AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Aangetekend

[redacted]

[redacted]

Datum
4 juli 2019

Ons kenmerk
z2019-12067

Uw brief van
15 mei 2019

Contactpersoon
[redacted]
070 8888 500

Onderwerp
Besluit op Wob verzoek

Geachte heer [redacted]

Bij brief van 15 mei 2019, ingekomen op 16 mei 2019, heeft u verzocht op grond van de Wet openbaarheid van bestuur (hierna: de Wob) om openbaarmaking van de questionnaire en de daarop ontvangen antwoorden van het Ministerie van Financiën, die is opgesteld in het kader van de "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" [1] aangenomen op 16 december 2015, opgesteld door de Article 29 Data Protection Working Party (WP29).

Op 6 juni 2019 bent u geïnformeerd omtrent de stand van zaken van uw Wob-verzoek.

Inventarisatie van documenten
Uw verzoek ziet op twee documenten. Op basis van uw verzoek is één document aangetroffen, nu bij inventarisatie is gebleken dat de questionnaire en de antwoorden van het Ministerie van Financiën zich in één document bevinden.

Zienswijzen
De AP heeft geconstateerd dat er derde belanghebbenden zijn die mogelijk bedenkingen hebben bij de openbaarmaking van documenten die onder de reikwijdte van uw verzoek vallen. Deze belanghebbenden zijn op 4 juni 2019 in de gelegenheid gesteld hierover een zienswijze te geven. Deze zienswijzen heeft de AP, voor zover van toepassing, in de belangenafweging meegenomen.

[1] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640466

Bijlage(n) 1

AUTORITEIT
PERSOONSGEGEVENS

Datum
4 juli 2019

Ons kenmerk
z2019-12067

Beoordelingskader
Op grond van artikel 3 van de Wob kan een ieder een verzoek om informatie, neergelegd in documenten over een bestuurlijke aangelegenheid, richten tot een bestuursorgaan. Artikel 3, vijfde lid, van de Wob bepaalt dat een verzoek om informatie wordt ingewilligd met inachtneming van het bepaalde in de artikelen 10 en 11 van deze wet. De gevraagde informatie wordt niet verstrekt wanneer zich één of meer uitzonderingen of beperkingen voordoen als vermeld in de artikelen 10 en 11 van de Wob.

Besluit
De AP is van mening dat zich ten aanzien van de door u verzochte documenten geen uitzonderingen of beperkingen voordoen, die openbaarmaking daarvan zouden beperken. De AP heeft besloten te voldoen aan uw verzoek tot openbaarmaking door toezending van de questionnaire en de daarop ontvangen antwoorden van het Ministerie van Financiën, nu deze zich in één document bevinden. De AP wijst er ten overvloede op dat de hiervoor genoemde questionnaire reeds openbaar gemaakt is als Annex bij de hier bovengenoemde guidelines, te raadplegen in de link in de voetnoot.

Een afschrift van dit besluit zendt de AP aan de belanghebbenden.

Hoogachtend,
Autoriteit Persoonsgegevens,
Namens deze,

[redacted]

Senior Adviseur Staftaken

Rechtsmiddelenclausule
Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit ingevolge de Algemene wet bestuursrecht een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag, onder vermelding van "Awb-bezwaar" op de envelop. Het indienen van een bezwaarschrift schort de werking van dit besluit niet op.

Cover letter

Dear *[National Tax Authority]*,

The Article 29 Working Party[1], the group of the data protection authorities of the European Union set up by Article 29 of the "Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", has prepared a questionnaire addressed to national tax authorities.

The main aim of the questionnaire is to assess 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 automatic inter-state exchange of data is an anti-evasion tool which has been foreseen by a number of legal instruments, at both international and European level (e.g. "Foreign Account Tax Compliance Act"- FATCA-, OECD/Council of Europe Multilateral Convention on Mutual Administrative Assistance in Tax Matters, OECD Common Reporting Standard, Directive 2011/16/EU on administrative cooperation in the field of taxation, Directive 2014/107/EU amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation).

The results of the questionnaire will provide the Working Party with useful background information for the preparation of WP29's Guidelines for a correct application of data protection principles in this sector, which will be soon addressed to national governments.

