or the oversight of the above. Only the persons or authorities mentioned above may use the information and then only for purposes spelled out in the preceding sentence.

To the contrary, the information exchanged should not be used for additional, incompatible purposes -not even when this is possible under the laws of the supplying jurisdiction and there is the authorization of the competent authority of such jurisdiction. The problem, in this respect, is not so much that alternative uses are possible in the supplying jurisdiction as the fact that, in application of this provision, alternative uses become possible in the receiving jurisdiction, in a way which is potentially harmful to individual rights. Such purpose elasticity restricts the individual rights to protection of personal data, as the purpose for data processing should be specified, explicit and legitimate and disclosed *ex ante* to the data subject.

[13] See the proposed General Data Protection Regulation, document COM/2012/011 final - 2012/0011 (COD).

14 See the Annex to the Art. 29 WP´s letter of 18.09.2014 on the OECD Common Reporting Standard: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140918_annex_oecd_common_reporting_standard.pdf.pdf

Exchange of personal data and rights of the data subject

Tax cooperation agreements should specify that the data subject shall be informed on data exchanges with a reasonable delay before the actual exchange of the data takes place (so that the individual concerned gets time to defend himself if relevant). The information provided should at the minimum inform the data subjects of the fact that their personal data will be sent to a competent authority for the purpose of fighting tax evasion, include a list of the category of data sent, a list of the receiving authorities in various countries and the contact of the controller in their country of residence and inform them of their right to object and their right of redress.

Miscellaneous clauses

In drafting a tax cooperation agreement, based on exchange of personal data, the parties should also consider the introduction of supervision and enforcement mechanisms, including the following:

- a third party beneficiary clause (to enable the data subject to enforce any breach of the data controller and recipient's obligations);
- clarification of the controller and recipient's obligations (*e.g.* requirement to respond to enquiries, provide a copy of the clauses to the data subject, submission to reviewing, auditing, etc.);
- a liability clause;
- clarification of governing law;
- power of the competent data protection authority to block or suspend the exchanges.

If not already provided by applicable data protection laws in force in the receiving Member States, other commitments on supervision and enforcement need to be adopted involving both the controller and the recipient, such as:

- direct verification by authorities (*e.g.* joint inspections, audits by independent bodies, etc.) or by the controller (*e.g.* audits);
- the obligation to designate an independent data protection officer;
- independent investigation of complaints (designation of contact points for enquiries);
- dissuasive sanctions, appropriate redress and compliance with Court decisions;
- an accountability clause (obligation to provide evidence of compliance to the competent data protection authority, either upon request or at regular intervals);
- transparency of the safeguards (e.g. publication of the instruments on the internet);
- termination of the agreement, arrangement, etc. in case of breach.

To conclude, considering that the drafting of specific clauses can be very complex, we recommend that competent tax authorities negotiating tax cooperation agreements with other countries consult national data protection authorities[15] in order to ensure a coherent application of the data protection safeguards mentioned in the preceding paragraphs.

[15] The contact details for data protection authorities are available at: http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm

ANNEX

Questionnaire to national tax authorities on automatic exchange of data for tax purposes

Please note that the following questions refer to existing bilateral/multilateral agreements providing for the automatic exchange of information for tax purposes. However, where possible, we would appreciate an answer also in respect of possible current negotiations for future agreements.

1. FATCA and other international tools - Status of international agreements in your country and cooperation with financial institutions and insurance companies

1.1. Did your tax authority sign a (bilateral or multilateral) agreement with the Government of the United States of America under the Foreign Account Tax Compliance Act (FATCA), or with any other authority outside of the EU on the automatic exchange of information for tax purposes?

1.2. If yes, can you provide us with a list of such authorities and a copy of the agreements?

1.3 If yes, is this agreement, or at least are its provisions on the automatic transfer of information binding on both your authority as well as the receiving authority, in particular as for the enforceability of data subjects' rights in the receiving country?

1.4. If not, what is the current state of negotiation of any agreements for the automatic transfer of information?

1.5. Could you explain to what an extent your authority has cooperated with the local representatives of the financial institutions and insurance companies that are subject to the international laws on automatic exchange of information for tax purposes?

1.6. In this context, were any (public) agreements or arrangements made with the private sector, and to what extent was this discussion reflected in your national law?

2. OECD Common Reporting Standard

2.1. The OECD Common Reporting Standard (CRS) sets forth due diligence standards for financial institutions to identify the "reportable accounts", and provides for a "Model Competent Authority Agreement" that may be used by states to exchange information for tax purposes. Does your national legal framework provide/intend to provide for the implementation of automatic exchange of information for tax purposes as foreseen by CRS?

2.2. If yes, can you provide us with a copy of the agreement?

2.3. Does your authority (intend to) use the Model Competent Authority Agreement as a basis for exchanging data?

2.4. If so, what is the definition given by your legal framework of "low risk accounts" to be excluded from data collection?

3. EU tools for administrative cooperation in the field of taxation (Directive 2011/16/EU and Directive 2014/107/EU)

3.1. Did your country implement Directive 2011/16/EU on administrative cooperation in the field of taxation?

3.2. Directive 2011/16/EU on administrative cooperation in the field of taxation was recently amended by Directive 2014/107/EU. When and how is the implementation of this Directive planned?

4. Aim of EU harmonisation

4.1. Do you plan or would you welcome any actions of harmonisation vis-à-vis the approaches in other Member States at EU level?

4.2. If so, how could/should such EU-level harmonisation be achieved in your view in terms of data protection?

a. Guidance by WP29 on the data protection content of the EU Legal framework and/or bilateral tax agreements

b. Application of the procedure envisaged in Article 218 of the EU Treaty (Commission submits recommendation to Council to open negotiation with consultation of WP 29). What are your views on further amendments of EU law, for instance by adding substantive data protection clauses? If so, are there any articles in the EU legal framework on automatic transfer of information for tax purposes that require clarification?

c. Adoption of the new Data Protection Regulation in 2015

d. Informal approach: Practical discussion with representatives of the WP29 and the European Commission on the impact of EU case law[16] on the content of such arrangements and the required minimum data protection content of international tax agreements to reduce the risk of negative court decisions.

5. Availability of data protection safeguards

As also stated by the WP29 in the Annex to the letter adopted on 18 September (see the Explanatory Note above), there are several data protection principles – as also interpreted by the EU Court of Justice in the data retention case[17] - to be taken into account by governments and competent institutions to make sure that the automatic exchange of information for tax purposes is carried out while ensuring the respect for data protection obligations under Directive 95/46/EC.
In this regard, what are the measures that are currently concluded or proposed (or developed

[16] For instance: impact of the Decision of the Grand Chamber of the Court of Justice on the "Data retention Directive": Cases C-293/12 and C-594/12, Digital Rights Ireland, Seitlinger a.o., published on http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ02937. As recalled in the Explanatory Note to this questionnaire, the ECJ Decision declared Directive 2006/24/EC (the "Data Retention Directive") invalid on the ground that European Union legislators had exceeded the limits of proportionality in forging the Directive.

[17] See previous footnote.

in the negotiations) in order to ensure data protection in accordance with national and EU law? Please answer by referring in particular to the following principles:

5.1. Availability of data protection safeguards - DPIA

5.1.1. Is a Data Protection Impact Assessment (DPIA) or a formal consultation of the national DPA being envisaged and at which stage?

5.1.2. Did you perform a Data Protection Impact Assessment during the negotiations of international agreements by:

a. contacting your national DPA for further information

b. your own assessment (please explain what guidance you used such as internal guidance by in-house or external counsel - e.g. law office -, public opinion or other means. Thank you also for providing us with a copy or summary of the content of this guidance to be able to check at least the summary of the data protection impact assessment.

c. other (please explain)

5.2. Availability of data protection safeguards - Legal basis in national law

5.2.1. Are bilateral or multilateral agreements, such as Tax Treaties, concluded for the purpose of exchange of information subject to formal ratification procedure by your national Parliament?

5.2.2. Did your country adopt a national law that provides for the possibility of automatic transfer of personal data for tax evasion purposes to third countries?

5.2.3. If so, can you give us the references of such law and specify which instruments at international level are transposed?

5.2.4. If not, have you prepared a first draft of a legal basis for the automatic transfer? Has your national data protection authority been involved in the process? If not, at which stage of the process do you plan to involve it? Is there any timeframe for the legislation process? When do you plan the law to enter in force?

5.3. Availability of data protection safeguards - Data to be exchanged

5.3.1. For each individual, does the collection of data regards only the total of the owned amounts at a certain date, or does it also cover each movement on the account?

5.3.2. What data are collected (current accounts; deposit accounts; credit cards; shareholdings; personal property and real estate, etc.) and what are the criteria to identify the data to be collected?

5.3.3. Does your national authority create a database of (and thereby duplicate) the collected data?

5.3.4. Does your national law contain provisions relating to:

a. identification of scope (data to be exchanged)

b. data quality (i.e. principles of proportionality, data minimization, data accuracy, maximum data retention period, etc. - *Content regarding these principles is further elaborated below*).