Therefore, on behalf of the WP29, we transmit the questionnaire – together with an Explanatory Note to provide a better understanding of the previous work of the WP29 in this field, and the aims of the questionnaire - **with the kind request to provide your answers to the following address: [*DPA's e-mail address*] by 18 May 2015.**

The WP29 thanks in advance for the cooperation and is convinced that starting a constructive dialogue with the institutions competent for tax matters is an important step to ensure that anti-evasion policies are conceived with due respect for the right to private life and the protection of personal data from earliest stages of procedure, as recognised by European and international legal instruments.

---

[1] The Article 29 Working Party is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Explanatory Note

The data protection authorities of the European Union, represented in the Article 29 Working Party (WP29) are examining the new developments at European and international level which aim to introduce mechanisms for the automatic inter-state exchange of personal data for tax purposes.

Part of the work of the WP29 is to investigate issues affecting individuals' right to the protection of personal data, as provided for by the EU data protection directive, Directive 95/46/EC[2].

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"), which (on the basis of the Multilateral Convention on Mutual Administrative Assistance in Tax Matters) includes common due diligence procedures to be used by financial institutions to identify reportable accounts, and contains a Model Competent Authority Agreement that may be used by States to allow the financial account information to be exchanged.

At European level, Directive 2011/16/EU on administrative cooperation in the field of taxation underwent a revision process which led to the adoption - on 9th of December 2014 - of Council Directive 2014/107/EU. Directive 2014/107/EU aims at ensuring a comprehensive Union-wide approach to the automatic exchange of information for anti-tax evasion, and substantially incorporates the OECD 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[3] and on 1st October 2012[4], concerning FATCA
- Letter on OECD CRS adopted on 18 September 2014[5].

More recently, on 4 February 2015[6], the WP29 adopted a "Statement on automatic inter-state

---

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

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

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

[5] 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

[6] The Statement is available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-

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 ECJ Decision of 8 April 2014[7] which 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. In such decision, the Court stressed the need for legislation to provide access for the competent national authorities to personal data and their subsequent use for purposes of prevention, detection or prosecution of criminal offences. The Court required objective criteria determining the limits for such operations, given the extent and seriousness of the interference with the fundamental rights as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. National legislators, competent authorities and institutions should be aware of this principle, which applies *a fortiori* for those processing operations designed to monitor behavior which does not have a criminal connotation.

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 can afford additional and consistent safeguards in terms of data protection.

To that end, the WP29 considers it 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.

In order to obtain such factual findings and background information, the WP29 prepared the questionnaire to be transmitted by each national DPA to national tax authorities.

Aims of the questionnaire

This questionnaire is mainly aimed to:

- Assess compliance of national tax authorities with European data protection law in the context of the automatic exchange of personal data for tax purposes;

- Gather more precise information on the current availability of specific data protection safeguards in the automatic data transfers, agreements and statements of protocol concluded between the national tax authorities and their counterparts in and outside of the EU;

- Gather background information for future preparation of 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.

* * *

recommendation/files/2015/wp230_en.pdf

[7] 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

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?
Yes

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

- FATCA-agreement between the Netherlands and the US;
- Several Memoranda of Understanding (MoU) regarding automatic exchange of information under the bilateral tax conventions.
- Outside the EU the Netherlands concluded MoU's on automatic exchange of information with Argentina, Australia, Canada, Ghana, Japan, New Zealand, South Corea.
- All bilateral tax conventions are published in the Bulletin of Acts;
- All MoU's are published in the Government Gazette (www.overheid.nl/staatscourant).

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?

- The FATCA-agreement is binding to the US and the Netherlands;
- The MoU's are binding to the Netherlands and the MoU-partner.

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

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?
The Ministry of Finance consulted on a regular basis with representatives of the financial institutions and insurance companies while negotiating the FATCA-agreement with the US. The consultations went on when we implemented the agreement in national legislation.

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?
There were no specific agreements or arrangements made with the private sector regarding FATCA

or regarding AEoI.

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? Yes

2.2. If yes, can you provide us with a copy of the agreement? Not necessary, we implement the EU Directive 2014/107/EU in our national law. Regarding non EU countries the Netherlands will use the aforementioned Model (MCAA).

2.3. Does your authority (intend to) use the Model Competent Authority Agreement as a basis for exchanging data? See answer in 2.2.

2.4. If so, what is the definition given by your legal framework of "low risk accounts" to be excluded from data collection?
In the definition of excluded account in our domestic legislation we refer to Section VIII, subparagraphs C(17)(a) through (g), of Annex I of Directive 2011/16/EU (which was added in Directive 2014/107/EU). This definition includes the low risk accounts that are excluded (Section VIII, subparagraph C(17)(g) of Annex I of Directive 2011/16/EU). In this definition we refer to a list of excluded accounts. This list will be published by the EU.

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? Yes

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? The implementation of Directive 2014/107/EU in national law will take place in 2015.

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? Yes

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[8] 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.

e. We are trying to harmonize the approaches of the EU member states regarding data protection principles towards third countries without adequacy decision. We are preparing a note that may be a good basis for discussing a possible common notification for EU countries under section 7,1,d of the CRS MCAA (specification of safeguards for the protection of personal data). The note will be prepared in consultation with Dutch data protection experts, TAXUD (informally) and the OECD Secretariat and will contain a draft notification that may be used by Competent Authorities of EU Member States to allow them to exchange information under the MCAA with non EU jurisdictions. It will also contain an overview of the data protection principles contained in the EU Data Protection Directive that are not part of the draft notification, together with a short explanation why they were not included. We do not see merit in the options a, b, c or d.

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[9] - 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 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? Yes, we made a DPIA and it was sent to the national DPA together with the bill implementing the Directive into national law.

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. The guidance of the in-house counsellors was orally.
c. other (please explain)

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

---

[8] 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.

[9] See previous footnote.

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? Yes

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? Yes

5.2.3. If so, can you give us the references of such law and specify which instruments at international level are transposed? In the 'Wet op de international bijstandsverlening bij de heffing van belastingen' (WIB) all Directives regarding exchange of information are implemented. The data protection safeguards in this law are equally applicable to the exchange of information with third countries.

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? N/A

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

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

The collection of data does not 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?

In general, the data collected may pertain to depository accounts, custodial accounts, equity and debt interests and cash value insurance/annuity contracts. However, low risk accounts, like retirement and pensions accounts, and accounts of low risk financial institutions, are excluded.
Most important criteria to identify the relevant accounts is whether the aforementioned accounts are financial institution-accounts held by (non excluded) reportable persons. E.g. under CRS reportable persons are: fiscal residents of a CRS-partner jurisdiction or passive non financial entities with one or more controlling persons that is a reportable person. Exclusions include: corporations whose stock is regularly traded on an established securities market (and their related entities); government entities; and Financial Institutions. A controlling person of a passive non financial entity is the natural person(s) who exercises control over the Entity (generally controlling ownership interest in the entity - often interpreted $\geq 25\%$ ownership).
For trusts (and equivalents), the settlor(s), trustee(s), protector(s), beneficiary(ies), and any other natural person(s) exercising effective control over the trust.
There are four different categories of financial accounts. There are preexisting individual accounts, new individual accounts, preexisting entity accounts and new entity accounts. For each category different due diligence rules apply.
See for detailed information on the data to be collected article 8 (3a) of the Directive 2011/16/EU, that will be implemented in our primary law (WIB) before the end of 2015. For FATCA the data to be collected by Financial Institutions has already been laid down in the law.

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

No, NL does not duplicate the 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*).

Yes. The Netherlands has implemented the data protection principles, as foreseen by Directive 95/46/EC. The data to be exchanged are identified in the law, see 5.3.2. The principles of proportionality, subsidiarity and so on, are implemented in the relevant laws, e.g. the Law on International Assistance (WIB), the Law on Protection of Personal data (Wbp), our General Tax Law (AWR), the Law on Data Retention (Archiefwet).

5.4. Availability of data protection safeguards - Proportionality[10]

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?[11]

Parties are prevented from engaging in "fishing expeditions" because - on the basis of the Directive on Administrative Cooperation (DAC) - our DTA's and our other EOI instruments may only request for information that is foreseeably relevant to the tax affairs of a given person. Furthermore, the requests for information from the Netherlands tax offices always have to go out via and after scrutiny by the Netherlands Competent Authority (B/CLO Almelo) who is dedicated to and well trained in strictly adhering to the legal framework on EOI.

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.).