5.4. Availability of data protection safeguards - Proportionality[18]

5.4.1. How are parties prevented from engaging in "fishing expeditions" or requesting information that is unlikely to be relevant to the tax affairs of a given person or ascertainable group or category of persons?[19]

5.4.2. How is automatic exchange of information carried out in practice? Please describe what technique is applied, and what it means in practice (are there any previous filtering mechanisms in place for data exchange, or which unique identifiers are used?, etc.).

5.4.3. What is your assessment on the necessity of the automatic transfer of information for tax evasion purposes?

5.4.4. Are bilateral automatic exchange mechanisms fully in place with all counterparties in foreign jurisdictions? I.e. Do you automatically receive for all countries the data related to your own data subjects[20]?

5.5. Availability of data protection safeguards - Data retention

5.5.1. Does your legislation provide for a specific data retention period? If so, please specify the minimum and the maximum retention periods.

5.5.2. How long do you store data received from institutions, insurance companies, etc.? How long do you store data you automatically receive from other countries, also participating in the automatic exchange?

5.5.3. Is there a procedure for the deletion or correction of obsolete or incorrect data?

5.6. Availability of data protection safeguards - Data Controller

5.6.1. What decisions does/did your authority take as for the forwarding of the data for tax evasion purposes?

---

[18] Based on the ECJ decision invalidating the Data Retention Directive (see the previous footnote), in order not to violate the proportionality principle, it is necessary to demonstrably prove that the planned processing is necessary and that the required data are the minimum necessary for attaining the stated purpose and thus avoid an indiscriminate, massive collection and transfer.

[19] Comments on article 4 of the Convention of 25 January 1988 of the OCDE and the Council of Europe on Mutual Administrative Assistance in Tax Matters, published on http://www.conventions.coe.int/Treaty/EN/Reports/Html/127-Revised.htm#article4

[20] Data subjects that are subject to the tax laws of your country while they have economic activities or receive income outside of your country.

5.6.2. In particular: Does your authority (intend to) provide "data warehousing" services for the automatic transfer of information to foreign counterparts? I.e. To what an extent does your authority store data forwarded by national institutions (banks, insurance companies, etc.) where such institutions are subject to foreign legislations on automatic transfer of information for tax purposes (e.g. FATCA or others)?

5.6.3. In particular: Does your authority (intend to) provide «data warehousing» services for data you automatically receive from other countries? If yes, please describe how these data are further processed.

5.6.4. In that case, does your authority accept full responsibility as a "data controller"[21] under Directive 95/46/EC vis-à-vis the data subjects?

5.6.5. If not, do you consider that (only) institutions or other parties are data controllers under the terms of EU Directive 95/46/EC? Why?

5.7. Availability of data protection safeguards - Transparency / Obligation to inform and reciprocity vis-à-vis your own data subjects

5.7.1. Are all your national laws and international arrangements related to the automatic transfer of personal data published? Please provide us with a list.

5.7.2. Do you require that foreign authorities inform the data subjects that are subjects of the tax laws of your country of the fact that their data is processed for tax evasion purposes?

5.7.3. If not, do you inform data subjects yourself upon reception of the information from foreign counterparts?

5.7.4. If not, what is the reason for non-application of the obligation to inform the data subjects that are subject to your own tax laws?

5.8. Availability of data protection safeguards - Purpose definition and limitation

5.8.1. Is there a clear-cut definition of "tax infringement" according to the national tax system?

5.8.2. If not, why not?

5.8.3. Does your law on automatic exchange of information provide for a clear limitation on the use of the exchanged information for tax purposes only? I.e. is the use of the exchanged information for other than tax purposes excluded (money laundering, corruption, financing of terrorism, etc.)? Are the conditions for eventual other purposes provided for? If so, which ones?

5.8.4. If not, is sufficient attention given in your national law to other legal instruments which are already available at EU or national level and should be considered in case of use of information for criminal matters? I.e. does your national law take into account the possibility

[21] See Article 2.d of Directive 95/46/EC.

to exchange information on criminal tax matters based on bilateral or multilateral treaties[22] on mutual legal assistance (to the extent they also apply to tax crimes), as well as on domestic legislation regulating the granting of such assistance[23]?

5.8.5. Does this purpose limitation safeguard apply also to the onward transfers from the receiving authority to third authorities?

5.9. Availability of data protection safeguards - Rights of data subjects

5.9.1. Does your national law provide for direct rights of access, rectification and right to object under articles 12-14 of Directive 95/46/EC vis-à-vis your authority? If so, please describe this procedure.

5.9.2. Are there limitations on/exceptions to the data subject's rights? If so, for what reason and what are the safeguards for the application of an exception? In particular, does your law (intend to) provide restrictions on the scope of the obligations and rights provided for in Article 10, Article 11(1), Articles 12 and 21 of Directive 95/46/EC, as foreseen by Article 25 of Directive 2011/16/EU?

5.9.3. Does your national law provide for direct rights of access, rectification and right to object under articles 12-14 of Directive 95/46/EC vis-à-vis the financial institutions, insurance companies, etc.?

5.10. Availability of data protection safeguards - Data security[24]

5.10.1. What security measures are (or are expected to be) in place? Please describe them briefly.

5.10.2. What kind of control (preventive and/or ex post) is carried out in order to ensure the correct adoption of security measures?

5.10.3. Please describe the technical parameters for any measures of encryption/integrity/traceability of exchanges that are in place to safeguard the transfer and storage of personal data.

---

[22] See a.o. the European Convention of 20 April 1959 on mutual assistance in criminal matters, published on http://www.conventions.coe.int/Treaty/en/Treaties/Html/030.htm

[23] See comment on article 1 § 1 of the Convention of 25 January 1988 of the OCDE and the Council of Europe on Mutual Administrative Assistance in Tax Matters, published on http://www.conventions.coe.int/Treaty/EN/Reports/Html/127-Revised.htm#article4, and the bilateral agreement on mutual legal assistance between the European Union and the United States of America of 25 June 2003, L181, 19 July 2003, p. 34.

[24] The potential implications of the technical options that might be chosen in order to implement automatic exchange of information, in particular in the light of the ECJ's decision of 8th April 2014 on the Data retention Directive, should be kept in mind.

5.11Availability of data protection safeguards - Accountability through security breach notification

5.11.1. Does your national law provide for an obligation to inform the competent authority (DPA or other) and/or the concerned data subjects in case of a security breach related to the data that is processed for tax purposes? Is such obligation envisaged for breaches at data warehouse level?

5.11.2. Does this obligation apply to the private sector (financial institutions, insurance companies, etc.) and/or the public sector (your tax authority)?

5.12. Availability of data protection safeguards - Accountability through DPO

5.12.1. Has your authority appointed a Data Protection Officer ("DPO") that is competent to deal with any questions, complaints, access/rectification requests related to the automatic transfer of information of data subjects?

5.12.2. If so, are the function description and competencies of this DPO established by law?

5.12.3. If not, why not?

5.12.4. Is the DPO involved in the legislation process to point out data protection issues at an early stage?

5.12.5. To your knowledge, have the institutions and insurance companies appointed a DPO to deal with similar questions as mentioned above?

5.13. Availability of data protection safeguards - Special categories of data - Protecting personal data on suspicion of fraud

5.13.1.What are the safeguards for the exchange of the special categories of data as provided for by Article 8 of Directive 95/46, in particular of data relating to offences, criminal convictions or sanctions? What are the safeguards for the exchange of information in case of suspicion of fraud?

5.14. Availability of data protection safeguards - Redress

5.14.1. Is the data that is automatically exchanged subject to legal oversight at national level (national DPA or national judicial or administrative authority) ?

5.14.2. In particular, is redress provided in case of erroneous/unlawful processing and transmission?

5.14.3. How is liability allocated between financial institutions and tax authorities?

5.14.4. Is a full exercise of the control by an independent authority ensured in the case of a data transfer to a third country, as explicitly required by Article 8(3) of the EU Charter of Fundamental Rights and highlighted by the ECJ in the data retention case[25]?

5.15. Availability of data protection safeguards - Other safeguards

5.15.1. Is there a sunset clause[26]/termination clause in bilateral arrangements to terminate the arrangements in case any of the following events happens: entry into force of the European data protection regulation, entry into force of another harmonisation regulatory action at EU level and/or other?

5.15.2. Do you plan any follow-up action in the coming years to take into account the changes that are expected to be implemented by the announced EU Regulation on data protection?

[25]In the ECJ's decision of 8 April 2014 invalidating the Data Retention Directive, the Court highlighted that the retention of data outside EU would prevent the full exercise of the control, explicitly required by Article 8(3) of the Charter, by an independent authority, which is an essential component of the protection of individuals with regard to the processing of personal data.

[26]A sunset provision or clause is a measure within a statute, regulation or other law that provides that the law shall cease to have effect after a specific date, unless further legislative action is taken to extend the law. Most laws do not have sunset clauses and therefore remain in force indefinitely.