Under CRS and FATCA the data to be exchanged are captured by the Financial Institutions in conformity with the due diligence and collecting procedures described in the CRS-standard and the FATCA-treaty with the US. Part of the due diligence procedures is capturing the foreign TIN. Part of the collecting procedure is the exclusion of low risk data.
The relevant data collected by the Financial Institutions are send to the Central Administration Center of the Tax Administration with a view to international exchange with the CRS-partners or the US. Both the CRS-standard and the FATCA-treaty will be c.q. are implemented in the national law and regulations on International Administrative Assistance (WIB).
With regard to IT technique: The automatic exchange of information shall be sent using a standard computerised format aimed at facilitating such automatic exchange.

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

Given the increased opportunities to invest abroad in a wide range of financial products and with a

[10] 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.

[11] 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

view to our longtime experience with EOI on request and spontaneous exchange it has become clear that these instruments are not tailored to combat tax evasion in the many situations where a tax administration has no (clear) indications (necessary to comply with the foreseeable relevancy criterion) that tax payers conceal taxable income or assets from their tax administration by using (bank) accounts or interposed vehicles abroad. This is only possible via automatic exchange.

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[12]?

For AEOI on (bank)account information we have in place the FATCA treaty with the US (signed in 2013). The first exchanges will take place in September 2015. Furthermore, as EU MS we are subjected to the DAC2 (to be implemented before 2016 and first exchanges starting as of September 2017). Furthermore, we have committed to being early adopter in the OECD/Global Forum CRS process. The Netherlands is party to the OECD/Council of Europe Multilateral Convention on Administrative Assistance on Tax Matters. The Netherlands signed the CRS-MCAA, based on article 6 of this Convention, in 2014. Before the end of this year, after the preliminary peer reviews regarding data protection and safeguards are completed, we expect to enter into exchange relationships under the CRS-MCAA, with the first exchanges starting as of September 2017.

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.

The Netherlands' tax legislation provides for specific data retention periods pertaining to the retention obligations for tax payers/third parties. The data retention period for most types of information (e.g. account information) is seven years (article 52 AWR). For a few specific types of information data retention periods may vary from 5 to 10 years. The retention period for retaining tax relevant information by the tax administration is regulated in the Law on Data Retention.

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?

The Law on Data Retention (Archiefwet) applies to both categories.

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

Yes. For this we have a standard procedure taken up in our Law on protection of personal data (Wbp) for requests and complaints. This procedure is made public by a leaflet called *"De Belastingdienst en de Wet bescherming persoonsgegevens (Wbp")*. This leaflet contains among more information on the right to view data and the correction of data by individual tax payers.

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?

---

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

The Netherlands competent authority has committed to and is therefore bound to adhere to the data protection safeguards required by the FATCA and CRS rules.

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)?

This question is not clear to us. The Netherlands does not intend to store the data forwarded by national institutions for FATCA or CRS purposes. We intend to exchange the data in conformity with our obligations in the FATCA-treaty and CRS (international) legal exchange instruments.

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.

The financial account information received on the basis of the FATCA treaty and CRS legislation/treaties will be forwarded to the tax offices to be taken into account in the usual process of checking/controlling the individual tax returns. Furthermore, we expect to be able to process these data in the framework of the pre filled tax return within a few years.

5.6.4. In that case, does your authority accept full responsibility as a "data controller"[13] under Directive 95/46/EC vis-à-vis the data subjects?

Yes. The Netherlands adheres to the Directive 95/46/EC.

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?

Not applicable.

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.

Yes. Our laws are published in the Staatsblad (Bulletin of Acts). Our international arrangements are published in the Tractatenblad (treaties) and the Staatscourant (government gazette). You may find them on www.overheid.nl.

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?

Yes, but they have to do that in a way that this may not jeopardize tax investigations.

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

---

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

Data subjects are aware of the data exchange as we publish all our international arrangements in this respect. We will also broadly publicize this information via other appropriate (social) media. Furthermore, the information received from counterparts will be used to determine the correctness of the tax return of the individual tax payer involved and – in the near future – to prefill the tax return of the individual tax payer involved.

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?

Not applicable.

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?

No.

5.8.2. If not, why not?

Tax infringement may take many forms. The essence is that there is tax infringement if and when tax laws have not been obeyed. With regard to not fulfilling the obligations to send in correct and timely tax returns and the obligations to cooperate with the tax administration we have specific provisions in our General Tax Law (AWR).

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?

Our law on international exchange of information (WIB) implements the EU Directives on Administrative Assistance and our treaty instruments. So, if the Directive and/or treaties allow for the use of exchanged information for other than tax purposes (which – under certain conditions – the Directive and some of our treaties do) this is allowed by our national law. The other purposes may be money laundering, corruption, financing of terrorism, social security. This depends on the legal instrument.
The conditions are usually reciprocal and having national laws allowing for this other use. For criminal tax matters we may also use mutual legal assistance treaties.

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 to exchange information on criminal tax matters based on bilateral or multilateral treaties[14] 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[15]?

---

[14] 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

[15] 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.

See 5.8.3.

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

Yes. Please note that the onward transfer from receiving authority to third authorities is often not possible or bound by strict limitations.

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.

The Dutch law on protection of personal data (Wbp) provides for direct rights of access, rectification en right to object.
Right of access (art. 35 Wbp): Any data subject may, at reasonable intervals, ask the controller whether personal data relating to him are processed. A request must be answered within four weeks. The answer must contain the following information: a summary of the data of the data subject processed by the controller, the purpose(s) of the data processing, the categories of data to which the processing relates, (categories of) recipients, information about the origin of the data
Right of rectification (art. 36 Wbp): A data subject may ask the controller to correct the data relating to him. The desired changes must be indicated in the request. Correction implies: correction, supplementing, deletion, blocking. The data subject must be informed within four weeks about the decision.
Right to object (art. 40 Wbp): when data are processed on the ground that this processing is necessary for the proper performance of a public law duty performed by the controller, the data subject may register an objection on grounds in connection with his particular personal circumstances. The controller has to decide whether the objection is well founded within four weeks.

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?

There are restrictions to data subjects rights based on art. 43 Wbp.
The obligation to provide information to data subjects, and requests for access and rectification may not have to be fulfilled if this is necessary

- In the interest of state security;
- For the prevention, investigation and prosecution of criminal offences;
- For important economic or financial interests of the state and other public bodies;
- For the protection of the data subject or of the rights and freedoms of others;
- For the supervision of compliance with legal provisions established for the investigation and prosecution of criminal offences, or in the economic and financial interest of the state and other public bodies.

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.?
The aforementioned articles (art. 35, 36 and 40 Wbp) apply to all controllers.

5.10. Availability of data protection safeguards - Data security[16]

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

- Background Checks and contracts for employees and contractors;
- Training and developing awareness of employees regarding confidential information;
- Access control: Access only to the information if someone is entitled to have access;
- Identification and authentication of a user by account name and password;
- Security assessments;
- Departure policy: end all access possibilities when an employee leaves;
- Physical Document Storage, Maintenance;
- Protection of the systems and communications;
- Risk assessment to identify risks and the potential impact of unauthorised access, use and disclosure of information.

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? See 5.10.1.

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.

- Cryptographic controls are being used in compliance with applicable laws and regulations. Tax offices follow the guidelines for protecting sensitive information and make use of encryption when prescribed and permitted by legislation and regulations. Legal requirements are incorporated in the security policy handbook of the Tax administration.
- Network encryption is applied to protect the confidentiality of sensitive and critical information during their transport over the National Domains. Transport of information between locations of the Tax Administration is standard encrypted. Part of PKI, SSL Portal and holders of certificates. For the common domain we use the CCN network.
- Content sent and received on physical media (such as dvd's, harddrives and usb-devices) is protected by using AES256 encryption, in a ZIP-container.
- Electronic data exchange via internet or private networks is protected with server (and sometimes client)side certificates (PKI-overheidscertificaten).
- Some exchanges protect the content by defining a SHA-512 digest value or are otherwise digitally signed.
- For some exchanges there is additional access control: username, password and sms-verification.

5.11 Availability 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?

A Law providing an obligation to inform the DPA about major security breaches in general is to be

[16] 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.

implemented this year.

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

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? Yes

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

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? Yes

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

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?

Under our international exchange instruments we can only exchange tax related information. The usual data protection safeguards and refusal grounds apply. The international exchange instruments and the confidentiality/data protection rules therein do not differ between categories of data.

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) ? Yes

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

5.14.3. How is liability allocated between financial institutions and tax authorities? There are no specific agreements between FI's and the tax authorities with respect to allocate the liability.

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[17]? No, the Netherlands only transfers

[17]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.

data to third countries with a sufficient level of data security. We don't know whether that third country has appointed an independent authority.

5.15. Availability of data protection safeguards - Other safeguards

5.15.1. Is there a sunset clause[18]/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? No

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?
Yes

[18] 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.